Council of the European Union

Brussels, 18 November 2025
(OR. en)

15560/25
ADD 1

**Interinstitutional File:**
**2020/0361 (COD)**

**COMPET 1179**
**MI 918**
**JAI 1707**
**TELECOM 408**
**CT 160**
**PI 197**
**AUDIO 115**
**CONSOM 260**
**CODEC 1836**
**JUSTCIV 188**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director |
| date of receipt: | 17 November 2025 |
| To: | Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union |
| No. Cion doc.: | SWD(2025) 368 final |
| Subject: | COMMISSION STAFF WORKING DOCUMENT Accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts |

Delegations will find attached document SWD(2025) 368 final.

Encl.: SWD(2025) 368 final

EUROPEAN
COMMISSION

Brussels, 17.11.2025
SWD(2025) 368 final

**COMMISSION STAFF WORKING DOCUMENT**
***Accompanying the document***

**Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee**

**on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts**

{COM(2025) 708 final}

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES



# ACRONYMS AND ABBREVIATIONS

| Acronym | Definition |
|---|---|
| AI Act | Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) |
| AVMSD | Directive 2010/13/EU of 10 March 2010 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), as amended by Directive (EU) 2018/1808 |
| BR | Regulation (EU) 2023/1542 of 12 July 2023 concerning batteries and waste batteries, repealing Directive 2006/66/EC and Regulation (EU) No 2019/1020 (Batteries Regulation) |
| Brussels Ia Regulation | Regulation (EU) No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) |
| CDSMD | Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market (Copyright in the Digital Single Market Directive) |
| CLP | Regulation (EC) No 1272/2008 of 16 December 2008 on classification, labelling and packaging of substances and mixtures (CLP Regulation) |
| CPC | Regulation (EU) 2017/2394 of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Consumer Protection Cooperation Regulation) |
| CRD | Directive 2011/83/EU of 25 October 2011 on consumer rights (Consumer Rights Directive) |
| DFA | Digital Fairness Act |
| DMA | Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) |
| DP | Regulation (EU) 273/2004 of 11 February 2004 on drug precursors, and Council Regulation (EC) No 111/2005 of 22 December 2004 laying down rules for the monitoring of trade between the Community and third countries in drug precursors |
| DSA | Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) |
| ECD | Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive) |
| Ecodesign | Regulation (EU) 2024/1781 of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products (Ecodesign for Sustainable Products Regulation) |
| EECC | Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code |
| EED | Directive (EU) 2023/1543 of 12 July 2023 on the exchange of electronic evidence in criminal matters (e-evidence Directive) |
| eIDAS | Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), as amended by Regulation (EU) 2024/1183 of 11 April 2024 (eIDAS 2 Regulation) |
| EMFA | Regulation (EU) 2024/1083 of 11 April 2024 establishing a common framework for media services in the internal market (European Media Freedom Act) |
| EPR | Regulation (EU) 2019/1148 of 20 June 2019 on the marketing and use of explosives precursors (Explosives Precursors Regulation) |
| E-privacy | Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) |
| EU | European Union |

| | |
|---|---|
| GDPR | Regulation (EU) 2016/679 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 (General Data Protection Regulation) |
| GPSR | Regulation (EU) 2023/988 of 10 May 2023 on general product safety (General Product Safety Regulation) |
| INFOSOC | Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive) |
| IPR | Intellectual Property Rights |
| IPRED | Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (IPR Enforcement Directive) |
| MCPR | Regulation (EU) No 305/2011 of 9 March 2011 laying down harmonised conditions for the marketing of construction products (Construction Products Regulation) |
| MSR | Regulation (EU) 2019/1020 of 20 June 2019 on market surveillance and compliance of products (Market Surveillance Regulation) |
| Net Neutrality | Regulation (EU) 2015/2120 of 25 November 2015 laying down measures concerning open internet access (Net Neutrality Regulation) |
| NIS2 | Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) |
| OLR | Regulation (EC) No 1005/2009 of 16 September 2009 on substances that deplete the ozone layer (Ozone Layer Regulation) |
| P2B | Regulation (EU) 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Platform-to-Business Regulation) |
| PLD | Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive) (under revision, COM(2022) 495 final) |
| PPWR | Proposal for a Regulation COM(2022) 677 final on packaging and packaging waste (Packaging and Packaging Waste Regulation) (not yet adopted) |
| Rome I | Regulation (EC) No 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I Regulation) |
| Rome II | Regulation (EC) No 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II Regulation) |
| STR | Regulation (EU) 2024/1028 of the European Parliament and of the Council of 11 April 2024 on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724 |
| TCO | Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online (Terrorist Content Online Regulation) |
| TSD | Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive) |
| TSR | Proposal COM (2023) 462, on the safety of toys (Toy Safety Regulation) |
| TTPA | Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising |
| UCPD | Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices (Unfair Commercial Practices Directive) |
| UCTD | Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Contract Terms Directive) |
| VAT | Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (VAT Directive) |
| VAWDV | Directive (EU) 2024/2810 of 14 December 2024 on combating violence against women and domestic violence (VAW Directive) |
| VLOP | Very Large Online Platform (as defined in Regulation (EU) 2022/2065 – Digital Services Act) |
| VLOSE | Very Large Online Search Engine (as defined in Regulation (EU) 2022/2065 – Digital Services Act) |

## 1. CHAPTER I: INTRODUCTION

During the negotiations towards the adoption of Regulation (EU) 2022/2065[1] (the **Digital Services Act** or **DSA**), co-legislators particularly insisted on the need for guidance towards public authorities, economic operators and citizens on the relationship between the DSA, as a horizontal fully-harmonized Regulation and part of the EU digital rulebook, and other pieces of sector-specific legislation.

Furthermore, co-legislators wanted to include a short-time review clause to allow for adaptions, if necessary, of the delineation between 'very large online platforms' (VLOPs) and 'very large online search engines' (VLOSEs).

Therefore, pursuant to Article 91 DSA, **by 17 November 2025** the European Commission shall evaluate and report to the European Parliament, the **Council** and the **European Economic and Social Committee** on:

> (a) the application of Article 33 DSA that sets out the threshold and process for designation of very large online platforms (VLOPs) and very large online search engines (VLOSEs), including the scope of providers of intermediary services covered by the obligations applicable to VLOPs/VLOSEs, and
>
> (b) the way that the DSA interacts with other legal acts, in particular those listed in Article 2(3) and (4) DSA.

This Staff Working Document accompanies the report which has been adopted as *Communication on the report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts.*

**Chapter II** provides an overview of the implementation of Article 33 DSA since it became applicable on 16 November 2022 pursuant to Article 93(2) DSA, and until the date of publication of the report. The chapter presents the designations as VLOPs and VLOSEs conducted during the reporting period and the Commissions' services assessment of the criteria behind those, including the threshold of 45 million average monthly active recipients ('AMARs') of the service in the Union that is established in Article 33(1) DSA.

**Chapter III** describes how the Digital Services Act interacts with the Union legal acts referred to in Article 2(3) and (4) DSA, and other legal acts that the Commission services identified to intersect with the DSA. The legal acts referred to in Articles 2(3) and (4) DSA are of particular importance due to their link to the scope and objectives of the DSA and the relevance of guaranteeing a complementary Union legal framework that effectively ensures a safe online environment.

**Chapter IV** includes information on the 2025 surveys which have been conducted for the overall preparation of the document that were addressed to i) the Digital Services Coordinators ("DSCs") and other competent authorities at national level ii) designated VLOPs and VLOSEs and non-designated online platforms and search engines, and iii) civil society organizations ("CSOs").

Finally, **Chapter V** concludes by presenting the main findings of this document.

The Commission services based its assessments on a study produced by an external contractor and on other data sources such as submissions by individuals and associations.

---

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1, ELI: Regulation - 2022/2065 - EN - DSA - EUR-Lex).

## 2. CHAPTER II: APPLICATION OF ARTICLE 33 OF THE DIGITAL SERVICES ACT

Given the novelty of the asymmetric approach introduced in the DSA, during the negotiations leading to the adoption of the DSA, co-legislators considered it necessary to evaluate, after the first three years of application of the Regulation, the implementation of Article 33 DSA, including whether the threshold established in Article 33 to designate VLOPs or VLOSEs[2] captured the relevant intermediary service providers that may lead to the best known systemic risks.

Recital 76 DSA explains that the asymmetric approach retained is due to the reach of very large online platforms and very large online search engines, which may cause systemic risks, different in scope and impact from those caused by smaller online platforms and may have a disproportionate impact in the Union. Such significant reach should be considered to exist where such number exceeds an operational threshold set at 45 million, that is, a number equivalent to 10 % of the Union population. Recital 137 DSA already advances that such threshold should allow to identify those services whose failure to comply with the specific obligations applicable to them may affect a substantial number of recipients of the services across different Member States and may cause large societal harms, while such failures may also be particularly complex to identify and address.

Pursuant to its Article 2(1), the DSA establishes a general legal framework applicable to all intermediary services provided in the Union, with an asymmetric system of obligations based on the function and reach of the services at stake. As clarified by recital 75, in view of their reach and systemic impact on the public debate, the dissemination of information, and economic transactions across the Union, services designated by the Commission as VLOPs or VLOSEs are subject to the broadest set of obligations.

Article 33 DSA establishes that the Commission shall designate such services as VLOPs or VLOSEs if their number of average monthly active recipients in the Union is equal to or higher than 45 million. This is, as clarified by recital 76, a number equivalent to 10% of the Union population. However, in accordance with Article 33(2) and recital 76 DSA, this operational threshold is subject to potential change in view of increases or decreases of the Union population (for instance in the case of new adhesions to the Union). According to that Article, the Commission is mandated to adjust such threshold where the Union's population increases or decreases at least by 5 % in relation to its population in 2020. According to the latest data from Eurostat, the population of the Union has increased by 2,7 million, which is far from that percentage.[3]

The DSA establishes additional obligations in Section 5 of Chapter III for the providers of these services and as regards the designated services, which enter into application four months after their designation.

Article 33(4) DSA establishes that the Commission, after consulting the Member State of establishment or after taking into account the information provided by the Digital Services Coordinator of establishment pursuant to Article 24(4) DSA, shall adopt a decision designating as a VLOP or VLOSE the online platform or the online search engine which has a number of AMARs equal to or higher than 45 million. To that end, that Article allows the Commission to take its decision on the basis of (i) data reported by the provider of the online platform or of the online search engine pursuant to Article 24(2) DSA, (ii) information requested pursuant to Article 24(3) DSA, or (iii) any other information available to the Commission.

To determine whether online platforms and online search engines reach the above-mentioned threshold of 45 million AMARs set out in Article 33 of the DSA, and, more broadly, to ascertain their size and reach, it is necessary that providers of such services make public the number of AMARs for each of their services.

In this context, Article 24(2) DSA obliges providers of online platforms and online search engines to publish information on AMARs of each of their services individually in the Union, by 17 February 2023 and at least once every six months thereafter, calculated as an average over the period of the past six months. The

---

[2] According to Article 33(1), online platforms and online search engines are considered 'very large' when they have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and after being designated as pursuant to paragraph 4 of the same Article.

[3] See: [demo_pjan] Population on 1 January by age and sex [last checked on 24 October 2025].

information on the number of AMARs must be made publicly available in a section of the platform or search engine's online interface. The number of AMARs in the Union shall be counted for each service individually, reflecting all unique recipients who are actually engaging with the service at least once in a given period of time.

The basic legal elements concerning the determination of the number of AMARs of the services in the Union are set out in Article 3(b), (p) and (q) and Article 24(4) DSA, as further clarified by recital 77. Moreover, on 31 January 2023, the Commission services published a guidance on the requirement to publish user numbers that aimed at answering some of the practical questions that had been raised on the provisions of the DSA concerning the obligation to publish information on the number of AMARs.[4]

The DSA defines under Article 3(b), a recipient of the service as "any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible". Article 3(p) of the DSA defines an active recipient of an online platform as "a recipient of the service that has engaged with an online platform by either requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface". Article 3(q) of the DSA defines an active recipient of an online search engine as "a recipient of the service that has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface".

Recital 77 DSA further clarifies how the notion of engagement must be interpreted for the purposes of determining whether a recipient of a service is an active recipient of that service. According to that recital, engagement is not restricted to mere interaction by the users with the information of the service by clicking on, commenting, liking, sharing, purchasing or carrying out transactions, but also refers to users being exposed to information disseminated in the service, such as viewing it or listening to it, as well as providing information, such as traders on online platforms that allow consumers to conclude distance contracts with traders. In contrast, owners of websites indexed by online search engines should not be considered active recipients given that they do not actively engage with the service.

The notion of engagement does not include incidental use of a service by recipients of another intermediary services where that other service indirectly makes available information hosted by the first service through linking or indexing. Moreover, recipients that use different online interfaces, such as apps and web browsers, including where services are accessed through different URLs or domain names, should be counted only once where possible. Further, providers are also allowed to discount automated users such as bots or scrapers, to the extent possible.

Finally, recital 77 specifies that the rules of the DSA cannot be understood as allowing or mandating the performance of specific tracking of individuals online.

### 2.1. Scope of designated services

Since the start of application of the DSA, and until the date of publication of this document, the Commission has adopted decisions designating 23 online platforms and 2 online search engines as VLOPs and VLOSEs, and one decision terminating the designation of a VLOP[5].

As the table below shows, the first batch of 19 designations took place in April 2023, solely seven months after the publication of the DSA, on the basis of the user numbers provided by the online platforms. Eight months later, the Commission designated three pornographic platforms; and, in April 2024, it designated one more pornographic platform and two fast-growing online marketplaces.

To give a sense of the rapid pace of evolution in this area, when the DSA was adopted, neither Temu nor Shein had entered the European market: Temu started offering its online marketplace service in Europe in April

[4] DSA: Guidance on the requirement to publish user numbers | Shaping Europe's digital future.

[5] All information regarding the designations and further enforcement actions can be found in https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

2023, and by October 2024 (six months after designation based on the information available to the Commission at the time) it reported approximately 93.7 million average monthly active users in the EU. Shein, in turn, originally a retailer operating in several Member States, started operating as a hybrid marketplace in the Union in June 2023; on February 2024, Shein reported an average of 108 million average monthly active recipients in the Union, and it was designated as a VLOP by the Commission two months later.

This illustrates that both the quantitative threshold, alongside the obligation for providers to publish AMARs every six months, and the designation process established in Article 33 of the DSA, are fit for purpose and adapt to a fast-changing online environment, as it is able to very quickly capture online platforms and online search engines even in scenarios of rapid growth after entering the Union market. In this sense, the number of designation decisions adopted has exceeded the estimation foreseen in the impact assessment in terms of number of designated entities.[6]

The designated intermediary services have to be, first and foremost, an "online platform" or an "online search engine" pursuant to Articles 3(i) and (j) DSA, respectively.

This is, as foreseen by the impact assessment of the DSA, a difference in relation to Regulation (EU) 2022/1925 (the 'DMA'), which relates to the different objectives of both Regulations.[7] While the DSA has the main objective of addressing societal risks, including economic risks, associated with the provision of the services that fall under its scope and, in particular, in relation to VLOPs and VLOSEs, the DMA primarily aims at tackling economic concerns associated with the gatekeeper power which undermines fairness and contestability in digital markets. While there may be an overlap between the categories of VLOPs and VLOSEs designated under the DSA, and of the core platform services provided by the designated gatekeepers under the DMA, the latter includes many more categories than the former (i.e. online intermediation services; online search engines; online social networking services; video-sharing platform services; number-independent interpersonal communications services; operating systems; web browsers; virtual assistants; cloud computing services; online advertising services).[8] This allows for a more granular scoping of the services taken into account for the purposes of the DMA in comparison to the DSA, where the scope of the relevant services is necessarily broader. Therefore, the designated VLOPs and VLOSEs cover a wide range of categories of intermediary services[9] including social media, marketplaces, adult-content platforms, app stores, and search engines.

Moreover, with the evolution of intermediary services, which often combine different functionalities that may fall within distinct legal definitions, the two legal categories of online platform and online search engine are becoming more intertwined. Additionally, some functionalities that fall under these legal categories are often combined with other functionalities beyond the scope of these categories, for example, because they are interpersonal communication services[10] or because they do not intermediate content from third parties. For example, this is the case of the designated VLOP Zalando, where products marketed directly by the provider of that service are displayed alongside products marketed by third-party sellers. In this case, the designation decision was subject to an action for annulment before the General Court, which delivered its judgement in Case T-348/23, *Zalando v Commission*, on 3 September 2025,[11] ruling that "*the Zalando platform must be regarded*

[6] Commission Staff Working Document Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC {COM(2020) 825 final} - {SEC(2020) 432 final} - {SWD(2020) 349 final part 1, page 27, and part 2, Annex 4.

[7] Impact Assessment of the DSA, part 2, page 64.

[8] Article 2 of the DMA.

[9] More than originally foreseen in the Impact Assessment of the DSA, part 2, page 64.

[10] Within the meaning of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

[11] ECLI:EU:T:2025:821.

*as an online platform within the meaning of Article 3(i) of Regulation 2022/2065 in so far as third-party sellers market products there under the Partner Programm*."[12]

Further, most intermediary services also evolve in themselves throughout time, which requires that the scope of the designated VLOPs and VLOSEs is sufficiently broad to take account of these technological and market realities. Given that Article 34(1) DSA establishes that providers of VLOPs and VLOSEs shall conduct the risks assessments referred to in that Article, among others, "*prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article*", it is crucial that the scope of the designated VLOPs and VLOSEs take account of such an evolutive nature of the functionalities that may impact the provision of those services.

This presents certain challenges related, among others, to the determination of the scope of the designated VLOPs and VLOSEs and the characterisation of newly launched features within the categories laid down in the DSA, as well as those related to the calculation of the average monthly active recipients in the Union of those services pursuant to Article 24(2) DSA. For example, in the above-mentioned *Zalando v Commission* case, the General Court ruled that,[13] "*[i]n so far as the applicant submits that it was unable to distinguish, from among the 83.341 million persons included for the purposes of calculating the [average monthly active recipients], those who had actually been exposed to information from third-party sellers from those who had not been exposed to that information, the Commission is entitled to consider that all those persons were deemed to have been actually exposed to that information*."

An overview of the designation decisions adopted until the publication of this document, the sector in which these services operate, and the Member State of establishment is presented below[14]:

***Table 1: Overview of the designation decisions adopted***

| Service | VLOP or VLOSE | Designation decision | Date of adoption of designation decision | Sector | Member State of establishment |
|---|---|---|---|---|---|
| AliExpress | VLOP | C(2023) 2736 final | 25 April 2023 | Marketplace | Netherlands |
| Amazon Store | VLOP | C(2023) 2746 final | 25 April 2023 | Marketplace | Luxembourg |
| App Store | VLOP | C(2023) 2726 final | 25 April 2023 | App Store | Ireland |
| Bing | VLOSE | C(2023) 2728 final | 25 April 2023 | Search engine | Ireland |
| Booking | VLOP | C(2023) 2748 final | 25 April 2023 | Marketplace | Netherlands |
| Facebook | VLOP | C(2023) 2756 final | 25 April 2023 | Social media | Ireland |
| Google Maps | VLOP | C(2023) 2737 final | 25 April 2023 | Mapping service | Ireland |
| Google Play | VLOP | C(2023) 2738 final | 25 April 2023 | App Store | Ireland |
| Google Search | VLOSE | C(2023) 2731 final | 25 April 2023 | Search engine | Ireland |
| Google Shopping | VLOP | C(2023) 2733 final | 25 April 2023 | Marketplace | Ireland |

[12] T-348/23, para 45.
[13] T-348/23, para 67.
[14] Information also available at the Commission's website: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

| | | | | | |
|---|---|---|---|---|---|
| Instagram | VLOP | C(2023) 2734 final | 25 April 2023 | Social media | Ireland |
| LinkedIn | VLOP | C(2023) 2735 final | 25 April 2023 | Social media | Ireland |
| Pinterest | VLOP | C(2023) 2729 final | 25 April 2023 | Social media | Ireland |
| Snapchat | VLOP | C(2023) 2730 final | 25 April 2023 | Social media | Netherlands |
| TikTok | VLOP | C(2023) 2720 final | 25 April 2023 | Social media | Ireland |
| X (formerly Twitter) | VLOP | C(2023) 2721 final | 25 April 2023 | Social media | Ireland |
| Wikipedia | VLOP | C(2023) 2742 final | 25 April 2023 | Encyclopedia | Netherlands |
| YouTube | VLOP | C(2023) 2725 final | 25 April 2023 | Social media | Ireland |
| Zalando | VLOP | C(2023) 2727 final | 25 April 2023 | Marketplace | Germany |
| Pornhub | VLOP | C(2023) 8842 final | 20 December 2023 | Adult content | Cyprus |
| Stripchat | VLOP | C(2023) 8844 final | 20 December 2023 – 27 May 2025 | Adult content | Cyprus |
| XVideos | VLOP | C(2023) 8850 final | 20 December 2023 | Adult content | Czech Republic |
| Xnxx | VLOP | C(2024) 4936 final | 26 April 2024 | Adult content | Czech Republic |
| Temu | VLOP | C(2024) 3757 final | 26 April 2024 | Marketplace | Ireland |
| Shein | VLOP | C(2024) 2842 final | 26 April 2024 | Marketplace | Ireland |

Four out of the 25 designations are subject to court proceedings. These are the designations of Amazon Store (T-367/23**)**, Zalando (T-348/23),[13] Stripchat (T-134/24), and Pornhub (T-138/24). At the moment of publication of this document, the General Court has adjudicated that the application brought about by Zalando in Case T-348/23 was unfounded, upholding the Commission's decision to designate Zalando as a VLOP.

### 2.2. Main conclusions on application of Article 33 DSA

During the first three years of application of the DSA, practice has shown that online platforms and search engines that present systemic reach in the European Union (whose average monthly active recipients are at least 10 % of the population), including those initially taken into consideration in the impact assessment of the DSA proposal and additional ones, have been formally designated as very large online platforms or very large online search engines, and therefore have been captured under the supervision of the European Commission. Until the date of publication of this document, the Commission has adopted decisions designating 23 online platforms and two online search engines as VLOPs and VLOSEs, and one decision terminating the designation of a VLOP.[15]

Additionally, this quantitative threshold has proved effective in drawing a line between the supervision of compliance by the relevant authorities of the Member States (the Digital Services Coordinators) to the

[15] All information regarding the designations and further enforcement actions can be found in https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

Commission, while close cooperation has been essential to ensure an effective application of the DSA and, in particular, of the assessment of potential new designations.

The three alternative data sources at the disposal of the Commission to base its designation decisions pursuant to Article 33(4) of the DSA - data reported by the provider of the online platform or of the online search engine pursuant to Article 24(2), information requested pursuant to Article 24(3) or any other information available to the Commission – allowed the Commission to use relevant information as necessary to assess whether online platforms or search engines reached the threshold on a case by case basis. So far, the Commission has made use of all these three data sources, alternatively, to base the designation decisions listed in table 1 above. In cases where providers had not published a number of average monthly active recipients in the Union above the threshold, the Commission requested information on the methodology that that provider used to calculate that number. Where necessary, the Commission resorted to information provided by third-party data providers that was relevant for these purposes and that was available to the Commission in a timely manner.

In light of the above, and taking into consideration that the growth of the population of the European Union since 2020 has not nearly reached the 5 % referred to in Article 33(2) of the DSA, the present document concludes that the designation process and quantitative threshold determined in Article 33 of the DSA for online platforms and online search engines to be subject to the most stringent DSA obligations has met its original purpose and is well calibrated to capture those services that may cause large societal harms due to their reach. The report, therefore, confirms the adequacy of this threshold.

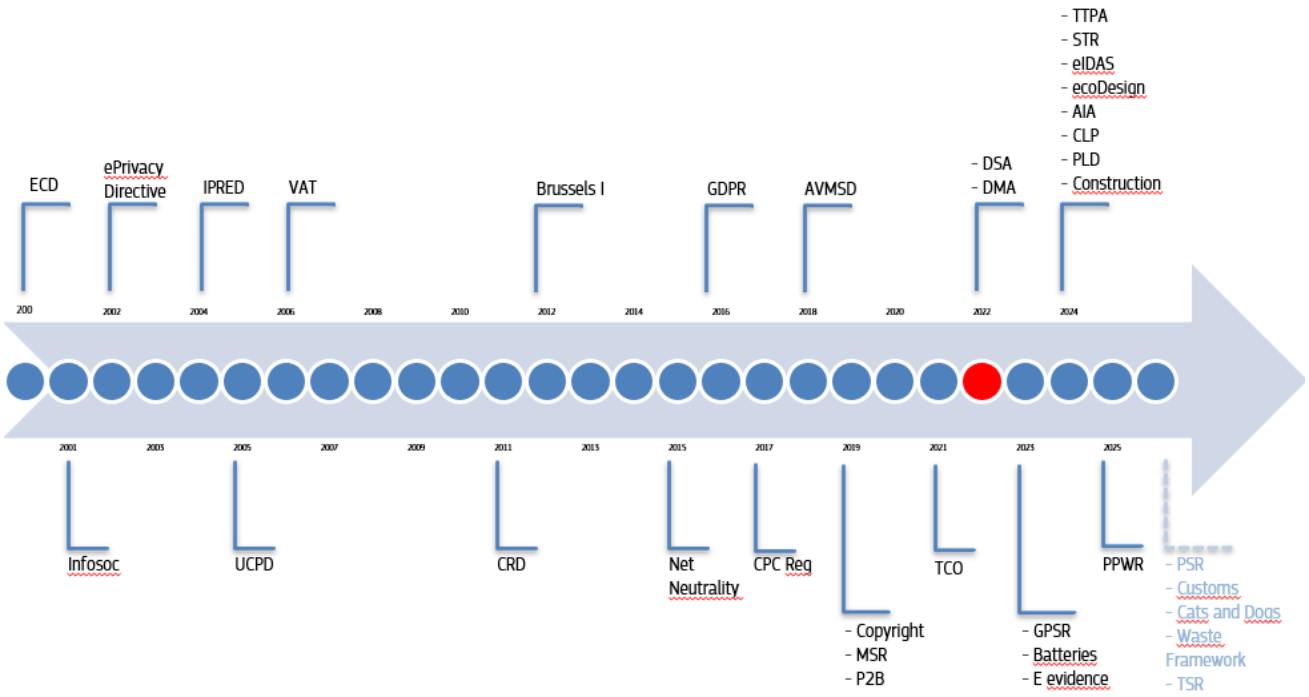
## 3. CHAPTER III: INTERACTION OF THE DIGITAL SERVICES ACT WITH OTHER LEGAL ACTS

### 3.1. Scope

**59 Union law instruments have been identified that interplay with the DSA** (listed in Annex 1 in chronological order) of which five[16] are still under negotiation or in preparation by the College and were therefore excluded from the analysis. Among the remaining 54 Union law instruments are all the legal acts directly referenced in Articles 2(3) and 2(4) DSA. However, the analysis is not limited to the legal acts referred to in those paragraphs – Article 91(2) requests the Commission to report on the way the DSA interacts with other legal acts, in particular (but not exclusively) those listed in Article 2(3) and (4). Indeed, the European Union has adopted a long list of instruments after the date of adoption of the DSA that interact with it in one way or another. Accordingly, this analysis has also taken into account all other Union law instruments that intersect with the DSA, which covers various sectors such as e-commerce and digital markets, product safety, environment, data protection and privacy, consumer protection, audiovisual, media and intellectual property, or democracy, security and justice.

[16] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010; Proposal for a Regulation of the European Parliament and of the Council establishing the Union Customs Code and the European Union Customs Authority, and repealing Regulation (EU) No 952/2013; Proposal for a Regulation of the European Parliament and of the Council on the welfare of dogs and cats and their traceability; Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse; Digital Fairness Act (public consultation and call for evidence opened on 17 July 2025 and closed on 24 October 2025).

*Figure 1: Chronology of the main instruments in scope of the report*




In that regard, two levels of analysis have been performed. On the one hand, Union law instruments that have a strong, direct interplay with the DSA, as they regulate the provision of information society services in general, or introduce sector-specific obligations also applicable to the provision of intermediary services within the internal market, have been subject to a more detailed analysis for each of those instruments (Annex 2). On the other hand, Union law instruments that show a more tangential or less direct interaction with the DSA in terms of scope, obligations, enforcement or practical implications, have been examined in an overarching analysis reflected in the form of a table (Annex 3).

Out of the identified and analysed 54 Union law instruments that, to varying degrees, interact with the DSA, 46 were found to fully complement the DSA, while eight had at least one provision which potentially overlaps with those of the DSA, as it applies to the same actors and the same subject matter as a provision of the DSA. In the majority of cases, the DSA thus interacts in a complementary manner with other Union law instruments, with the DSA often referencing or building upon existing frameworks, serving as a baseline for sectoral rules, or operating in parallel to address related or similar regulatory objectives but with a different scope, focus or audience. As a result, these links are mutually reinforcing and contribute to a coherent, comprehensive, and integrated regulatory framework for digital services in the EU.

This is consistent with Article 2(4) DSA, which provides that the DSA is without prejudice to other Union legal acts insofar as they regulate other aspects of intermediary services in the internal market or specify and complement the DSA. Accordingly, the DSA should not incidentally or unintentionally amend those acts, but it nevertheless applies to matters not covered or not fully addressed by them, as well as to areas where they allow Member States to adopt measures at national level (see Recital 10 DSA).

In a reduced number of instances, as it will be further analysed in this report, a certain degree of overlap has been identified with regards to the DSA and its relation to sector-specific legislation, requiring careful interpretation to ensure legal clarity and coherent enforcement. It should be noted, however, that these overlaps do not deny the overall complementarity also of these instruments.

To accurately map and analyse the Union law instruments that interact with and potentially overlap with the DSA, a taxonomy categorising the various types of interplay and overlap which could occur between the

provisions of the DSA and other Union law instruments has been developed. All terms used throughout this analysis, including the annexes, should be interpreted in accordance with these definitions.

*Table 2: Taxonomy*

| Taxonomy | Description |
|---|---|
| **Interplay** but no overlap | The provisions of the analysed Union law instrument specify or create additional obligations to the provisions of the DSA, designed to build on or work together with the DSA (or vice versa). Therefore, they are complementary. |
| **Overlap** in the **obligation** | The provisions of the analysed Union law instruments and the DSA overlap in their material and personal scope, meaning they regulate the same subject matter for the same type of actors. These provisions may allow for simultaneous application and are usually compatible. However, in some instances, they may envisage different outcomes where they prescribe actions that might not be fulfilled at the same time, which must be resolved via legal conflict rules. |
| **Overlap** in the **enforcement** | Provisions empowering the European Commission or Member States authorities to enforce obligations in relation to the same or similar types of situations (same obligation covering same type of stakeholder) and the enforcement powers are given to different authorities. |

### 3.2. Interplays

The analysis identified **a wide range of complementary interplays between the material scope of the DSA and that of other Union law instruments**.

The DSA **allows other instruments to 'plug in' to the DSA's horizontal framework**, either by adopting its general principles or by layering out additional sector-specific requirements. As a horizontal instrument, the **DSA also refers to existing instruments**, either by simply referencing established frameworks or by providing additional, more prescriptive provisions.

This distribution demonstrates a balanced and multifaceted regulatory landscape, where the DSA both leverages and reinforces existing rules while also serving where appropriate as a foundation for further sectoral adaptation. The following sub-sections explore each of these categories in detail. The aim of this section is to provide an overview of the types of complementary interplays that exist across key themes between the DSA and other instruments (which are presented and analysed in detail in the fiches in Annex 2).

#### *3.2.1. The instrument 'plugs in' to the DSA horizontal framework*

In some cases, the reference to the DSA does not bring new sectoral obligations but rather integrates the DSA's principles and procedures into the sectoral context, for instance by determining what is considered illegal content. The Toy Safety Regulation (TSR) (Article 14) further illustrates this approach, by treating offers for non-compliant toys as illegal content under the DSA, putting them in the scope of the due diligence obligations concerning illegal content, such as the notice and action mechanisms. In a similar manner, the most recent energy labelling delegated acts (adopted after the DSA) incorporate a recital that clarifies that information concerning 'the labelling and marking' referred to in Article 31(2), point (c) of the DSA (compliance by design) should, in the context of energy labelling, be understood as encompassing both the energy label and the product

information sheet[17]. By 'plugging' into the DSA, these instruments leverage its harmonised procedures, risk management obligations, and liability framework, creating a more integrated and effective system for regulating intermediary services and protecting consumers and users across the EU. In other instances, the sectoral instrument empowers judicial or administrative authorities to issue removal or information orders that can in turn give rise to the specific DSA obligations pursuant to its Articles 9 and 10. As an example, the Directive on combating violence against women and domestic violence (VAWDV) obliges Member States to empower national authorities to issue orders to ensure the prompt removal of or disabling of access to publicly accessible material linked to online gender-based violence, while underlining that these orders must meet the requirements in Article 9(2) DSA.

Most often, however, sectoral instruments as part of a broader framework also applicable to the provision of intermediary services, introduce additional, specific requirements, sometimes for the purpose of compliance with the DSA, layering detailed obligations atop the DSA's horizontal framework. This requires important efforts of coordination in the legislative and the enforcement phases, as the obligations set out in the sectoral instrument need to be enforced within the framework established by the DSA.

For instance, in the area of **user interface design and trader information obligations**, instruments such as the Short-Term Rental Regulation (STR) (Article 7) impose stricter requirements for short-term rental platforms, building on Article 31 DSA's general interface design and information duties. Similarly, the Construction Products Regulation (CPR) (Article 28(1)(a)) mandates that online interfaces enable the display of 'CE marking' and digital product passport information for construction products. The same applies to the Explosive Precursors Regulation (EPR), where Article 8(5)) EPR requires online marketplaces to ensure traders meet their obligations to verify prospective customers when making available explosives precursors, a duty that complements Article 31 DSA which provides for compliance by design.

The Batteries Regulation (BR) (Article 62(6) and recital 104) requires platforms to collect additional, battery-specific information from producers. Similarly, the Waste Framework Directive (WFD) (Article 30(1)) and the Packaging and Packaging Waste Regulation (PPWR) (Articles 30(1)-(3)) also expand trader traceability obligations for online platforms, particularly in the context of textiles and packaging. This trend is being extended by the recently adopted TSR and the still to be adopted Regulation on the Welfare of Cats and Dogs.[18]

The GPSR (Articles 22 and 35) exemplifies this layering by specifying concrete deadlines for processing product safety notices (Article 22(8)), mandating registration with the Safety Gate Portal (Articles 22(1), 22(7)), requiring direct consumer notifications (Article 35), and elaborating on information and compliance by design requirements (Articles 22(3), 22(9), 22(11)).These measures go beyond the DSA's general due diligence and notification requirements, topping up the level of consumer protection in the product safety domain.

In the field of **systemic risk management**, the AI Act (Recital 118 and Article 55) interacts with the DSA's framework (Article 34 DSA), to the extent that AI systems or models are embedded into designated VLOPs and VLOSEs, they are therefore subject to the risk-management framework provided for in DSA and, consequently, the corresponding obligations of the AI Act should be presumed to be fulfilled, unless significant systemic risks not covered by DSA emerge and are identified. The DSA risk management framework is equally referred to in the EMFA (Article 18) and in the TTPA (recital 46, without mention in the operative part).

In the area of **illegal content**, the Terrorist Content Online Regulation (TCO) (Articles 3, 4, 9, 11) establishes a dedicated regime for the removal of terrorist content, requiring hosting service providers in the scope of the Regulation to act within one hour of receiving a removal order and to provide specific user notification and redress options, with the DSA's general rules complementing where they cover aspects not addressed or not fully addressed under the TCO.

---

[17] For example, see recital (20) of Commission Delegated Regulation (EU) 2023/2534 with regard to energy labelling of household tumble dryers.

[18] Proposal for a Regulation of the European Parliament and of the Council on the welfare of dogs and cats and their traceability.

In the area of **political advertising transparency and data access**, the TTPA (Articles 11, 12, 13(2), 17, 18, 26(1), 26(3), 28(2), 39, 40(8)) complements, for the provision of intermediary services, the DSA's general rules by introducing enhanced transparency and accountability standards, as well as specific data protection requirements, justified by the impact of this specific category of advertising on core democratic process. This includes *inter alia* more granular transparency requirements, including on the financial aspects of advertising activities, the creation of an EU repository for online political ads, explicit consent standards and additional researcher access rights, ensuring a higher standard of accountability and oversight in the political advertising sphere.

Finally, while Articles 19 and 29 DSA exclude from certain of its obligations those providers of intermediary services which qualify as **small or micro-sized companies**, similar obligations are imposed on those providers in other instruments. For instance, while the DSA excludes providers of online platforms that qualify as micro or small enterprises as defined in Recommendation 2003/361/EC from compliance with the obligation to offer a high level of protection of minors, similarly crafted rules in Article 28b AVMSD apply to small and micro-sized video sharing platforms; Article 7(3) TCO imposes transparency reporting obligations to all online platforms, regardless of their size, therefore including also micro and small enterprises which are exempted from the transparency reporting obligations in the DSA. Similarly, Articles 7 and 8 STR, or Articles 7 and 8 EPR apply some of the provisions applicable to providers of online marketplaces to providers of all sizes. In addition, the transparency requirements with regards to ranking parameters of search results set out in Article 6a of the Consumer Rights Directive (CRD) or Article 7(4a) of the Unfair Commercial Practices Directive (UCPD), and more generally all the traders' obligations under the UCPD and the CRD apply in any business-to-consumer (B2C) relationship, including relationships between online platforms and consumers, regardless of the size of the online platform and thus also to providers which are excluded from similar obligations under the DSA.

### *3.2.2. Specific rules establish a similar obligation but with different scope/focus*

This category captures instances where the identified instrument introduces obligations that share similar objectives with those established in the DSA yet differ in their specific focus or scope. Rather than duplicating or directly building upon existing provisions, the DSA obligations operate in parallel, addressing related but distinct regulatory aspects. This parallelism ensures that the DSA and other instruments collectively contribute to a more holistic and comprehensive regulatory framework, with each set of rules complementing the other.

In the area of **orders to act against illegal content and to provide user information**, Articles 9 and 10 DSA harmonise specific minimum conditions that such orders should fulfil in order to give rise to the complementary obligation of providers of intermediary services to inform the relevant authorities about the effect given to those orders, while the legal basis to issue such orders can be found in other instruments such as the e-evidence Regulation, the Consumer Protection Cooperation Regulation, the IPRED and INFOSOC, while Brussels Ia Regulation provides the procedural framework for jurisdiction, recognition, and enforcement of such orders across Member States.

**Transparency and user rights** are also addressed in parallel by the DSA and other instruments. For example, the DSA requires providers of intermediary services to set up accessible, up-to-date, and user-friendly contact points for authorities and service recipients (Article 11 and 12 DSA), while Article 22(1) and (2) GPSR and Article 28(1)(b) CPR require online marketplaces to establish contact points for product safety or construction product notifications. While these obligations have a similar rationale (and the contact points can be the same in practice), each regime retains its own focus and audience and can apply in parallel.

Transparency is further reinforced by obliging providers of intermediary services to include information on content restriction on their services in their terms and conditions and to publish annual transparency reports under Articles 14 and 15 DSA. These complement similar transparency obligations in other instruments, such

as Article 7 TCO Regulation and the Net Neutrality Regulation's requirements for contractual transparency and reporting on traffic management practices (Article 4).

Other complementary obligations occur as regards **transparency reporting obligations** of the DSA and those of the **TCO**. Article 15 DSA, read together with Articles 24 and 42 DSA where applicable, requires all intermediary services to publish annual transparency reports covering content moderation across all categories of illegal content, including terrorist content. After the adoption of the Implementing Regulation on transparency reporting,[19] online intermediaries need to publish such reports by February each year (and in August for VLOPs and VLOSEs). Article 7(2) TCO instead imposes a specific obligation on hosting services that have taken action to address the dissemination of terrorist content to publish a transparency report by 1 March each year, with detailed information on compliance with TCO removal orders, content moderation measures, number and outcome of complaints and other elements. Therefore, both reports must include information on content moderation measures regarding terrorist content, however according to different formats and on different timelines.

Other examples of parallel obligations include the duty to appoint a **legal representative** in the EU, which appears in Article 13 DSA, Article 3(4) EED, Article 17 TCO, Article 27 GDPR, and Article 21 Transparency and Targeting of Political Advertising Regulation (TTPA). Across these frameworks, the underlying obligation is substantively the same: non-EU providers must ensure an enforceable presence within the Union through a designated representative. However, the objectives of the legislation and scope of responsibilities and required functions differs, while, leaving open the possibility to appoint the same entity as legal representative for the purposes of such frameworks.

Further, the DSA's obligations on **traceability of traders** (Article 30 DSA) complement the requirements on product and manufacturer transparency under the GPSR (Article 22) transparency of hosts under the Short-Term Rental Regulation (STR) (Article 5), and the Digital Product Passport under the Ecodesign Regulation. Each of these focuses on different aspects of traceability, whether of traders, products, or buyers of regulated goods. These regimes may apply in parallel, ensuring both product and trader traceability in online platforms.

Finally, the DSA's requirements for **compliance functions** (Article 41 DSA) and **transparency** in advertising (Article 26 DSA) operate alongside the GDPR's requirements for Data Protection Officers (Article 37 GDPR) and transparency and restrictions on profiling (Articles 13, 14, 15 and 22 GDPR), as well as the Digital Markets Act (DMA, Article 27) transparency obligations for gatekeepers. Given that each of these frameworks has a slightly different scope, audience and set of requirements, together they form a comprehensive and mutually reinforcing approach to digital regulation in the EU.

### *3.2.3. DSA refers back to another legal instrument*

When the DSA refers back to another instrument, it does so in two distinct ways. In a limited number of cases, the DSA simply refers to or relies on existing frameworks without adding further obligations, such as referencing established enforcement procedures, definitions, or mechanisms. For example, Article 30(1)(b) DSA allows providers of online platforms to act as relying parties under the electronic Identification, Authentication and Trust Services Regulation (eIDAS Regulation) and accept eID for the purpose of identifying traders concluding distance contracts with consumers in the EU. Similarly, Article 28(4) DSA, as clarified by Commission guidelines on protection of minors[20], anticipates the use of European Digital Identity (EUDI)

[19] Commission Implementing Regulation (EU) 2024/2835 of 4 November 2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council, *OJ L, 2024/2835, 5.11.2024.*

[20] Communication from the 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/2025/6826.

Wallets for age verification in line with eIDAS, supporting a harmonised approach to age verification across the EU.

However, in the majority of cases, the DSA goes further compared to other pieces of EU law when it comes to online intermediary services, by providing additional or more specific provisions, thus making regulatory requirements more prescriptive and tailored to the digital context. This is particularly evident in the way the DSA builds on and complements the ECD. While the ECD established foundational principles for regulating information society services, the DSA introduces more detailed, harmonised, and prescriptive obligations. Article 12(2) DSA refers back to the ECD's basic transparency requirements (Article 5 ECD) but expands them by requiring intermediaries to designate a single point of contact and make public the information necessary for users to communicate with them. In the area of commercial communications, Article 26 DSA updates and strengthens the ECD's requirements (Article 6 ECD) by mandating real-time ad identification, and Article 39 DSA goes further for VLOPs and VLOSEs by requiring public advertising repositories. Similarly, Article 31(1) DSA builds on Articles 5 and 6 ECD by requiring online marketplaces to design their interfaces to enable traders to comply with pre-contractual information duties, while Article 21 DSA expands on Article 17 ECD by establishing a certification system for out-of-court dispute settlement bodies. Article 45 DSA reinforces the ECD's encouragement of codes of conduct (Article 16 ECD) by providing more specific obligations.

**Transparency and user rights**, in the context of online intermediary services, are further enhanced by the DSA in comparison to other EU legislation. Article 15 DSA introduces mandatory transparency reporting for content moderation. In the area of advertising and recommender systems, Articles 26, 27 and 28(2) DSA apply in addition to Article 5(3) e-Privacy Directive that requires providing clear information and obtaining consent to meet the condition of the GDPR for the use of tracking technologies, as well as the transparency requirements and restrictions on profiling and automated decision-making under Articles 13, 14, 15 and 22 GDPR, while also ensuring VLOPs must provide a recommender system not based on profiling (Article 38 DSA).

The DSA also imposes additional **due diligence obligations** on hosting services, particularly in relation to illegal content, which includes any information which in itself or in relation to an activity, is not in compliance with other Union law instruments. Articles 16, 17 and 20 DSA set out specific obligations for hosting services, including putting in place a notice and action mechanism (Article 16), providing statements of reasons for content removal (Article 17), and providing an internal compliant handling mechanism (Article 20). These requirements ensure that hosting services take a proactive and transparent approach whenever they engage in content moderation. Article 31 DSA introduces a compliance by design obligation, ensuring that online interfaces of online platforms enable traders that use those platforms to meet their information duties set out in Article 6 CRD and Article 7 UCPD.

Collectively, these examples demonstrate how the DSA not only refers to existing Union law instruments but also builds on and strengthens them, ensuring that the regulatory framework remains robust, harmonised and fit for the evolving digital landscape.

#### *3.2.4. Special remarks on certain DSA articles*

The analysis of the material scope interplay between the DSA and other Union law instruments reveals a diverse and dynamic interaction, where some DSA articles can be highlighted as most relevant:

**Articles 4 to 8 DSA**: The DSA lays down fully harmonised rules on the provision of intermediary services in the Internal Market, establishing a framework for the conditional exemption from liability tailored to specific categories of providers of intermediary services ('mere conduit', 'caching' and 'hosting' services), under certain requirements and as interpreted by the Court of Justice in a well-established case law based on the ECD. Besides, the DSA also transfers from the ECD the prohibition of general monitoring obligations.

Several instruments predating the DSA cross-referred to the liability exemptions and prohibition of general monitoring obligations under the ECD (for instance, GDPR, AVMSD, TCO, EPR, CDSMD, IPRED). After the adoption of the DSA, the references to these liability exemptions and the prohibition of general monitoring

obligations are construed as referring to the respective provisions under the DSA and have continued to set a standard in other instruments, such as the STR Regulation, AI Act or the TTPA.

**Article 9 DSA** stands out as the most interconnected provision with other legal instruments. Its procedures for handling removal orders are routinely adopted or referenced by sectoral instruments such as the CPR, ESPR, or VAWDV. This may indicate a trend towards procedural harmonisation, where Article 9 sets out the minimum requirements for orders to act against illegal content.

**Article 16 DSA** also features prominently in relation to notice and action mechanisms for illegal content. Instruments such as the TTPA, CDSMD, GPSR and CPR frequently reference or build upon the notice and action mechanism of Article 16, either by adopting its horizontal procedures or by introducing sector-specific requirements such as stricter deadlines for product safety notices under the GPSR.

**Article 26 DSA** is a key provision for advertising transparency, requiring online platforms to clearly identify advertisements, provide accessible information on ad targeting parameters, and prohibits presenting advertisements based on profiling using special categories of personal data as defined in the GDPR. This article interacts with provisions in the UCPD, ECD, GDPR and E-privacy Directive, which set general standards for advertising and data protection requirements that must also be complied with by the advertising sector which the DSA complements with more operational and specific requirements. The TTPA provides further layers on stricter, sector-specific transparency and targeting requirements for political advertising. This example illustrates again the nuanced interactions between Union law instruments.

**Articles 30 to 32 DSA** illustrate the DSA's role in elevating standards for transparency, traceability, and compliance in online platforms allowing consumers to conclude distance contracts with traders, such as in particular online marketplaces. Traceability requirements under Article 30, compliance by design under Article 31 and right to information under Article 32 are frequently referenced by new sectoral instruments like the BR, STR Regulation, and GPSR, in order to increase accountability, whilst the DSA sets a high baseline that sectoral rules can build upon to address particular risks or market characteristics.

### 3.3. Potential overlaps

Beyond the areas where the DSA operates in a complementary manner with other Union law, there are instances in which some of its provisions might overlap with those of existing instruments.

The sections below present the main findings of this analysis, organising them thematically to illustrate the salient areas of overlap across the regulatory landscape:

- Transparency obligations of recommender systems and transparency reporting obligations
- Manipulative and deceptive practices
- Complaint handling and user redress
- Statement of reasons
- Protection of minors
- Notice-and-action, reporting and feedback
- Compliance by design
- Enforcement

#### *3.3.1. Transparency obligations of recommender systems and transparency reporting obligations*

Transparency obligations are one of the main areas of potential overlaps between the DSA and the identified legislation. The DSA establishes horizontal requirements in Article 14 (terms and conditions) and Article 27 (recommender system transparency). Furthermore, transparency reports are imposed on the basis of the

cumulated effect of Articles 15, 24 and 42 DSA. Sectoral and consumer protection instruments impose similar duties, but with different personal scopes and formats.

The **P2B Regulation** requires online intermediary services to explain restriction, suspension and termination grounds and ranking parameters (Articles 4 and 5), and to provide notice for amendments in terms and conditions (Article 3(2)). These obligations overlap substantially with Articles 14 and 27 DSA but are more detailed in relation to business users (B2B). P2B should therefore be regarded as *lex specialis* in B2B contexts, while the DSA remains applicable more generally.

The **CRD** (Article 6(1)(a)) applicable to online marketplaces, and the **UCPD** (Article 7(4a)) applicable to comparison tools (excluding search engines, to the extent that they are covered by the P2B requirements regarding ranking transparency), require disclosure of ranking parameters in a dedicated section of the online interface. This adds to the DSA's requirement for online platforms (Article 27) requiring the same information to be disclosed in the terms and conditions. There is accordingly an overlap of information obligations for online marketplaces in this case. Insofar as Article 27 DSA provides a more specific obligation than these instruments and there is a conflict between them, the DSA prevails. However, where there is no conflict, both overlapping obligations can remain applicable.

The duplication increases compliance burdens by requiring providers to disclose similar information multiple times in different formats and locations.

### *3.3.2. Manipulative and deceptive practices*

The prohibition of manipulative or deceptive design, often referred to as 'dark patterns', is addressed across several legal frameworks. These rules share the same objective but differ in scope and enforcement, resulting in duplication without contradiction.

The DSA expressly prohibits manipulative or deceptive design of online interfaces (Article 25), supplemented by the obligation to ensure a high level of protection for minors (Article 28).

The **UCPD** prohibits misleading actions and omissions (Articles 6–7) and aggressive practices (Article 8), with a blacklist of specific prohibited commercial practices (Annex I). The UCPD blacklist captures several practices that can be regarded as dark patterns (e.g. false scarcity claims) whilst other behaviours that are commonly regarded as dark patterns can be addressed under the general UCPD rules as misleading or aggressive practices when they affect consumers' transactional decisions, subject to case-by-case assessment. As the UCPD is limited to B2C contexts, while the DSA applies more broadly, the relationship is complementary. In practice, the UCPD acts as *lex specialis* over the DSA in regard to manipulative design practices, while Article 25 DSA applies to manipulative designs not addressed by the UCPD (or the GDPR).

The **AI Act** prohibits the placing on the market or use of AI systems that deploy manipulative or exploitative techniques (Article 5(1)(a) and (b)). These obligations overlap with Article 25 DSA where online platforms deploy AI-based systems for personalised recommendations or interface design. The AI Act applies in this case to the placing on the market and design stage, while the DSA governs the use of AI systems in platform environments. The instruments therefore apply in parallel and cumulatively, with different regulatory touchpoints.

### *3.3.3. Complaint handling mechanism and user redress*

Obligations relating to complaint handling mechanism and user redress are another area of potential overlaps between the DSA and sector-specific instruments. While the substantive objectives are aligned – aiming at access to effective remedies - the frameworks sometimes impose parallel mechanisms that apply simultaneously, which could lead to procedural duplication.

The DSA establishes a multi-layered framework. Article 20 requires online platforms to provide an internal complaint-handling system for users affected by restriction, suspension or termination decisions. Article 17 further requires a statement of reasons for such measures, while Article 21 introduces the possibility of out-of-court dispute settlement. Finally, Article 53 grants recipients of intermediary services the right to lodge complaints with the Digital Services Coordinator of the Member State of establishment.

The **P2B Regulation** imposes comparable duties. Article 11 requires providers of online intermediary services to maintain an accessible and free internal complaint-handling system, while Articles 12 and 13 require engagement in mediation and transparency regarding mediators. Article 11(4) also requires providers to publish annual statistics on complaints. These provisions mirror the internal and external complaint-handling architecture of the DSA but apply specifically in B2B relationships. In practice, the P2B is to be regarded as *lex specialis* in relation to the DSA, given its more detailed regulation of the platform-to-business user relationship. Nevertheless, both instruments remain applicable, obliging providers that fall under both regimes to operate two overlapping complaint-handling processes.

The **TTPA** introduces a dedicated complaint mechanism for political advertising. Article 24 provides for the right to notify suspected infringements and obliges competent authorities to act upon them, with heightened urgency in the context of electoral periods. Where political advertising is disseminated via intermediary services, the same conduct may simultaneously fall within the scope of the DSA right to lodge a complaint (Article 53 DSA) and, if moderation decisions are involved, the internal complaint-handling system under Article 20 and out-of-court settlement under Article 21 DSA. The TTPA does not displace the DSA but applies in parallel, leading to a duplication of remedy avenues.

Complaints concerning consumer law breaches are generally addressed by national consumer authorities, including through the CPC network. In these cases, the DSA applies without prejudice to consumer protection law (Article 2(4) DSA), meaning that complaints may be processed under both regimes, albeit by different authorities.

On its part, the **AVMSD** (Article 28b(3)(i)) mandates video-sharing platforms to establish and operate transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints in relation to implementation of certain measures to protect minors and the general public, whereas the DSA (Article 20) provides stricter obligations for video-sharing platforms' (VSP) internal complaint-handling systems (free, electronic, with "human in the loop"). Here, the AVMSD remains relevant and applies to audiovisual-specific elements not covered in the DSA (e.g. content rating or providing for parental control systems).

Under the **CDSMD**, online content-sharing service providers must put in place an effective and expeditious complaint and redress mechanism, which must fulfil similar requirements as under Article 20 DSA in terms of effectiveness, timeliness and human review. Article 20 DSA however provides further details not regulated under the CDSM, by requiring that the complaint mechanism must be provided free-of charge, user friendly and for a minimum period of six months after the content moderation measure. Therefore, Article 20 DSA operates as a complementary layer that refines and operationalises the redress rights established under Article 17 CDSM, providing clearer procedural safeguards and broader applicability in content moderation contexts.

Taken together, the DSA (Articles 17, 20, 21, 53), P2B (Articles 11 to 13), TTPA (Article 24), the AVSMD (Article 28b) and the CDSM (Article 17(9)) each provide structured complaint-handling and redress mechanisms. The P2B should be considered *lex specialis* for B2B relationships, while the TTPA applies in parallel in the context of political advertising and the AVMSD applies to audiovisual-specific elements not covered in the DSA, therefore VSPs must integrate their reporting and feedback systems to comply with both the AVMSD and DSA. Although substantively aligned, these duplications may result in administrative inefficiencies, fragmented oversight, and potential uncertainty for users and businesses as to the appropriate redress mechanism.

#### *3.3.4. Statement of reasons*

The DSA establishes a general obligation for providers of hosting services to issue a statement of reasons whenever they restrict or disable access to content (Article 17). This includes a requirement to specify the factual and legal grounds, the role of automated means, and available redress mechanisms.

Comparable obligations exist under sectoral legislation. The **P2B Regulation** requires online intermediary services to provide business users with clear reasons for suspension or termination of services (Article 4). While narrower in scope, the P2B regime substantially overlaps with Article 17 DSA, but in B2B relations, should be regarded as *lex specialis*. Providers are nonetheless required to comply with both frameworks.

The **TTPA** introduces only a specific notification duty. Under Article 15(9), political advertising publishers must inform sponsors or service providers when measures are taken against political advertisements. Where the political advertising publisher is a provider of hosting services and political advertisement is deemed unlawful under the TTPA, it may also qualify as "illegal content" under Article 3(h) DSA, triggering Article 17. In such cases, both instruments apply in parallel.

Moreover, according to Article 11 **TCO**, when a hosting service provider removes or disables access to terrorist content, it must inform the content provider of these measures and, upon request, provide information on the reasons for the removal or disabling as well as the available remedies. Where "terrorist content" also qualifies as "illegal content" under the DSA, this obligation potentially overlaps with Article 17 DSA. Both obligations therefore apply simultaneously, with the requirements for a statement of reasons issued in accordance with Article 17 DSA however being more detailed and therefore operating as a complementary layer that refines and operationalises the statement of reasons required under Article 11 TCO.

Finally, the **AVMSD** requires mechanisms for feedback to users regarding illegal and harmful content, while the DSA provides more detailed rules on statement of reasons (Articles 16 and 17), enhancing accountability of online intermediary services providers. The AVMSD remains relevant and applies for the reporting, flagging and similar obligations related to harmful content. As regards feedback mechanisms on statement of reasons, the more detailed DSA's rules on these matters should prevail to the AVMSD.

#### *3.3.5. Protection of minors*

Both the DSA (Article 28) and the **AVMSD** (Articles 6a and 28b (1)-(3)) require online intermediaries to implement measures to protect minors. The DSA frames this obligation in broad terms, requiring platforms to ensure a high level of privacy, safety, and security for minors across all services. By contrast, the AVMSD focuses specifically on video-sharing platforms and audiovisual content, obliging them to protect minors from content likely to impair their development.

Although these obligations share the same protective objective, their application is inconsistent. For example, a platform that is both an online platform under the DSA and a video-sharing platform under the AVMSD must simultaneously comply with the general duty to safeguard minors and with the sector-specific rules governing audiovisual content. For VLOPs, this layering is further compounded by the systemic risk assessment and obligations in Articles 34 and 35 DSA, which include risks to children's rights. The result is not a direct contradiction but a fragmented regime, with overlapping standards and authorities.

#### *3.3.6. Notice-and-action, reporting and feedback*

The DSA (Articles 16, 17 and 20) lays down detailed rules for notice-and-action procedures, statements of reasons, and internal complaint-handling. These obligations are harmonised and apply horizontally to all hosting service providers. The AVMSD, on its part, requires VSPs to establish reporting and feedback mechanisms covering not only illegal content but also harmful – yet legal – content. This broader material scope differs from the DSA, which is limited to illegal content as regards Article 16 (notice and action), but not Articles 17 nor 20 that encompass both illegal content or content incompatible with the terms and conditions.

Similarly, the CDSMD (Article 17(4)) sets out a copyright-specific notice-and-action regime, including obligations regarding notice-and-takedown as well as notice-and-stay-down. The coexistence of these systems may result in complexity with practical consequences for how the concerned online intermediaries can and should design their notice and action mechanism in light of the applicable frameworks: one under the DSA for illegal content, another under AVMSD for illegal or harmful audiovisual content, and another under the CDSMD for copyright-protected works.

### *3.3.7. Compliance by design*

The DSA (Article 31) obliges online platforms allowing consumers to conclude distance contracts with traders to ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information.

Other instruments, as for instance six energy labelling delegated acts adopted in 2019 (and therefore prior to the DSA) set out similar information and compliance by design obligations for hosting service providers that allow the direct selling of the concerned products through their internet website, requiring the service provider to enable the showing of the electronic label and electronic product information sheet on the display mechanism in accordance with the provisions of the delegated acts, and to inform the trader of the obligation to display them.[21]

[21] See for example Article 5 of Commission Delegated Regulation (EU) 2019/2016 with regards to energy labelling of refrigerating appliances.

*3.3.8. Enforcement*

The DSA (Articles 56 and 65) foresees a multi-layered enforcement framework, entrusting national Digital Services Coordinators and conferring special powers on the Commission in respect of VLOPs and VLOSEs, while each one of the other analysed pieces of Union law may diverge from this configuration. For instance, the CRD (Article 23(2)) provides for enforcement by national consumer protection authorities.

Where the same conduct triggers obligations under several frameworks, this creates parallel supervisory tracks. Following the previous example, an online marketplace's recommender system is subject to transparency rules under the DSA and its search result ranking is regulated under the CRD, each potentially enforced by different competent authorities. In the case of VLOPs, enforcement by the Commission under the DSA may coincide with simultaneous enforcement by national authorities under consumer law. This does not generate a direct conflict of law, but creates challenges where diverse enforcement frameworks intersect, therefore requiring close coordination between authorities.

Finally, for instance, product-related legislation is traditionally enforced in the country where the consumer resides ("country of destination" principle). The DSA on the other hand applies the country-of-origin principle, with Commission competence for supervision of and enforcement vis-à-vis VLOPs and VLOSEs. Services-related legislation also follows a country-of-origin principle, but regulators or competent authorities appointed may be different bodies than the Digital Services Coordinators appointed under the DSA. This creates a need for coordination between parallel enforcement proceedings responding to the infringement of intermediary obligations under different legal instruments and enforcement frameworks that are triggered by the same conduct by the intermediary.

*3.3.9. Overlaps with national laws*

On some occasions, overlaps do not necessarily appear at European level, but by way of introduction of additional obligations in national laws. Directives, for instance, traditionally leave to Member States a relative margin of manoeuvre as to the legal means to achieve those objectives, and in some instances allow Member States to impose more detailed or stricter measures.

In this regard, the DSA legislators took notice of the evidence of legal fragmentation and differentiated application of the existing rules by Member States, and ultimately by national courts, as well as of the increased tendency to adopt national legislation with extraterritorial effects, undermining the well-functioning of the internal market.

Accordingly, the DSA fully harmonises the rules applicable to intermediary services in the internal market in accordance with the objectives set out in its recital 9. Therefore, Member States should not adopt or maintain additional national requirements relating to the matters falling within the scope of the DSA, since this would affect the direct and uniform application of those fully harmonised rules. Besides, where the provisions of national law pursue other legitimate public interest objectives, they still need to comply with Article 3 of Directive 2000/31/EC. In this regard, CJEU rulings C-622/22 and C-376/22 have underscored the impossibility for Member States to impose abstract general obligations on providers of intermediary services. In this context, since the adoption of DSA in 2022, the Commission has received and assessed in light of the DSA approximately 160 draft national laws notified via the Technical Regulation Information System TRIS)[22] pursuant to Directive (EU) 2015/1535 and has reacted to 32 notified laws with either a detailed opinion or comments, or detailed opinions and comments in accordance with that Directive.[23]

In particular, the Commission has issued detailed opinions where it established that, if adopted in the version notified, the national drafts would have been incompatible with the rules laid down in the DSA as they were

[22] Prevention of technical barriers to trade | TRIS - European Commission.
[23] Data available on 24 October 2025.

considered to duplicate, supplement or contradict the specific provisions of the DSA and its full harmonisation effect. The Commission issued comments where it established that, if adopted in the version notified, the notified draft, although in accordance with EU law, raised issues of interpretation in light of the DSA or called for details of the arrangements for its implementation.[24]

The detailed opinions issued by the Commission pursuant to Article 6(2) of Directive (EU) 2015/1535 often refer to an overlap with the provisions on risk assessment and risk mitigation measures (Articles 34 and 35 of the DSA)[25], followed by incompatibility with the prohibition to introduce general monitoring or active fact-finding obligations (Article 8 DSA)[26] and the provisions on protection of minors (Article 28 DSA))[27]. The Commission, moreover, regularly found that the notified drafts were duplicating, overlapping or contradicting with the provisions of the DSA on terms and conditions (Article 14 DSA))[28], transparency reporting obligations (Articles 15, 24 and 42 DSA))[29], notice and action mechanisms (Article 16 DSA))[30], trusted flaggers (Article 22 DSA))[31] and the provisions applicable to online marketplaces (Chapter III, Section 4 DSA), especially the rules on traceability of traders (Article 30 DSA)).[32]

In addition, in the majority of notified drafts assessed in light of the DSA, the Commission found that the national drafts would overlap with the supervision and enforcement architecture set out in Chapter IV of the DSA, insofar as the supervision and enforcement system under the notified drafts would also apply with regard to service providers outside the jurisdiction of the notifying Member States and to VLOPs in as much as they were covered by the scope of the notified drafts.

Through the comments issued in accordance with Article 5(2) of Directive (EU) 2015/1535, the Commission raised issues of interpretation of provisions of national drafts with regard to the DSA's liability regime (Articles 4 to 6 DSA)[33], prohibition to introduce general monitoring or active fact-finding obligations (Article 8 DSA)[34], provision on orders to act against illegal content (Article 9 DSA)[35] and data access (Article 40 DSA)[36].

Following the issuance of the reactions, the Commission regularly held regulatory dialogues with the notifying Member States, in accordance with Article 6(2) of Directive (EU) 2015/1535, according to which the Member State to which a detailed opinion is addressed is required to inform the Commission of the action it intends to take on such opinion. In some instances, following the dialogue with the Commission, the notifying Member State proposed amendments which the Commission considered satisfactory and therefore resulted in the draft being in compliance with the DSA[37].

---

[24] All the Commission reactions are accessible via the TRIS database, available at the following link, after searching for the specific notification number: Search the database | TRIS - European Commission.
[25] See for instance TRIS 2023/0461/FR, 2023/554/IT, 2023/632/FR, 2023/759/LT, 2024/93/FR, 2024/188/DE, 2024/288/HU, 2024/344/HU, 2024/374/IE, 2024/578/IT, 2024/0598/DE, 2025/22/IT, 2025/336/FR.
[26] E.g. TRIS 2023/461/FR, 2023/554/IT, 2023/759/LT, 2024/93/FR, 2024/188/DE, 2024/288/HU, 2024/374/IE, 2024/0598/DE, 2025/22/IT, 2025/336/FR.
[27] E.g. TRIS 2023/461/FR, 2023/554/IT, 2023/632/FR, 2024/188/DE, 2024/288/HU, 2024/344/HU, 2024/578/IT.
[28] E.g. TRIS 2022/871/IRL, 2023/554/IT, 2023/632/FR.
[29] E.g. TRIS 2022/871/IRL, 2023/554/IT, 2023/632/FR, 2024/578/IT, 2025/209/FR.
[30] E.g. TRIS 2023/461/FR, 2023/632/FR, 2024/2/HU, 2024/344/HU.
[31] E.g. TRIS 2022/871/IRL, 2023/632/FR.
[32] E.g. TRIS 2022/871/IRL, 2024/598/DE, 2025/209/FR, 2025/336/FR.
[33] E.g. TRIS 2023/554/IT.
[34] E.g. TRIS 2023/554/IT.
[35] E.g. TRIS 2023/0461/FR.
[36] E.g. TRIS 2023/759/LT.
[37] E.g. TRIS 2024/598/DE.

In light of the assessment of national draft laws under the TRIS procedure, on some occasions, the Commission was able to analyse and identify the interlinks between the DSA and other EU Acts, such as the AVMSD[38] and the Batteries Regulation[39].

In conclusion, the TRIS notification procedure is of paramount importance to the well-functioning of the internal market. The Commission services remain vigilant on the national draft laws notified pursuant to Directive (EU) 2015/1535 to ensure that online intermediaries are not subject to additional regulatory barriers within the Single Market.

### *3.3.10. Conclusion on overlaps*

As described above, the overlaps between the DSA and sector-specific legislation requires careful interpretation to ensure legal clarity and coherent enforcement.

The analysis reveals that the DSA, based on a very solid complementarity with other pieces of Union law, overlaps with some provisions of a small number of other Union law instruments, mainly focused-on design-based and transparency obligations, highlighting the general call, in Union law, for due diligence obligations by online platforms. While these overlaps largely reflect the DSA's role as a horizontal baseline operating alongside sectoral regimes, they may also create practical challenges in terms of legal interpretation and coherent enforcement.

[38] E.g. 2024/578/IT.
[39] E.g. 2024/598/DE.

# 4. CHAPTER IV: RESULTS FROM THE SURVEY ANALYSIS

Three targeted surveys were conducted as part of this the support document, addressed respectively to civil society organisations (CSOs), Digital Services Coordinators (DSCs) and other relevant authorities, VLOPs and VLOSEs as well as other providers of online intermediary services. The purpose of these surveys was to gather practical insights from a diverse range of stakeholders regarding the application of the DSA in the broader context of the EU digital regulatory framework.

The three surveys were launched by the Commission services and received a total of 97 responses – 20 from CSOs, 56 from DSCs and other authorities, and 21 from VLOPs and other service providers. In addition, one additional VLOP provided some insight in writing (but did not complete the survey)

This chapter provides a comparative analysis of the responses received across all three surveys, grouped into three themes: user awareness and experience; overlaps between the DSA and other instruments; and suggestions for improvements. A detailed analysis, per question, of each survey is presented in Annex 3.

## 4.1. User awareness and experience

Across all three surveys stakeholders reported that most users lacked a clear understanding of which Union laws applied to their online activities. 75% of CSOs reported that users did not know which Union laws were relevant, and while 65% thought users might have heard of these laws, most were unsure of their significance. Only 30% of CSOs considered users to be aware of the DSA, and none believed users were familiar with the specific laws relevant to their own situations. National authorities echoed this assessment: 82% believed users had at least heard of the laws, but only 21% considered users aware of the DSA's protections, and just 5% felt users both knew the laws and understood how they protected them. Over one-third of authorities (38%) believed users did not know which EU rules applied to online intermediaries at all.

**This limited awareness was reported as resulting in practical challenges for both authorities and platforms.** National authorities reported that a significant proportion (21%) "often" or "fairly often" received complaints, reports, or queries for which they were not competent, while nearly half (45%) encountered this "sometimes" and a third (34%) considered that misdirected complaints happened "rarely." Open comments revealed that, from the perspective of the DSCs and other relevant national authorities, users frequently expressed dissatisfaction with enforcement or confusion about which authority was responsible, especially in complex areas such as online marketplaces. It also highlighted that many users were unable to distinguish between the DSA, GDPR, consumer protection laws, and sector-specific regulations, leading to misunderstandings about which authority was competent for their issue. According to these authorities, users also tended to expect a single point of contact for all digital platform-related concerns, further increasing the likelihood of misdirected complaints. Feedback from VLOPs and other platforms reinforced this picture. Civil society organisations reported that user complaints, reports, or queries were most commonly submitted to the wrong department or contact point either "sometimes" or "rarely" (38% each), with smaller shares indicating this occurred "fairly often" (14%) or "often" (10%). Quantitative data highlighted the scale of the issue: one online marketplace reported that in 35–40% of notices, the subject of the violation was incorrect and required rerouting, and 25% of seller-submitted notices were sent to the wrong contact point. Another provider reported 4–10 misdirected complaints per week. Qualitative feedback from platforms also noted that misdirection could result from authorities bypassing official channels and contacting employees or subsidiaries directly, adding complexity and delays to the process.

CSOs further highlighted that users frequently encountered unclear or contradictory information from online platforms and search engines, with 85% reporting this happened often or sometimes. Consistency in the application of EU rules was also seen as lacking, with 65% of CSOs indicating users had experienced inconsistent or unclear outcomes. Only one CSO believed users were fully aware of how to enforce their rights or raise complaints, while the majority felt users needed additional support or were completely unaware of the appropriate channels and authorities. Authorities corroborated these findings, citing unclear or evolving

definitions of intermediary services, national and sectoral differences in authority remits, and users' expectations of immediate intervention or resolution as additional sources of confusion.

**Despite these challenges, some of the respondents reported seeing improvements**. One online marketplace credited the legal clarity introduced by the DSA for enhancing transparency and improving processes for users, leading to a general decrease in the number of user submissions that were incorrectly assigned internally. Some authorities also established processes to redirect complaints and were undertaking efforts to improve public awareness but acknowledged that user understanding remained nascent and would require sustained, long-term educational initiatives.

### 4.2. Potential overlaps

All stakeholder groups recognised that the DSA did not operate in isolation but interacted with a range of existing Union law instruments, often resulting in significant overlaps and, at times, direct conflicts. The scale of this issue was particularly pronounced among VLOPs and platforms, with 71% reporting overlapping provisions and 62% citing conflicting or contradictory rules. Half of the enquired national authorities and 45% of CSOs also reported encountering overlaps.

A central theme across all groups was the intersection between the DSA and the **GDPR**. CSOs, authorities, and platforms all pointed to uncertainty regarding DSA provisions on dark patterns, targeted advertising, and recommender systems. For example, the reuse of user data through recommender systems under Article 27 DSA was perceived as overlapping with GDPR transparency and consent requirements (Articles 6 and 7 GDPR), sometimes leading to perceived overlaps or parallel scrutiny by different authorities.

Another commonly cited area was the overlap between the DSA's prohibition of manipulative interface design and the **UCPD**. Both authorities and platforms noted that the DSA did not clearly distinguish between dark patterns and unfair commercial practices, leaving uncertainty about regulatory leadership and enforcement. CSOs added that the DSA's exclusion of consumer-to-business practices left interpretative gaps that national courts needed to fill.

Authorities and platforms also highlighted the intersection with the **AVMSD**, especially for video-sharing platforms designated as VLOPs under Articles 33–34 DSA, which also fell within AVMSD's scope. This was reported as resulting in overlapping removal and compliance powers for national audiovisual regulators, Digital Services Coordinators, and the Commission.

Platforms and authorities also identified procedural overlaps with the **e-Commerce Directive** (country-of-origin principle and liability exemptions), the **Platform-to-Business Regulation** (transparency and traceability provisions), and the **Consumer Rights Directive** (points of contact and recommender-system transparency). Platforms also provided concrete examples of duplicative requirements, such as DSA Articles 11–12 and Article 31 overlapping with **GPSR** Articles 22(1), 22(2), and 22(9), and DSA Articles 2 and 6 misaligning with **GPSR** Articles 4 and 22 regarding marketplace liability and the duties of economic operators.

Platforms, in particular, highlighted issues with the **Union Customs Code** reform[40] (contradicting DSA Articles 2 and 6 and GPSR's exclusion of marketplaces from the product-safety chain), **Digital Fairness Act, the Audiovisual Media Freedom Act, and the Artificial Intelligence Act** (notably DSA Article 34 vs. AI Act Article 3(65)) or measures that could possibly be included in the forthcoming **Digital Fairness Act**. These instruments were perceived as introducing parallel or inconsistent obligations, especially regarding transparency, reporting, and systemic risk assessment.

**All groups agreed that the cumulative effect of these overlaps was substantial**. Platforms provided quantitative estimates, reporting that 15–20% of IT resources and 5–15% of legal working capacity were currently devoted to implementing new legislation, with expectations that this could rise to 20–30% as DSA

[40] The Customs reform proposal is currently under negotiation.

familiarity increased. Industry sources suggested that up to 30% of EU tech companies' resources might be consumed by compliance due to regulatory complexity. Authorities and CSOs emphasised the confusion and uncertainty this created for users and advocates, who might face dismissed complaints, inconsistent enforcement, or gaps in protection.

### 4.3. Suggestions for improving the digital regulatory framework

A central recommendation across all stakeholder groups was the need for clearer, more accessible guidance and communication from EU institutions and regulators. CSOs, authorities, and platforms alike called for the publication of practical guidelines, FAQs, handbooks, and real-world case studies to clarify how the DSA and other relevant legislation should be applied in practice. For example, 39% of authorities specifically requested more interpretative documents, and platforms echoed this need by emphasising the value of detailed explanatory notes and regular updates. CSOs further suggested joint guidance from bodies such as the European Commission and the European Data Protection Board (EDPB), especially on complex issues like dark patterns and the interplay between the DSA, GDPR, and UCPD. Additionally, CSOs proposed the development of regulatory mapping tools or databases, as well as digital rights dashboards and public EU-wide digital hubs, to help both users and businesses navigate the complex legal landscape.

All groups strongly advocated for greater harmonisation and streamlining of EU digital regulation to reduce unnecessary overlaps and administrative complexity. This was the top priority for VLOPs and platforms, with 76% identifying the need for fewer overlaps between different rules, and 57% calling for clearer indications on the applicability of EU rules to concrete situations. CSOs and authorities similarly emphasised the importance of clearer identification of the competent authority and more explicit guidance on which legislation applied in specific scenarios. Authorities also highlighted the need to harmonise definitions across legal instruments (18%), noting that references such as "without prejudice to the GDPR" did not resolve practical conflicts or overlaps. Platforms, in particular, warned against regulatory overreach and called for outcome-oriented, practical rules that were mindful of the cumulative burden on businesses.

**Improved coordination and cooperation among regulatory authorities was also a recurring theme**. Over a third (38%) of platforms stressed the importance of exchanges and cooperation between national competent authorities, while 30% of authorities advocated for formal cooperation frameworks, joint interpretation efforts, and harmonised methodologies to ensure consistency in enforcement and avoid duplication or gaps. CSOs also saw enhanced coordination, both at the EU and national levels, as essential for effective enforcement and information sharing, particularly in cross-border or overlapping cases. Platforms specifically recommended a "one-stop shop" approach for cross-border services to streamline compliance and reduce the risk of inconsistent enforcement.

**All groups also highlighted the need for clearer delineation of roles and competences among regulatory bodies**. CSOs called for clearer identification of the competent authority, and 20% of authorities requested the establishment of central contact points and mapping of responsibilities to make it easier for users and authorities to identify the correct point of contact. Platforms also identified this as a priority (19%), recognising that clarity in regulatory responsibilities was essential for both compliance and user support.

Platforms and authorities emphasised the importance of flexibility and proportionality in the regulatory framework, calling for rules that were adaptable to the size, nature, and business model of different online intermediary services. Platforms stressed that the framework should be responsive to technological and market developments, and authorities noted the importance of taking into account the needs of specific sectors such as agri-food, education, and media. CSOs, meanwhile, urged special attention for children and vulnerable users, including making reporting tools more accessible and allowing representatives to bring cases on their behalf.

There was a shared recognition of the value of ongoing dialogue and engagement between regulators, service providers, and stakeholders. Platforms, in particular, stressed the importance of regular exchanges to ensure that the regulatory framework remained relevant and effective in a rapidly changing digital landscape. Authorities

and CSOs also supported the sharing of best practices and case law to support consistent interpretation and application of the rules.

CSOs offered several other recommendations, such as improved communication for users (including age-appropriate information), effective enforcement of sanctions, adequate resources for Trusted Flaggers, and standardised criteria for determining when services fell under multiple regulatory frameworks. Authorities highlighted the need for strengthening cross-border enforcement and clarifying the operation of notice mechanisms. Platforms emphasised the importance of practical, outcome-oriented rules and warned of the resource and innovation costs associated with regulatory complexity.

## 5. CHAPTER V: CONCLUSIONS

From the assessment carried out, the Commission services conclude that the existing categorisation of online intermediary services is future proof and therefore capable to grasp the rapid evolution of digital services and its underlying technologies, being able to capture the latest features, such as generative AI solutions.

Nonetheless, this statement does not preclude a possible revision of such categorization for the upcoming second DSA report, pursuant to Article 91(2) DSA and due by 17 November 2027.

Besides, the Commission services also concludes that the threshold of 45 million average monthly active recipients of the service is appropriate to cover those online platforms and search engines, which due to their role in facilitating public debate, economic transactions and the dissemination to the public are of particular importance and should therefore be subject to the most stringent DSA obligations. Given the experience gathered so far, the number is suitable and fit-for-purpose to address the societal risks characteristic for such services, which are different in scope and impact from those caused by smaller platforms.

On the other hand, the Commission services concludes that the DSA is, overall, highly complementary to other Union law instruments, which clearly reflects is horizontal fully-harmonised nature and rules applicable to online intermediary services providers, such as online platforms.

In the vast majority of cases, the DSA and other Union law instruments interplay in ways that are mutually reinforcing, with provisions designed to either build on one another or apply in parallel. Sector-specific legislation "plugs-in" to the DSA, serving as a horizontal baseline for sectoral rules, or establishes parallel obligations that pursue similar objectives with a different scope or focus. Such interplay ensures a balanced and multifaceted regulatory landscape, where the DSA leverages and reinforces existing rules, thus ensuring regulatory consistency across the Union law acquis.

The DSA's role as a harmonised baseline is further reinforced by the fact that many recently adopted or revised Union law instruments explicitly refer to the DSA, incorporating its principles and procedures into their own frameworks, ensuring legal certainty and avoiding duplication.

Similarly, the DSA itself is rich in references to other Union law instruments, most notably, Article 2(4) clarifies 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 this Regulation," followed by an explicit, non-exhaustive list of key legal acts. This "without prejudice" provision is fundamental, as it ensures that the DSA does not override or diminish the application of sectoral or horizontal rules in these areas. However, it is important to recognize that Article 2(4) DSA does not mean that the EU legal acts referenced in the list automatically are carved out from the DSA. Rather, the DSA remains a maximum harmonisation instrument that only gives precedence to provisions in other instruments that regulate *other* aspects of the provision of intermediary services (i.e., aspects not already harmonized by the DSA), or that provide *additional* or *complementary* obligations.

Despite this overall complementarity, the analysis also identified a limited number of potentially overlapping provisions between the DSA and other Union law instruments, resulting in cumulative obligations, regarding, among others, transparency obligations and recommender systems, manipulative and deceptive practices ("dark patterns"), complaint handling mechanisms and user redress, or and statement of reasons. In most cases, these overlaps do not seem to create a substantive conflict but rather entail the simultaneous application of both provisions. Nevertheless, they may be perceived as increasing compliance burdens and give rise to practical challenges in terms of legal interpretation and coherent enforcement.

On top of that, the legislative pace needs also to be taken into consideration. Since DSA was adopted and during the last Commission mandate, further relevant Union acts have been adopted, which interact with the DSA, and more are being negotiated or are under preparation.

## ANNEX 1: LIST OF INSTRUMENTS ANALYSED (BY CHRONOLOGICAL ORDER)

| Adoption date | Number | Full official name (short title) |
|---|---|---|
| **15 Apr 1993** | 93/13/EEC | Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (EUR-Lex) |
| **8 Jun 2000** | 2000/31/EC | Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive). (EUR-Lex) |
| **22 May 2001** | 2001/29/EC | Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive). (EUR-Lex) |
| **12 Jul 2002** | 2002/58/EC | Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). (EUR-Lex) |
| **11 Feb 2004** | 273/2004 | Regulation (EC) No 273/2004 on drug precursors. (EUR-Lex) |
| **31 Mar 2004** | 648/2004 | Regulation (EC) No 648/2004 of the European Parliament and of the Council of 31 March 2004 on detergents (EUR-Lex) |
| **29 Apr 2004** | 2004/48/EC | Directive 2004/48/EC on the enforcement of intellectual property rights. (EUR-Lex) |
| **11 May 2005** | 2005/29/EC | Directive 2005/29/EC concerning unfair business-to-consumer commercial practices (Unfair Commercial Practices Directive) (EUR-Lex) ) |
| **11 Jul 2007** | 864/2007 | Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (EUR-Lex) |
| **17 Jun 2008** | 593/2008 | Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (EUR-Lex) |
| **16 Dec 2008** | 1272/2008 | Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures (CLP). (EUR-Lex) |
| **10 Mar 2010** | 2010/13 | Directive (EU) 2010/13/EU on audiovisual media services (Audiovisual Media Services Directive). (EUR-Lex) |

| | | |
|---|---|---|
| **9 Mar 2011** | 305/2011 | Regulation (EU) No 305/2011 laying down harmonised conditions for the marketing of construction products (Construction Products Regulation). (EUR-Lex) |
| **25 Oct 2011** | 2011/83/EU | Directive 2011/83/EU on consumer rights (Consumer Rights Directive). (EUR-Lex) |
| **12 Dec 2012** | 1215/2012 | Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels Ia Regulation). (EUR-Lex) |
| **21 May 2013** | 2013/11/EU | Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (Alternative Dispute Resolution Directive) (EUR-Lex) |
| **25 Nov 2015** | 2015/2120 | Regulation (EU) 2015/2120 laying down measures concerning open internet access (Net Neutrality / Open Internet Regulation). (EUR-Lex) |
| **27 Apr 2016** | 2016/679 | Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation — GDPR). (EUR-Lex) |
| **8 Jun 2016** | 2016/943 | Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (EUR-Lex) |
| **4 July 2017** | 2017/1369 | Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (EUR-lex) and its delegated acts |
| **12 Dec 2017** | 2017/2394 | Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws (CPC Regulation). (EUR-Lex) |
| **11 Dec 2018** | 2018/1972 | Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (EECC) (EUR-Lex) |
| **17 Apr 2019** | 2019/790 | Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market (DSM Copyright Directive). (EUR-Lex) |
| **20 Jun 2019** | 2019/1020 | Regulation (EU) 2019/1020 on market surveillance and compliance of products (Market Surveillance Regulation — MSR). (EUR-Lex) |
| **20 Jun 2019** | 2019/1148 | Regulation (EU) 2019/1148 on the marketing and use of explosives precursors. (EUR-Lex) |

| | | |
|---|---|---|
| **20 Jun 2019** | 2019/1150 | Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (Platform-to-Business Regulation). (EUR-Lex) |
| **25 May 2020** | 2020/740 | Regulation (EU) 2020/740 of the European Parliament and of the Council of 25 May 2020 on the labelling of tyres with respect to fuel efficiency and other parameters, amending Regulation (EU) 2017/1369 and repealing Regulation (EC) No 1222/2009 (EUR-Lex) |
| **29 Apr 2021** | 2021/784 | Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. (EUR-Lex) |
| **30 May 2022** | 2022/868 | Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (EUR-Lex) |
| **14 Sep 2022** | 2022/1925 | Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act — DMA). (EUR-Lex) |
| **14 Dec 2022** | 2022/2555 | Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) (EUR-Lex) |
| **10 May 2023** | 2023/988 | Regulation (EU) 2023/988 on general product safety (General Product Safety Regulation — GPSR). (EUR-Lex) |
| **31 May 2023** | 2023/1115 | Regulation (EU) 2023/1115 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation. (EUR-Lex) |
| **12 Jul 2023** | 2023/1542 | Regulation (EU) 2023/1542 concerning batteries and waste batteries (Batteries Regulation). (EUR-Lex) |
| **12 Jul 2023** | 2023/1543 | Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence (e-evidence Regulation — EPOR). (EUR-Lex) |
| **12 Jul 2023** | 2023/1544 | Directive (EU) 2023/1544 laying down harmonised rules on the designation of legal representatives for the purpose of gathering electronic evidence (e-evidence Directive — EED). (EUR-Lex) |
| **18 Oct 2023** | 2023/2411 | Regulation (EU) 2023/2411 of the European Parliament and of the Council of 18 October 2023 on the protection of geographical indications for craft and industrial products (EUR-Lex) |

| | | |
|---|---|---|
| **13 Dec 2023** | 2023/2854 | Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) (EUR-Lex) |
| **7 Feb 2024** | 2024/573 | Regulation (EU) 2024/573 of the European Parliament and of the Council of 7 February 2024 on fluorinated greenhouse gases (EUR-Lex) |
| **13 Mar 2024** | 2024/900 | Regulation (EU) 2024/900 on the transparency and targeting of political advertising. (EUR-Lex) |
| **11 Apr 2024** | 2024/1028 | Regulation (EU) 2024/1028 on data collection and sharing relating to short-term accommodation rental services (Short-Term Rental Regulation). (EUR-Lex) |
| **11 Apr 2024** | 2024/1183 | Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing a European Digital Identity framework (European Digital Identity Regulation / eIDAS-2). (EUR-Lex) |
| **11 Apr 2024** | 2024/1083 | Regulation (EU) 2024/1083 of 11 April 2024 establishing a common framework for media services in the internal market (European Media Freedom Act) (EUR-Lex) |
| **11 Apr 2024** | 2024/1143 | Regulation (EU) 2024/1143 of the European Parliament and of the Council of 11 April 2024 on geographical indications for wine, spirit drinks and agricultural products, as well as traditional specialities guaranteed and optional quality terms for agricultural products (EUR-Lex) |
| **14 May 2024** | 2024/1385 | Directive (EU) 2024/1385 on combating violence against women and domestic violence. (EUR-Lex) |
| **13 Jun 2024** | 2024/1781 | Regulation (EU) 2024/1781 establishing a framework for the setting of ecodesign requirements for sustainable products (Ecodesign for Sustainable Products Regulation — ESPR). (EUR-Lex) |
| **7 Feb 2024** | 2024/590 | Regulation (EU) 2024/590 of the European Parliament and of the Council of 7 February 2024 on substances that deplete the ozone layer (EUR-Lex) |
| **18 Jul 2024** | 2024/1689 | Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (EUR-Lex) |
| **23 Oct 2024** | 2024/2865 | Regulation (EU) 2024/2865 of the European Parliament and of the Council of 23 October 2024 amending Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures (EUR-Lex) |
| **18 Nov 2024** | 2024/2853 | Directive (EU) 2024/2853 on liability for defective products (Product Liability Directive — PLD). (EUR-Lex) |

| | | |
|---|---|---|
| **27 Nov 2024** | 2024/3015 | Regulation (EU) 2024/3015 of the European Parliament and of the Council of 27 November 2024 on prohibiting products made with forced labour on the Union market (EUR-Lex) |
| **27 Nov 2024** | 2024/3110 | Regulation (EU) 2024/3110 of the European Parliament and of the Council of 27 November 2024 laying down harmonised rules for the marketing of construction products and repealing Regulation (EU) No 305/2011 (EUR-Lex) |
| **19 Dec 2024** | 2025/40 | Regulation (EU) 2025/40 on packaging and packaging waste (Packaging and Packaging Waste Regulation — PPWR). (Adopted 19 Dec 2024; OJ number 2025/40). (EUR-Lex) |
| **11 Mar 2025** | 2025/516 | Council Directive (EU) 2025/516 of 11 March 2025 amending Directive 2006/112/EC as regards VAT rules for the digital age (EUR-Lex) |
| **10 Sep 2025** | 2025/1892 | Directive (EU) 2025/1892 of the European Parliament and of the Council of 10 September 2025 amending Directive 2008/98/EC on waste (EUR-Lex) |
| **Under negotiation / Pending publication (no adoption date yet)** | | |
| **15 May 2022** | COM(2022) 209 | Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (CSAM Regulation). (EUR-Lex) |
| **28 Jun 2023** | COM(2023) 367 | Proposal for a Regulation on payment services in the internal market (Payment Services Regulation — PSR). (EUR-Lex) |
| **17 May 2023** | COM(2023) 258 | Proposal for a Regulation establishing the EU Customs Code and the European Union Customs Authority (customs reform). (EUR-Lex) |
| **28 Sept 2023** | COM(2023) 462 | Proposal for a Regulation on the safety of toys (Toy Safety Regulation — recast). (EUR-Lex) |
| **7 Dec 2023** | COM(2023) 769 | Proposal for a Regulation on the welfare of cats and dogs and their traceability. (EUR-Lex) |

## ANNEX 2: DETAILED ANALYSIS (BY CHRONOLOGICAL ORDER)

### Directive (EU) 2000/31/EC ([41]) – [E-Commerce Directive]

*General Information*

The E-Commerce Directive (ECD) was adopted on 8 June 2000, with a transposition deadline of January 2002. Over time, the ECD has been complemented by sector-specific and service-specific legislation addressing areas such as data protection, copyright, audiovisual services, and consumer protection. The Court of Justice of the European Union (CJEU) has also played a key role in ensuring a uniform interpretation and application of the ECD's core principles amidst emerging digital services and technologies.

Building on this foundation, the Digital Services Act (DSA), adopted in 2022, updates and broadens the regulatory framework by introducing new obligations and repealing the ECD's provisions on intermediary liability (Articles 12 to 15) (Article 89 DSA). Furthermore, it states that references to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 4, 5, 6 and 8 of this Regulation, respectively. Therefore, any reference in other legislation to Articles 12 to 15 ECD are now a cross-reference to the DSA.

The ECD "seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States" (Article 1(1)). The ECD has been instrumental to build a strong single market for information society services, firmly anchored in its "country of origin principle" established in its Article 3.

*Personal scope*

The ECD regulates information society services (ISS), which are an autonomous concept defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient" in the Technical Standards Directive (see Article 2 lit. ECD in conjunction with Article 1 lit. b Directive (EU) 2015/1535); see also recital 18 ECD for non-exhaustive examples of ISS in the ECD-context.[42] This is a core concept that also lies underneath the DSA, as it covers a sub-category of information society services. In that sense, the jurisprudence of the CJEU interpreting this concept in the context of the ECD is also highly relevant for interpreting the scope of the DSA.[43]

---

[41] 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').

[42] Directive 98/34 of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, OJ [1998] L 204/37 as amended by Directive 98/48, Art. 1(2). This Directive is now replaced by the Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ [2015] L 241/1, Art.1(b).

[43] The CJEU ruled in ECD-related cases C-291/13 *Papasavvas* and C-484/14 *McFadden* in relation to the ECD that ISSs do not have to be paid for by the recipient; they can be free and financed through advertising revenue; in the cases of C434/15 *Uber Spain* and C-320/16 *Uber France*, the Court held that Uber's online intermediation is part of a transport service, so Uber is classified as a transport service provider rather than an ISS provider. This is because Uber controls key aspects like fares, vehicle quality, and safety standards, making the app an accessory to the main transport service. This ruling can be seen at the origin of the wording of recital 6 DSA. Finally, in the C-390/18 *Airbnb Ireland* case, the Court found Airbnb to be an ISS provider because it does not exert decisive control over the hosting services. The online intermediation is the main service offered, distinct from the accommodation itself, and thus qualifies as an ISS.

The ECD applies only to Information Society services established in the Union. It establishes the principle of home-state control (that of the "main establishment in the Union"), while all other Member States should refrain from imposing restrictions to the provision of the services from the home state (cf. Article 3 ECD).[44]

In the *Cornelius de Visser* case (C-292/10), the Court clarified that the internal market clause (Article 3(1) and (2) ECD) does not apply when the provider's place of establishment is unknown, as the clause presupposes the identification of the Member State, where the provider is actually established. Furthermore, Recital 58 (and *Viagogo* case C-70/22) explicitly excludes any extraterritorial application of the ECD, meaning that content originating from Information Society service providers outside the EU targeting EU customers falls outside the Directive's scope.

*Material scope*

The ECD establishes harmonised rules on issues such as transparency and information requirements for information society service providers (Articles 4 to 6); commercial communications (Articles 7 to 8); and electronic contracts (Articles 9 to 10). The provisions on the limitation of liability for intermediary service providers (Articles 12 to 15) have been replaced by new corresponding provisions in the DSA.

*Enforcement*

The ECD does not create a separate competent authority and leaves much to the discretion of the Member States. Cooperation between Member States (Article 19) is limited mainly to designating contact points and sharing information with each other and the Commission. Sanctions are left to the discretion of Member States (Article 20), as long as they are effective, proportionate, and dissuasive.

*Interactions with the DSA*

The ECD does not contain any references to the DSA as it was adopted prior to the DSA. Note however, that according to Art. 89(2) DSA, references to Articles 12 to 15 ECD shall be construed as references to Articles 4, 5, 6 and 8 of the DSA.

Being the "precursor" and the main milestone in the regulation of information society services, the ECD has many and deep interactions with the DSA. The DSA refers to the ECD throughout its preamble, as well as in Articles 2, 3, 12, 89, and 90. The references are intended to highlight the complementarity and interplay between both instruments and highlight that the DSA updates the ECD's liability exemption regime, and does not affect the application of the ECD (Article 2 DSA) with regards to areas such as commercial communications (i.e. advertising) or information requirements.

Regarding **personal scope**, the DSA applies to intermediary services (Article 2(1) DSA) also covered by the ECD, as they by nature constitute information society services:

- The definition of ISS in the DSA contains a cross-reference to Article 1(1)(b) Directive (EU) 2015/1535. That definition was already present in the previously applicable Directive 98/34/EC, as amended by Directive 98/48/EC, and is also identical to the definition laid down in the ECD.

- The notion of an 'intermediary service' DSA is taken from the title of Section 4 of the ECD and the definitions contained in Article 3(g) DSA closely reflect the wording of Articles 12 to 14, which referred to a 'mere conduit' service, a 'caching' service, and a 'hosting' service. In other words, intermediary services in the DSA are only those ISS that provide mere conduit, caching or hosting services. In other words, the

[44]The CJEU's ruling in C-376/22 (*Google Ireland and Others v KommAustria*) reaffirmed the supremacy of this principle, holding that Member States cannot impose general and abstract obligations on providers established in another Member State. Likewise, In Joined Cases C-662/22 (*Airbnb Ireland*) and C-667/22 (*Amazon Services Europe*), the CJEU held that national measures are incompatible with EU law unless they satisfy rigorous conditions under EU obligations.

notion of intermediary services is potentially narrower than the notion ISS (recital 18 ECD provides a non-exhaustive list of ISS in the context of ECD).

- Since its adoption, the provisions of the ECD have also been widely interpreted by the CJEU, in particular as regards the exemption of liability of hosting and mere conduit services and the prohibition of general monitoring obligations; this case-law has been in a way codified in the recitals of the DSA, and remains relevant for the interpretation of Articles 4 to 8 DSA.

On **territorial scope**, the geographical scope of the DSA is broader than that of the ECD as it includes an extraterritorial dimension whereas the ECD does not. The DSA applies to "intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, *irrespective of where the providers of those intermediary services have their place of establishment*" (Article 2 (1) DSA, emphasis added).

Regarding the **material scope**, the DSA builds upon the foundational framework established by the ECD and related CJEU jurisprudence, further detailing and expanding the obligations for intermediary services. The two legislative instruments operate in a complementary and mutually reinforcing manner. The following highlights key areas of interplay between the DSA and the ECD, organised according to relevant DSA articles:

- Article 9 DSA addresses orders issued by national judicial or administrative authorities requiring providers of intermediary services to act against specific illegal content. Recital 38 of the DSA clarifies that such orders do not, in principle, restrict the freedom to provide services, meaning the country-of-origin principle established in Article 3 ECD does not apply in these cases. Consequently, authorities of other Member States than the one in which a provider of intermediary services is established may issue such orders. The recital clarifies that the application of the DSA does not lead to a conflict with the principles of the ECD, and that both these legal acts can be enforced in parallel in these circumstances. Furthermore, the ECD does not harmonise the minimum conditions of injunctions by courts or administrative bodies; it simply recognises that these are possible (Articles 12(3), 13(2) and 14(3) ECD), and indeed necessary (Article 18(1)).

- Article 15(2) ECD allows Member States to impose targeted obligations on service providers, such as informing authorities of suspected illegal activities or disclosing information to identify users, while making clear that general monitoring is prohibited (see also recital 47). Article 10 of the DSA sets out a harmonised framework for how such information orders must be issued and executed. The DSA thus provide more specific additional obligations to complement the ECD. That is, while the ECD established the foundational principle that Member States may impose targeted information obligations, the DSA operationalises and harmonises these obligations across the EU. Furthermore, Article 10 DSA introduces additional safeguards for service providers and users, such as requirements for orders to be issued by competent judicial or administrative authorities, that were not explicitly required under the ECD

- Article 5 ECD requires that providers of information society services make certain basic details easily, directly, and permanently accessible, such as their name, geographic address, etc. Article 12(2) DSA refers back to the obligations provided under the ECD (thereby reaffirming the continued relevance of the ECD's requirements) and expands on them by requiring intermediary service providers to designate a single point of contact for direct communication, and to make public the information necessary for the recipients of the service to identify and communicate with their points of contact.

- Article 31(1) DSA requires providers of online marketplaces to design and organise their online interfaces in a way that enables traders to comply with their EU law obligations regarding precontractual information, compliance, and product safety information. This will allow online marketplaces to ensure that third party traders comply with obligations they have pursuant to Articles 5 and 6 of the ECD (information obligations), as well as Article 3 of Directive 98/6/EC, with Recital 74 of the DSA explicitly referencing these provisions as examples.

- Article 6 ECD requires that commercial communications "which are part of, or constitute" an **information society services** be clearly identifiable (Article 6 lit. a), with transparent identification of the natural or legal person (Article 6 lit. b) and of the terms of promotions or competitions (Article 6 lit. c). Article 26 DSA builds on this (recital 68 DSA) by mandating that **online platforms** clearly identify advertisements in real time, including both the advertiser and the payer (if different), provide accessible information on ad targeting parameters, allow users to declare commercial content, and prohibit profiling based on sensitive data. Article 39 DSA further extends these obligations for providers designated as very large online platforms (VLOPS) or very large online search engines (VLOSES) by requiring them to make publicly available information related to the identification of the advertisement and the person on whose behalf the advertisement is presented, in a single advertising repository. This creates an additional (but complementary) obligation to Article 6(b) ECD, which did not specify the need for a repository. While there is some duplication of the core requirement in relation to online platforms, i.e. certain hosting services, the DSA updates and expands the ECD framework, thereby making the two instruments complementary rather than duplicative.

- Article 45 DSA on codes of conduct aligns with and reinforces the obligations under Article 16 ECD, which requires Member States and the Commission to encourage the development of codes of conduct at the EU level by trade, professional, and consumer associations or organisations to contribute to the implementation of Articles 5 to 15 of the ECD.

- Article 17(1) ECD requires Member States to ensure that national legislation does not hinder the use of out-of-court dispute resolution schemes for information society services and Article 17(2) further encourages Member States to promote the voluntary use of ADR procedures, to ensure procedural guarantees for the parties involved, and to facilitate the communication of relevant information about such bodies to the European Commission. In the specific context of online platforms, Article 21 DSA is significantly more detailed and prescriptive, establishing a certification system for out-of-court dispute settlement bodies specifically for disputes related to online platform content decisions, including internal complaint handling failures. The DSA thus provides additional, complementary obligations.

Finally, when it comes to the **enforcement**, in contrast to the ECD, which gave Member States considerable discretion in its enforcement, the DSA establishes a stronger framework with fines up to 6% of annual worldwide turnover, periodic penalty payments for ongoing violations, and enforcement powers for the European Commission (for VLOPs) and national regulators. In terms of empowered authorities, while the ECD is enforced by ministerial authorities, and also subject to the CPC mechanism, the DSA enforcement is entitled to independent bodies (the Digital Services Coordinators). However, both instruments are based on the country-of-origin principle, where a given provider is subject only to the rules (and enforcement) of the country where it is established (or, in the case of the DSA, has appointed a legal representative).

*Special remarks on overlaps*

The DSA regulates intermediary services, which are a sub-category of information society services. Some of the obligations under the DSA highlighted above can be seen as specifications of similar ECD provisions and therefore as duplicative. However, the DSA obligations outlined above which may seem to overlap with Articles 5 or 6 ECD in particular are not an overlap, but apply as a complement (both articles of the ECD specify that they apply "in addition to other information requirements established by Community law"). Furthermore, some of the DSA obligations apply only to a narrow set of intermediary services, i.e. online platforms, whereas the ECD applies to information society services.

In the event of an overlap, Article 2(3) DSA states that the DSA 'shall not affect' the application of the ECD. The wording chosen (and the fact that the ECD is treated differently, under paragraph (3), from all other Union law instruments included in paragraph (4)) indicates that the DSA has been crafted to avoid any conflict with the ECD.

In sum, the ECD is the immediate "precursor" to the DSA. Concomitantly, the DSA and the ECD exhibit a significant interplay in their scope, working together to regulate intermediary services, a sub-set of information

society services, within the digital environment. The ECD establishes the initial legal framework for information society services in the EU, setting out key principles such as limited liability for intermediaries and transparency requirements. However, its provisions are high-level and leave significant discretion to Member States, resulting in a framework that is foundational but not comprehensive or fully harmonized. Building on this foundation, the DSA introduces more detailed, rules for intermediary services designed to address the complexities and evolving challenges of today's online ecosystems. Rather than replacing the ECD, the DSA complements and strengthens it by introducing targeted and updated rules for intermediary services, while many foundational provisions of the ECD continue to apply.

The ECD thus remains essential when assessing the compatibility of national laws regulating information society services or, as the case may be, intermediary services, with Union law. The assessment follows a tiered approach: first, it must be determined whether the national measure falls within the full harmonisation scope of the DSA, which would render the national law incompatible with Union law due to the DSA's overriding effect. If not covered by the DSA, the second step is to verify whether national law is governed by any sector-specific Union legislation that might apply. Lastly, if neither the DSA nor sector-specific Union law applies, the national measure must be evaluated against the country-of-origin principle established by the ECD, ensuring that Member States do not impose additional obligations beyond those permitted under the Directive. This layered testing mechanism underscores the continuing relevance of the ECD as a baseline instrument in the evolving regulatory landscape of information society (and intermediary) services.

## Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society ([45]) – [InfoSoc Directive]

*General Information*

The InfoSoc Directive was adopted on 22 May 2001 and came into force on its day of publication, 22 June 2001. The Directive harmonises key rights granted to authors and neighbouring rightsholders (the reproduction right, the right of communication to the public and the distribution right) and – to a lesser degree – exceptions and limitations to these rights. It also harmonises the protection of technological measures and of rights management information, sanctions and remedies. Since its adoption, the Directive has been amended twice, in 2017[46] and 2019[47].

The Directive aims to adapt legislation on copyright and related rights to technological developments and particularly to the information society, while providing for a high level of protection of intellectual property. It also seeks to implement 2 international treaties that were concluded in December 1996: the World Intellectual Property Organisation (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty.

*Personal scope*

The personal scope of the InfoSoc Directive (Directive 2001/29/EC) covers a defined set of actors involved in the creation, distribution and exploitation of copyright-protected works. It primarily targets rightsholders such as authors, performers, phonogram producers, film producers and broadcasting organisations (Articles 2-4). It also applies to users of protected content, including individuals and institutions accessing, reproducing or otherwise using works.

The Directive directly addresses intermediary services providers in the context of sanctions and remedies (Article 8(3)) and indirectly in the context of temporary acts of reproduction that have no independent economic significance (Article 5(1)).

*Territorial scope*

The InfoSoc Directive applies within the territory of the EU Member States (Article 1(1)) and governs acts that occur within the EU, such as reproduction, communication to the public and distribution (Articles 2-4).

*Material scope*

The InfoSoc Directive harmonises key economic rights in the digital environment, specifically the rights of reproduction, communication to the public and distribution (Articles 2-4). It applies to all types of copyright protected works and subject matter, including literary, musical, audiovisual and phonograms – with the exception of those excluded in Article 1(2), for example computer programmes.

---

[45]Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; OJ L 167, 22.6.2001, p. 10–19.

[46]Directive (EU) 2017/1564 of the European Parliament and of the Council of 13 September 2017 on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society; OJ L 242, 20.9.2017, pp. 6–13.

[47]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, PE/51/2019/REV/; OJ L 130, 17.5.2019, pp. 92–125

It covers both physical and digital uses, particularly addressing digital transmission and storage technologies. The Directive also establishes a framework for limitations and exceptions to these rights (Article 5), including for uses such as quotation, parody, teaching and temporary acts of reproduction (including the transmission in a network between third parties by an intermediary in Article 5(1) which is of relevance for the DSA).

*Enforcement*

The InfoSoc Directive does not contain a dedicated chapter detailing its enforcement regime. However, it sets out key provisions to ensure that stakeholders can enforce their rights effectively at national level (Article 8). It requires Member States to provide for appropriate sanctions and remedies, including damages, injunctions and seizure of infringing goods (Articles 8(1) and 8(2)).

Article 8(3) provides a crucial enforcement tool within the InfoSoc Directive as it enables rightsholders to obtain injunctions against intermediaries whose services are used by third parties to infringe copyright, even if the intermediary is not directly liable. These remedies are enforced according to the law of the Member State for which protection is claimed.[48]

The InfoSoc Directive is complemented in its enforcement by the mechanisms defined in Directive 2004/48/EC on the enforcement of IP rights (IPRED) (see dedicated fiche).

*Interactions with the DSA*

Recital 16 of the InfoSoc Directive clarifies that it is without prejudice to provisions relating to liability in the e-Commerce Directive (Directive 2000/31/EC); the relevant liability exemption provisions and the prohibition on general monitoring obligations are now incorporated in the DSA. This is relevant, as both the Infosoc Directive and the e-Commerce Directive explain that they were negotiated in parallel, in order to be consistent.[49]

Moreover, as per Article 89 DSA, any references to Articles 12 to 15 e-Commerce Directive should be construed as references to Articles 4, 5, 6, and 8 DSA, respectively.

The DSA references the InfoSoc Directive as part of the copyright *acquis* to which it is without prejudice in as far as the regulation of other aspects of the provision of intermediary services is concerned, in Recital 11. This denotes the intention that the InfoSoc Directive continues to apply on specific matters of copyright and related rights, and their enforcement (in conjunction with Directive 2004/48/EC on the enforcement of IP rights).

On **personal scope**, InfoSoc Directive and the DSA reveal complementary but distinct regulatory approaches.

---

[48]Article 8 of the Rome II Regulation clarifies that the lex loci protectionis applies to copyright infringement, covering both the requirements for protection and its scope. Jurisdiction is established according to the rules of the Brussels I Regulation. Article Article 7(2) of the Brussels I Regulation provides special jurisdiction for certain disputes, including torts such as copyright infringement. Jurisdiction lies with the courts of the place where the harmful event occurred or may occur.

[49]See recital 50 ECD ("It is important that the proposed directive on the harmonisation of certain aspects of copyright and related rights in the information society and this Directive come into force within a similar time scale with a view to establishing a clear framework of rules relevant to the issue of liability of intermediaries for copyright and relating rights infringements at Community level") and Recital 16 InfoSoc Directive ("(16) Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in 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")(4), which clarifies and harmonises various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonised framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive").

As noted above, the InfoSoc Directive primarily applies to rightsholders at large; users of protected content (individuals or entities engaging in lawful uses, including under exceptions). Intermediaries within the meaning of the DSA are only covered in the context of the obligation for Member States to ensure the possibility for rightholders to apply for injunctions against intermediaries (Recital 59 and Article 8(3) InfoSoc Directive), and, to the extent that the exception to reproduction right under Article 5(1) may apply to their activities (recital 33) . The Directive does not define "intermediaries", nor does it categorise them by type or scale. In turn, the DSA generally covers all different categories of online intermediary services providers, while InfoSoc addresses them only when their services are used as a channel for copyright and/or related rights infringement (Article 8(3) InfoSoc Directive).

Regarding **territorial scope**, the InfoSoc Directive applies within the territory of EU Member States, which are required to transpose its provisions into national law (Article 1(1) and Recital 6 InfoSoc Directive). Accordingly, if it is established that the relevant restricted act (reproduction, communication to the public) took place in a Member State, the conflict of laws rules apply in the Rome I and II (applicable law) and Brussels Regulations (jurisdiction). The DSA explicitly applies to online intermediary service providers regardless of establishment, provided they offer services to users in the EU (Article 2(1) and Recital 7 DSA). The territorial scope of the substantive and enforcement provisions of the InfoSoc Directive is tied to the relevant rules on applicable law and jurisdiction, in accordance with the Rome I and II Regulations, and the Brussels Ibis Regulation, respectively.

Referring to **material scope**, while the InfoSoc Directive defines what constitutes copyright restricted act through harmonization of exclusive rights, the DSA regulates how platforms may respond in certain scenarios to the infringement of those rights in the online environment, including copyright infringements. The DSA's material scope excludes substantive IP law but arguably provides procedural safeguards and governance tools that complement InfoSoc enforcement against intermediaries in Article 8(3) InfoSoc Directive. It can be concluded that there is no overlap between the two.

The InfoSoc Directive provides for private **enforcement** by rightsholders, through injunctions against intermediaries whose services are used to infringe copyright (Article 8(3) and Recital 59). It relies on national courts and procedural rules transposed by Member States, without establishing a centralised enforcement system. Article 8(3) InfoSoc Directive allows rightsholders to request injunctions from national courts against intermediaries whose services are used by third parties to infringe copyright.

Article 9(1) DSA requires intermediaries "to inform the [judicial or administrative] authority issuing the order [...] of any effect given to the order without undue delay", provided the order meets the minimum requirements indicated in Article 9(2). In this view, the DSA "tops-up" the injunctive relief offered by the InfoSoc Directive by establishing a regime of obligations once an injunction is issued. This order must be based on national or Union law, and intermediaries must comply swiftly and transparently.

*Special remarks on interplay*

There is no overlap and both DSA and the InfoSoc Directive interplay in a complementary manner.

# Directive 2002/58/EC ([50]) – [e-Privacy Directive]

*General Information*

The e-Privacy Directive (ePD) was adopted on 12 July 2002. As per Article 17, Member States were required to transpose the Directive before 31 October 2003. The Directive has been amended since its adoption through:

- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

As per Article 1(1), the ePD aims to ensure the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the EU.

*Personal scope*

The ePD applies to the electronic communications sector, including telecoms operators, internet access providers and providers of interpersonal communications services (e.g. email, VoIP, messaging apps, video chat platforms).

Specifically, as per Article 3 ePD, the Directive 'shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices'.

To provide further detail, Article 2 ePD refers to definitions in Directive 2002/21/EC, since replaced by the European Electronic Communications Code[51] (EECC). This law defines an 'electronic communications service' (ECS) as: 'a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

- '*Internet access service*' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120 (the Open Internet Regulation) – i.e. "a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used";

- *'Interpersonal communications service'*, defined in Article 2(5) of the EECC as "a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which

[50]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

[51]Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1972

enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service"; and

- Services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

- The ePD also has extended scope through Articles 5(3) and 13, which apply to ECS, as well as 'website operators (e.g. for cookies) or other businesses (e.g. for direct marketing)'[52].

*Territorial scope*

As per Article 3, the ePD shall apply to the processing of personal data in connection with the provision of publicly available ECS in public communications networks in the Union. While this provision is not explicit on the territorial application of the ePD, the 2015 assessment of transposition concluded that 'national provisions of a Member State transposing the ePrivacy Directive will be applicable to network and service providers operating on the territory of that Member State. As a result, the ePD is also applicable to network and service providers not established in the European Union, as long as they are providing networks and/or services on the territory of the Union'.[53]

*Material scope*

The ePD establishes rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It also bans unsolicited communications where the user has not given consent. Key provisions of relevance include:

- Article 1 outlines the scope and aim of the ePD, as detailed above.
- Article 4 provides rules on the security of processing, including placing obligations on providers of publicly available ECS to: (i) take appropriate technical and organisational measures to safeguard the security of their services, with specific requirements for the protection of personal data; (ii) notify the competent national authority and users of personal data breaches; and (iii) maintain an inventory of personal data breaches.
- Article 5 provides rules on the confidentiality of communications and the related traffic data. Article 5(1) prohibits listening, tapping, storage, or other kinds of interception or surveillance by persons other than the user without consent, while Article 5(3) establishes the EU's core rules on the use of cookies and similar technologies on user devices, requiring consent based on clear and comprehensive information about the purpose of processing for the storage of information, or the gaining of access to information already stored, in the terminal equipment of a user.
- Article 6 regulates the processing and storage of traffic data with the purpose of protecting user privacy.
- Article 13 requires prior consent for unsolicited communications and opt-out for use of contact details provided in the context of a sale for direct marketing.

*Enforcement*

In the ePD, enforcement is primarily governed through Article 15a (which was introduced by the 2009 amendment). Competent national authorities and, where relevant, other national bodies in each Member State

[52]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. Last accessed on 27 August 2025 at: https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

[53]European Commission, (2015) ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation. A study prepared for the European Commission DG Communications Networks, Content & Technology by timelex and Spark. Last accessed on 27 August 2025 at: https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data

shall have the power to order the cessation of infringements (Article 15a(2)). They shall have the necessary investigative powers and resources, including the power to obtain relevant information (Article 15a(3)). National regulatory authorities (NRAs) may adopt measures to ensure effective cross-border cooperation and notify such measures to the Commission under Article 15a(4). Depending on the Member State, these NRAs could be Data Protection Authorities (DPAs) or telecommunication regulators.

Penalties, including criminal sanctions where appropriate, are to be established by the Member States in accordance with Article 15a(1).

*Interactions with the DSA*

The ePD contains no references to the DSA. The DSA contains references to the ePD in Article 2(4)(g) as regards scope – it states that the DSA is without prejudice to the rules laid down by other legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing [the DSA], including: Union law on the protection of personal data, in particular the GDPR and the ePD. This is supplemented by Recital 10 of the DSA, while Recital 68 links to the ePD in the context of the provision of information relating to online advertising – specifically, the DSA 'is without prejudice to the provisions laid down in Directive 2002/58/EC [i.e. the ePD] in particular those regarding the storage of information in terminal equipment and the access to information stored therein' (i.e. the provisions of Article 5(3) ePD).

Regarding the **personal scope**, a range of digital service providers are subject to obligations under both the ePD and the function-based classification set out in the DSA. These can span all different types of intermediary services as defined in Article 3(g) of the DSA:

- 'Mere conduit' intermediary services. While 'internet access services', as categorised and defined under the EECC (with reference to the Regulation 2015/2120), are not explicitly named as examples of 'mere conduit' intermediary services within the DSA, providers of such services are considered to be covered by the definition of a 'mere conduit' intermediary service as they focus on the provision of access and the transmission of information rather than storage and dissemination of information. As defined in Article 3(g)(i), 'mere conduit' services are defined as the 'transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'. In addition, as clarified in Recital 29 DSA, 'mere conduit' intermediary services can include 'voice over IP and other interpersonal communication services', which are also explicitly defined within the EECC (which is referenced by the ePD).
- 'Caching' services. Providers of ECS as per the ePD can also be considered as 'caching' services under the DSA if they perform 'automatic, intermediate and temporary storage of [information] for the sole purpose of making more efficient the information's onward transmission' (defined in Article 3(g)(ii) and Article 5 DSA).
- 'Hosting services', including online platforms, VLOPs and, where applicable, VLOSEs. If an ECS provider as per the ePD also stores the information provided by, and at the request of, a recipient of the service, they are considered to be a 'hosting' service under the DSA (defined in Article 3(g)(iii) DSA). Further, in specific contexts, such ECS providers can be considered as: an 'online platform' if they also disseminate that information to the public (Article 3(i) DSA) – i.e. beyond interpersonal communications between a finite number of persons determined by the sender (as clarified by Recital 14 DSA); and a VLOP, should they meet the criteria outlined in Article 33(1) DSA.

Referring to the **territorial scope**, both the ePD and the DSA have similar reach; however, the DSA, through Article 2(1), addresses the issue of territorial application explicitly and directly, while the ePD deals with the issue indirectly through Article 3 and the transposition of the Directive by the Member States.

On **material scope**, the DSA explicitly states in Article 2(4)(g) that it applies without prejudice to Union law regulating other aspects or complementing and specifying the DSA on the protection of personal data, including the ePD.

The material scope of the DSA, and thus the nature of the interplay with the material scope of the ePD, differs based on the type of intermediary service:

- **Providers of ECS under the ePD and 'mere conduit' and/or 'caching' service providers under the DSA** – the obligations of the two laws in this situation apply in parallel. EPD requires providers to meet due diligence obligations relating to the provision of information to users when obtaining consent for: (i) the storing of information, or the gaining of access to information already stored, in the terminal equipment of a user/subscriber (Art. 5(3) ePD); (ii) the processing of traffic data for the purposes of marketing ECS or providing value added services (Art. 6(3) and (4) ePD); and (iii) the processing of location data other than traffic data (Art. 9(1) ePD).

  This is further complemented in the DSA by the requirements for transparency reporting under Art. 15. which apply if a provider has undertaken 'any content moderation' and unless the provider is an SME and also not a VLOP. There are no such requirements under the ePD.

- **Providers of ECS under the ePD and hosting services under the DSA** – Articles 16-18 DSA set out additional due diligence obligations for hosting services. These articles include notice and action mechanisms (Article 16 DSA), statement of reasons (Article 17 DSA), and notification of suspicions of criminal offences (Article 18 DSA). If an ECS is also a hosting service, it has to comply with these DSA's additional due diligence obligations.

- **Providers of ECS under the ePD and online platforms under the DSA** – beyond the general provisions applicable to 'mere conduit' and 'hosting' intermediary services, as outlined above, providers of online platforms and VLOPs are subject to additional cumulative obligations under the DSA. The most relevant is the interaction of Article 5(3) ePD with DSA transparency requirements:

  - Article 26 DSA governing advertising on online platforms and Article 27 DSA on recommender systems complement Article 5(3) ePD. If advertising or recommender systems implemented by online platforms use information stored in the terminal equipment of a subscriber or user (e.g. cookies or other tracking technologies), unless they meet the specific exemptions outlined in Art. 5(3) ePD, then the ePD requirements for consent for 'the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user' must first be fulfilled, in addition to the compliance with Article 6 GDPR. The definition of consent under the GDPR applies (Art. 4(11) & 7, supplemented by Recitals 32, 42, and 43). The provisions of the DSA then apply in parallel, ensuring additional transparency for users on the functioning of these systems.

  - Article 34 and 35 DSA on risk assessment and mitigation of risks for VLOPs are also relevant. Through these Articles, the DSA requires VLOPs to assess and mitigate risks related to negative effects for the exercise of fundamental rights, including to respect for private and family life enshrined in Article 7 and the protection of personal data under Article 8 of the Charter of Fundamental Rights of the EU. While not legally required, this could include consideration of the risks related to the use of tracking technologies in different contexts without interfering with the obligations to obtain consent set out in Article 5(3) ePD, and could further reinforce the security of processing requirements outlined in Article 4 ePD. The provisions of the two laws are complementary in this regard.

With regards to **enforcement**, distinct enforcement systems comprising competent national authorities in each Member State are implemented under the two laws. These authorities (NRAs under the ePD, DSCs and CAs under the DSA) have distinct legal remits, but they may find themselves supervising the same providers. Within this context, investigatory, complaint-handling and transparency enforcement powers can intersect.

However, the DSA explicitly empowers DSCs to ensure cooperation at national level with other national competent authorities to streamline supervision and enforcement of the DSA (Article 49(2) as regards general cooperation; Article 53 as regards the right to lodge a complaint; supplemented by Article 57(2) on mutual assistance). This should facilitate alignment at the practical level.

*Special remarks on interplay*

As detailed above, while a number of areas of interplay between the DSA and the ePD have been identified, the provisions mutually reinforce each other and no overlaps occur, thus resulting in a complementarity between them.

## Regulation (EC) No 273/2004 ([54]) – [Drugs Precursors Regulation]

*General Information*

Regulation (EC) No 273/2004 (Drugs Precursors Regulation, DP) was adopted on 11 February 2004 and entered into force in the EU Member States on 18 August 2005. Exceptionally, Articles 9, 14, and 15 of the DP became directly applicable at the date of publication, in order to permit the adoption of the measures provided for in the text of the Articles, such as guidelines on facilitation of cooperation within the chemical industry (Article 9), measures for implementation of the Regulation (Article 14), and the adoption of the rules of procedure of the relevant committee of Member State representatives (Article 15).

The Regulation aims to establish harmonised control and monitoring measures within the Union concerning the trade of certain substances that are frequently used in the illicit manufacture of synthetic drugs and new psychoactive substances. Its central goal is to prevent the diversion of these so-called "drug precursors" from legitimate trade into illicit drug production channels.

*Personal scope*

The DP regulates "operators" as defined in Article 2(d) as "any natural or legal person engaged in the placing on the market of scheduled substances", where placing on the market denotes the supply (whether for return of payment or free of charge) of scheduled substances in the Union, or the "storage, manufacture, production, processing, trade, distribution or brokering of these substances for the purpose of supply in the Union" (Article 2(c)).

*Territorial scope*

The Regulation applies within the territory of the EU, covering intra-Community trade of scheduled substances that are frequently used in the illicit manufacture of narcotic drugs or psychotropic substances.

*Material scope*

The DP's material scope focuses on regulating operators who are involved in the placing on the market—defined broadly to include manufacture, import, export, distribution, and brokering—of scheduled substances listed in Annex I. These substances are divided into categories based on their risk of diversion, with Category 1 being subject to the most stringent controls.

Operators placing Category 1 substances on the market are required to obtain a license and designate a responsible officer (Article 3(1)-(3)), while those dealing with Category 2 substances must designate a responsible officer and register their premises with the competent authorities (Article 3(6)). Operators must also ensure that customer declarations are obtained and retained for supplies of Category 1 and 2 substances, specifying the intended use (Article 4). Certain exemptions apply for small quantities of Category 2 substances, as set out in Annex II. In addition, detailed documentation obligations apply to all transactions involving these substances, including requirements to identify the substances, quantities, and parties involved (Article 5). These records must be retained for at least three years and be made available to competent authorities upon request.
The Regulation also imposes labelling obligations (Article 7), requiring that scheduled substances be clearly marked with their names as listed in Annex I. Operators must notify authorities of any suspicious transactions that may indicate potential diversion to illicit drug manufacture (Article 8). Special provisions are foreseen for public entities such as pharmacies, veterinary dispensaries, and the armed forces, which may be granted special

[54]Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors (Text with EEA relevance), OJ L 47, 18.2.2004, p. 1–10.

licenses or registrations for official use. Overall, the material scope of the Regulation is preventive in nature, aiming to safeguard the legal supply chain against diversion by imposing traceability, transparency, and oversight requirements on relevant economic operators within the EU.

*Enforcement*

According to Article 11(1) of the DP, each Member State shall designate the competent authorities responsible for applying the Regulation and inform the European Commission accordingly. As per Article 12 DP Member States must lay down the rules on applicable penalties for infringement which must be effective, proportionate and dissuasive. To ensure enforcement, Article 10(1) of the DP prescribes that Member States must enable their competent authorities to obtain all necessary information about orders or activities involving scheduled substances, to inspect business premises in order to obtain evidence of irregularities as well as to detain and seize consignments which are not in accordance with the Regulation.

*Interactions with the DSA*

The DP does not include any reference to the DSA. A 2020 evaluation of the DP suggested in fact that it should address online marketplaces more directly (as is the case in the Explosive Precursors Regulation).[55]

Regarding the **personal and territorial scope**, the DP applies to operators, defined in Article 2(d) as "any natural or legal person engaged in the placing on the market of scheduled substances", regardless of the sales channel. This includes both physical and online environments but does not directly regulate intermediary service providers as defined in the DSA (i.e. hosting services, online platforms, or search engines). However, indirect interplay arises where online marketplaces or platforms act as facilitators or intermediaries for transactions involving scheduled substances. In such cases, the DP obligations fall on the seller (the economic operator), but the DSA may impose complementary due diligence obligations on the online intermediary, for instance through notice and action mechanisms (Article 16 DSA), risk mitigation duties for illegal content (Article 34-35 DSA), or transparency reporting obligations (Articles 24 and 42 DSA).

In other words, two setups can be envisaged regarding how scheduled substances are made available on the Union via online marketplaces, which will apply differently depending on the role played by the marketplace, on a pure or hybrid model.

On the one hand, online intermediary platforms allowing traders to conclude distance contracts with customers are subject to the requirements laid down in the DSA. On the other hand, where the provider of a marketplace qualifies as an economic operator such as manufacturer, distributor or importer, the DSA would not apply, and instead the marketplace is subject to specific sectoral obligations according to Regulation (EC) 273/2004.

With regards to the **material scope**, there is a complementary interplay in material scope between the DSA and the DP in areas where both instruments regulate aspects of online commerce, public safety, and the traceability of goods. The DSA establishes horizontal obligations for providers of online platforms allowing consumers to conclude distance contracts with traders, including traceability of traders (Article 30), platform design enabling compliance with Union law (Article 31), and consumer information requirements (Article 32) which are applicable across all product categories. In parallel, the DP introduces sector-specific, vertically framed rules governing the lawful marketing, distribution, and control of scheduled substances used in the illicit manufacture of drugs. Specifically, Articles 3–5 and 7 of the DP impose obligations on economic operators concerning classification, licensing, documentation, and labelling of precursor chemicals. These apply to all channels of trade, including online.

[55] Report from the Commission to the European Parliament and the Council on Evaluation of the EU drug precursors regulations, accessible via: REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Evaluation of the EU drug precursors regulations - Publications Office of the EU

In this regard, the DP supplements the DSA by prescribing detailed rules for a high-risk product category, while the DSA ensures that the platforms enabling such transactions implement mechanisms to support compliance with applicable laws. Further complementarity arises in the area of illegal content and systemic risk mitigation. Under Article 3(h) DSA, content involving the unlawful sale of substances restricted by the DP constitutes "illegal content" for the purposes of the DSA's notice-and-action framework (Article 16). Additionally, Articles 34 and 35 DSA require Very Large Online Platforms (VLOPs) to assess and mitigate systemic risks to public health—risks that may include the diversion of chemical precursors for illicit drug manufacture. Taken together, the DSA provides a horizontal framework ensuring online intermediaries adopt due diligence mechanisms that facilitate legal compliance, while the DP vertically regulates the handling of a specific class of sensitive goods.

On another vein, there is parallel application of **enforcement** mechanisms under the DSA and the DP, with each instrument assigning oversight responsibilities to distinct national authorities. Under Article 12 DP, Member States are required to adopt national rules on penalties for breaches of the regulation, but the DP does not prescribe harmonised thresholds or specific penalty levels. In contrast, Article 52(3) DSA introduces harmonised ceilings for fines, including a maximum of 6% of the annual worldwide turnover of the provider in the preceding financial year. This reflects the DSA's horizontal enforcement harmonisation across the digital internal market. Both instruments require national designation of competent authorities – Article 11 DP for the precursor framework and Article 49 DSA for digital services. The DSA also mandates the appointment of one of the competent authorities as Digital Service Coordinator per Member State.

*Special remarks on interplay*

As detailed above, both legislations can coexist and interplay, resulting in a complementarity application.

## Directive 2004/48/EC ([56]) – [Intellectual Property Rights Enforcement Directive]

*General Information*

The Intellectual Property Rights Enforcement Directive (IPRED) was adopted on 29 April 2004 and came into force on 20 May 2004 (Article 21) with the implementation date for the Member States set for 29 April 2006 (Article 20). On 29 November 2017 the Commission published an evaluation report of the Directive.[57]

The IPRED provides a minimum set of measures, procedures and remedies allowing effective civil enforcement of intellectual property rights (IPRs) across the EU, ensuring standardised level of protection throughout the internal market. The directive's main objective is to ensure that the same tools are available throughout the EU for rightsholders and innovators to be able to enforce their IPRs. In addition to tackling counterfeiting and piracy, it also aims to achieve other objectives which include promoting innovation and business competitiveness, safeguarding employment in Europe and ensuring consumer protection.

*Personal scope*

The personal scope of IPRED (Article 4) extends to a range of subjects entitled to seek enforcement of IPRs through the measures, procedures, and remedies established by the Directive. This includes primarily the holders of IPRs themselves, as recognised under the applicable national law.

Additionally, the Directive encompasses other persons authorised to use these rights, notably licensees. Furthermore, the Directive acknowledges collective rights management organisations that are regularly recognised as having a right to represent rights holders. Lastly, the Directive covers professional defence bodies that are duly recognised as having the authority to represent rights holders.

According to recital 18 the personal scope is to be interpreted broadly. Like the InfoSoc Directive, the IPRED does not impose obligations to intermediaries, but mandates Member States to ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right (Article 11 IPRED), and to allow for interlocutory injunctions against intermediaries (Article 9 IPRED) or information orders (Article 8 IPRED), the latter being limited by the application of competing fundamental rights, namely privacy/data protection.[58]

*Territorial scope*

The Directive applies to all persons and entities within the Member States, as per national law implementing the Directive (Article 2(1)).

*Material scope*

---

[56]Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights

[57]European Commission, Evaluation: Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, Staff Working Document SWD(2017) 431 final, 29 November 2017, accompanying COM(2017) 708 final. Last accessed on 30 June 2025, https://ec.europa.eu/docsroom/documents/26601.

[58]*Bonnier Audio AB and Others v Perfect Communication Sweden AB*, Case C-461/10, 19 April 2012, ECLI:EU:C:2012:218..https://curia.europa.eu/juris/document/document.jsf;jsessionid=8EE22EF782EA86784E12186D92C662D3?text=&docid=114613&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5421829

The material scope of the IPRED encompasses a range of measures, procedures, and remedies aimed at the effective enforcement of IPRs, relying on Member States civil enforcement systems. Article 8 grants rightsholders the right to request information from infringers and certain third parties about the origin and distribution of infringing goods and services, thereby facilitating the identification and cessation of unlawful activities[59].

Article 9 provides for provisional and precautionary measures, allowing courts to impose interim actions to prevent or halt ongoing infringements, ensuring that rights are protected promptly and effectively. Furthermore, Article 10 sets out corrective measures, including the recall, removal from the market, or destruction of infringing goods and materials, thereby addressing the consequences of infringement.[60]

Moreover, Article 11 empowers courts to issue permanent injunctions against infringers and intermediaries, providing a lasting remedy to prevent recurrence of violations. Lastly, Article 12 allows for alternative measures, such as monetary compensation, in appropriate cases, offering flexibility in enforcement to accommodate different circumstances.

*Enforcement*

IPRED builds on national civil procedural law practices in Member States that continue to coexist. It allows national judicial authorities to take appropriate measures to protect IPRs. The general obligation is set out in Article 3(1), which requires Member States to provide the necessary measures, procedures, and remedies to ensure the effective enforcement of IPRs within their jurisdictions. This obligation mandates that national legal systems equip competent authorities with the powers needed to prevent and address infringements, thus enabling rightsholders to protect their interests effectively. Enforcement typically takes place in the Member State where the infringement occurs or where the infringing services are provided.

*Interactions with the DSA*

The IPRED was adopted in 2004 prior to the DSA. It does refer to the Regulation 2000/31/EC (e-Commerce Directive –ECD) in recital 15.[61] As per Article 89 DSA, any references to Articles 12 to 15 e-Commerce Directive should be construed as references to Articles 4, 5, 6, and 8 DSA, respectively.

The DSA explicitly references the IPRED in Recital 11: "It should be clarified that this Regulation is without prejudice to Union law on copyright and related rights, including Directives 2001/29/EC, 2004/48/EC [IPRED] and (EU) 2019/790 of the European Parliament and of the Council, which establish specific rules and procedures that should remain unaffected."

Additionally, Article 2(4)(b) reiterates 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* this Regulation, in particular, the following: […] Union law on copyright and related rights".

Regarding **personal scope**, IPRED (Article 4) primarily encompasses holders of IPRs, authorised users such as licensees, recognised collective rights management organisations, and professional defence bodies. Notably, the Directive explicitly addresses intermediaries in Arts. 9 and 11, providing for provisional and precautionary measures, as well as injunctions issued by judicial and administrative authorities against intermediaries whose services are used by third parties to infringe IPRs. This inclusion recognises the role intermediaries may play in facilitating infringement and grants rightsholders the ability to target such actors within the enforcement

[59] *Castorama Polska and Knor*, Case C-628/21, Court of Justice, 27 April 2023, ECLI:EU:C:2023:312; *Bastei Lübbe*, Case C-149/17, Court of Justice, 18 October 2018, ECLI:EU:C:2018:842.
[60] *Procter & Gamble International Operations*, Case C-355/21, Court of Justice, 13 October 2022, ECLI:EU:C:2022:791.
[61] Establishing that IPRED should not affect 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 (6).

framework. While IPRED also applies to copyright, the specific regime for injunctions against online intermediaries in case of copyright infringement remains governed by Article 8(3) InfoSoc Directive (see dedicated fiche). This provision is similar to the injunction provision in IPRED.

While both the IPRED and the DSA cover intermediaries, the substantial rules differ and allow for complementary application of both.

On **territorial scope** the IPRED, as established in Article 2(1) and Recital 10, applies within the internal market of the Member States, regardless of where the infringers are established. Its enforcement measures under the Directive are limited to actions within the national jurisdictions of EU Member States. Article 2(1) DSA provides that it applies to intermediary services offered to recipients who have their place of establishment or are located within the Union, regardless of where the providers of those intermediary services themselves are established. Therefore, the rules for determining territorial scope are different in the DSA and the IPRED.

With regards to **material scope**, the IPRED and DSA differ in subject matter but intersect and complement each other in their regulation of intermediaries. The IPRED's material scope centres on the enforcement of IPRs through specific measures.

Recital 11 DSA explicitly clarifies that the DSA is without prejudice to the IPRED; it acknowledges that specific rules and procedures concerning IP enforcement remain unaffected. This means that the enforcement mechanisms of the IPRED, particularly those relating to injunctions and other remedies against infringements, still apply where both instruments are relevant.

Article 8 IPRED grants rightsholders a specific right to information from infringers and certain third parties, possibly including online intermediaries concerning the origin and distribution of goods or services infringing IPRs. This right is a targeted enforcement tool designed to aid in identifying the source and scope of infringement, thereby enabling effective legal action. Article 8(2) IPRED mentions information that courts may order to be provided by infringers (or in certain scenarios intermediaries) to give them in relation to an IP infringement (specifically, what information the infringer and the intermediary must provide to courts). In turn, Article 10 DSA also includes specific obligations directed at providers of intermediary services, as they shall promptly inform the issuing authority, or any authority named in the order, of its receipt and execution, including if and when it was carried out (Article 10(1)) as well as inform the recipient of the service concerned of the order received and the effect given to it (Article 10(5)). Article 10(2) DSA sets out the formal requirements that must be met by the order to trigger these obligations. Article 10(3) DSA describes how the order shall be transmitted to the competent Digital Services Coordinator (DSC), and how that DSC shall transmitted that order to other DSCs (Article 10(4) DSA).

These obligations do not conflict with those potentially imposed on intermediaries in Article 8 IPRED, especially those concerning the content of the information to be provided as listed in Article 8(2). The DSA rules complement the IPRED, meaning that where the formal requirements set out in Article 10(2) DSA are fulfilled, an order under Article 8 IPRED will also trigger the obligations of the provider under Article 10 DSA.

Article 9 IPRED empowers courts (not also administrative authorities as DSA) to impose provisional and precautionary measures to prevent or halt ongoing infringements of IPRs. These interim measures are designed to act swiftly to preserve the status quo and avoid further harm before a final judicial decision. Article 11 IPRED provides for injunctions against infringers and intermediaries whose services are used by third parties to infringe IPRs. These injunctions can be permanent and serve as a decisive enforcement remedy to prevent recurrence of infringement. Article 9 DSA applies in a complementary manner to such orders, by setting out formal requirements in Article 9(2), that, if fulfilled by an order issued under Article 9 or 11 IPRED, would trigger the obligation of the provider under Article 9(1) DSA, to inform the issuing authority without any delay of any follow up given to the orders, specifying if and when the order was applied.

When it comes to **enforcement**, regarding enforcement mechanism, the IPRED relies on national authorities and judicial bodies empowered to grant enforcement measures, reflecting a decentralised enforcement model

within Member States based on national civil law. This can differ between Member States depending on their national legal traditions.

Given the limited overlaps in material scope between the IPRED and the DSA, the enforcement mechanisms of both instruments act in complementarity.

*Special remarks on interplay*

In sum, the DSA and the IPRED establish complementary legislative frameworks. IPRED focuses specifically on enforcing intellectual property rights through national judicial and administrative measures targeting infringers and intermediaries involved in infringement. The DSA regulates intermediary services across the EU with a centralised enforcement involving DSC and the Commission. While both legal instruments regulate intermediaries and provide mechanisms for information disclosure and interim and permanent measures as described above, these mechanisms do not overlap but interplay, complementing each other.

# Directive 2005/29/EC ([62]) – [Unfair Commercial Practices Directive]

*General Information*

The Unfair Commercial Practices Directive 2005/29/EC (UCPD) was adopted in 2005 and entered into application on 12 December 2007. In December 2021, the European Commission adopted the current, updated guidance on the UCPD – Notice on the interpretation and application of the Unfair Commercial Practices (hereinafter: "the UCPD guidance").[63]

The UCPD aims to protect consumers from unfair business-to-consumer (B2C) commercial practices before, during, and after a transaction. Its main objective is to approximate the laws of Member States relating to unfair commercial practices and ensure a high level of consumer protection, thereby contributing to the proper functioning of the internal market. The Modernisation Directive (EU) 2019/2161 updated the UCPD to strengthen its enforcement and to address specific digital challenges. Specifically, the Modernisation Directive reinforced the UCPD rules by expressly prohibiting in all circumstances certain additional online practices such as false consumer reviews. Directive (EU) 2024/825 on empowering consumers for the green transition further amended the UCPD to enhance consumer protection related to sustainability and green claims. The European Commission's recent Digital Fairness Fitness Check report, published in October 2024, highlights the limitations of the UCPD (as well as of the Consumer Rights Directive (CRD), and Unfair Contract Terms Directive (UCTD)) in effectively addressing certain identified challenges in digital markets.[64]

*Personal scope*

As per Article 3(1), the UCPD only applies to business-to-consumer (B2C) commercial practices. The obligations under the UCPD are imposed on traders, as defined in Article 2(b) UCPD, that is any natural or legal persons acting for purposes relating to their trade, business, craft, or profession, and anyone acting in the name of or on behalf of such persons. Traders must ensure that their commercial practices towards consumers comply with Directive's rules. Business-to-business (B2B) transactions, consumer-to-consumer (C2C) transactions, or consumer-to-business (C2B) transactions fall outside the UCPD's scope.

The UCPD can apply to non-EU traders by virtue of Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II). This Regulation applies '*in situations involving a conflict of laws, to non-contractual obligations in civil and commercial matters*'. When the conditions of Article 6(1) of the Rome II Regulation are fulfilled, for example, if the misleading advertising harms the collective interests of EU consumers, the UCPD applies irrespective of where the trader is established, i.e. also to traders outside the EU. Pursuant to Article 6(4) of the Rome II Regulation, the law that is applicable may not be derogated from by a choice-of-law agreement.

*Material scope*

---

[62] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22–39).

[63] Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, OJ C 526, 29.12.2021, pp. 1–129, available at: https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-and-price-indication/unfair-commercial-practices-directive_en

[64] Commission Staff Working Document - Fitness Check on EU consumer law on digital fairness, 4 October 2025, available at https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en

The UCPD applies to a wide range of practices, actions or omissions, by any trader involved in the promotion, sale, or supply of a product or service to consumers (Article 2(d)). The notion of a 'commercial practice' is broadly defined ensuring a wide scope of application. For example, for the UCPD to apply, there is no need for a consumer and a trader to be bound by a contract[65], Unfair practices may arise if they breach the trader's professional diligence (Article 5), if they are misleading (Article 6 and 7) or aggressive (Articles 8 and 9), provided that they materially impact or are likely to impact the average consumer's transactional decision-making. These general, principle-based provisions are complemented by Annex I that sets out a list of specific unfair practices that are prohibited in all circumstances, without the need for case-by-case assessment of their impact on the average consumer (the "blacklist" of unfair practices).

In the case of conflict between the provisions of the UCPD and other Union law regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects (Article 3(4)). The UCPD is then lex generalis in regulating unfair commercial practices, acting as a "safety net".

*Enforcement*

The UCPD approximates the rules on unfair practices against consumers, using the "average consumer" as benchmark for assessing whether the practice has or is likely to cause the consumers to take a transactional decision that they would not have taken otherwise. Special rules apply when the commercial practice targets vulnerable consumers or particular groups of consumers. The UCPD does not prescribe how national authorities should enforce its provisions. Instead, it requires Member States to ensure effective means to combat unfair commercial practices to protect consumers. These include adopting legal provisions allowing persons or organisations with legitimate interest (e.g., competitors) to take legal action or bring complaints before competent administrative authorities. Member States decide whether courts or administrative bodies handle these cases, whether actions can target multiple traders or code owners promoting non-compliance, and if accelerated procedures (interim or definitive) apply.

It is noteworthy that the Representative Actions Directive (Directive (EU) 2020/1828) empowers qualified entities to bring collective legal actions on behalf of consumers against infringements of EU laws, including those under the UCPD and the DSA, thereby strengthening enforcement of the rights of recipients of the service across the internal market.

The application and enforcement of the UCPD falls within the competence of authorities and courts at Member State level. The European Commission does not have direct enforcement powers to take action against traders for unfair commercial practices under the UCPD. Cooperation among Member States is ensured via the Consumer Protection Cooperation (CPC) Regulation, which strengthened the so-called "CPC Network", facilitated by the Commission, with the objective of monitoring the implementation and effectiveness of the consumer acquis.
The Modernisation Directive 2019/2161 strengthened the enforcement provisions of the UCPD by further harmonising the rules on penalties. It introduced indicative and non-exhaustive list of criteria for the imposition of penalties and required Member States to provide for the possibility to impose fines of up to at least to 4 % of the trader's annual turnover in the Member State(s) concerned (Article 13(3)) in cases where penalties are imposed by Member States in a coordinated manner in the context of the actions of the CPC network. It also required Member States to ensure that consumers harmed by unfair commercial practices have access to proportionate and effective remedies, including compensation for damage.

*Interactions with the DSA*

The UCPD does not contain any references to the DSA. However, Annex II of the UCPD (on Union law provisions setting out rules for advertising and commercial communication) refers to Articles 5 and 6 of the e-Commerce Directive (2000/31/EC).

[65] Case C-281/12 Trento Sviluppo ECLI:EU:C:2013:859.

The DSA establishes (Article 2(4)) that it is without prejudice to Union law rules regulating the provision of information society services in general, regulating *other aspects* of the provision of intermediary services in the internal market or *specifying and complementing* the harmonised rules set out in the DSA, making explicit reference to the UCPD in this regard. Another express reference to the UCPD can be found in Article 25(2) DSA. That provision stipulates that the prohibition related to dark patterns does not apply to practices already covered and prohibited by the UCPD.

On **personal scope**, the Directive applies to all traders that engage in commercial practices directed at consumers within the EU, irrespective of the medium used (online or offline), the sector of activity, or the legal form of the trader. It also applies to persons acting on behalf of the traders. The DSA clarifies that consumers are considered to be 'recipients of the service' for the purpose of the DSA (recital 2) Consequently, both UCPD and DSA may apply to the same B2C relationships, provided that the recipient of the service is a consumer and that the intermediary service provider is a trader under Article 2(b) UCPD. The latter assessment is made on a case-by-case basis, considering whether the online platform acts either for purposes relating to its business or in the name or on behalf of another trader. If an online platform qualifies as a trader, it must comply with EU consumer law regarding its commercial practices given the UCPD's broad definition of commercial practices as any activity directly connected to the promotion, sale, or supply of products to consumers (Article 3(1) UCPD).

Referring to **territorial scope**, both the UCPD and the DSA cover service providers that are located within the EU or outside the EU, as long as they offer a service to recipients located in the Union (Art 2 DSA) or in case of the UCPD the conditions of Article 6(1) of the Rome II Regulation are fulfilled.

With respect to **material scope**, the UCPD applies to the business-to-consumer (B2C) relationship within the context of broadly defined "commercial practices" .[66] This means that the UCPD applies in pre-, post-, as well as contractual situations. The Court of Justice has recognised that practices influencing the intention to purchase a product may amount to consumers taking a transactional decision, leading to the applicability of the UCPD.[67] Similarly, the European Commission has indicated that trader's activities influencing the consumer's choice to visit a store or to scroll content may also affect consumers' transactional decisions [68]. Consequently, many of the activities of online platforms fall within the scope of "commercial practices" leading to their recipients taking "transactional decisions". Still, the DSA could be perceived as applying more broadly, encompassing not only transactional but also any non-transactional aspects of platform-to-consumer interactions that would fall outside of the scope of "commercial practices" impacting consumers' transactional decision-making, like personalised experiences offered by social media platforms.

For example, the DSA lays down the online platforms' transparency obligations (as regards the identity of the points of contact for Member States' authorities, the Commission and the Board and vis-à-vis recipients of the service), provisions related to dark patterns (Article 25 which also specifies that the prohibition of dark patterns shall not apply to practices covered by UCPD and GDPR), online advertising (Article 26, 28 and 39) as well as recommender system transparency (Articles 27 and 38), and detailed obligations related to content moderation (Articles 16, 17, 18, 20, 21, 22, and 23).

A practice by an online intermediary that infringes these DSA rules could potentially also infringe the UCPD, such as its Article 5 prohibiting practices contrary to professional diligence (e.g. failure to comply with the DSA obligations on removal of misleading third-party commercial content or with the obligation to enable third-party suppliers of products to provide mandatory consumer information), Articles 6 and 7 addressing misleading practices (e.g. presenting advertisements failing to ensure that they are identified as such), and Article 8

[66] The UCPD guidance (section 2.3).
[67] Case C-281/12 Trento Sviluppo ECLI:EU:C:2013:859.
[68] The UCPD Guidance (section 2.4).

addressing aggressive commercial practices, provided that these infringements of the DSA fall withing the scope of commercial practices and negatively affect the consumers' transactional decisions.

It is true that, for example, Article 26 DSA provides more specific and operational requirements for advertising transparency and Article 12 DSA specifically deals with information about the point of contact. According to Article 3(4) UCPD, EU rules regulating specific aspects of unfair commercial practices (*lex specialis)* prevail and apply to those practices in case of conflict. The Court of Justice [69] has clarified that "*conflict such as that envisaged in Article 3(4) of Directive 2005/29 is present only where provisions, other than those of Directive 2005/29, which regulate specific aspects of unfair business practices, impose on undertakings, in such a way as to leave them no margin for discretion,* ***obligations which are incompatible with those laid down in Directive 2005/29***." Accordingly, only in that case the application of the UCPD is excluded, whereas in other cases, where the obligations laid down by *lex specialis* and those laid down in the UCPD are "compatible", the application of the UCPD is not excluded and is possible.

The UCPD and DSA material scopes also interplay as regards the provision of pre-contractual information. Article 7(4)(f) of the UCPD, in alignment with Article 6a CRD, requires online marketplaces to disclose to consumers whether parties offering goods/services on their interface are traders (that is, whether they declared to the online marketplace that they offer goods/services as part of their commercial activity). Article 30(1) and (7) of the DSA, in turn, obliges online platforms allowing consumers to conclude distance contracts with traders to collect certain information from traders prior to providing their service to them and disclose part of this information to recipients of the service in a clear, easily accessible and comprehensible manner. This constitutes more specific and complementary information to the more general obligation under the UCPD to identify the B2C character of a transaction.

Another form of interplay between the UCPD and the DSA is that between the transparency obligations under Article 7(4)(a-e) and (b) of the UCPD and an online marketplace's so-called 'compliance by design' obligations under Article 31(1) and (2) of the DSA. Under Article 7(4)(a-e) and (b) of the UCPD, traders – including traders offering goods or services on an online marketplace – are required to provide information on the characteristics of a product and on their identification. Article 31(1) and (2) of the DSA complements this provision, by obliging online marketplaces to design and organise their online interface in a way that enables traders offering products or services on their marketplace to provide such mandatory consumer information. The information obligations under the UCPD applies to the traders offering goods and services, while the DSA provides an obligation on the online platforms to facilitate such a disclosure, and consequently also the compliance with legal obligations that traders have under the UCPD.

On **enforcement**, as a consumer law instrument, the UCPD is enforced by national authorities and courts in the Member States. In cross-border cases, national consumer authorities cooperate and coordinate their enforcement actions in the CPC Network in accordance with the cooperation mechanism established by the CPC Regulation. The DSA establishes a specific public enforcement framework for the enforcement of online intermediaries' obligations under the DSA, at national and European level and based on where the intermediary service provider is established ('country-of-origin' principle). That public enforcement framework is distinct and separate from the public enforcement framework for consumer law, mainly focused where the consumers reside.

*Special remarks on overlaps*

Some elements need to be highlighted as follows:

- **Deceptive and manipulative design**: Article 25 of the DSA prohibits online platforms from deceptive or manipulative design (so-called "dark patterns"). This prohibition shall not apply to practices covered by UCPD or Regulation (EU) 2016/679 (GDPR). This means that if a dark pattern of an online platform violates the UCPD, its illegality will be determined according to the requirements of the UCPD, not the DSA.

[69] Joined Cases C-54/17 and C-55/17, Wind Tre, para. 61.

Dark patterns are generally understood as deceptive and manipulative interface design features such as creating click fatigue, misleading choice architecture, nagging and shaming, pressuring through scarcity claims [70]. Such practices fall under the scope of the general UCPD provisions when they materially impact consumers' transactional decision-making. Moreover, "dark patterns" are also often presented as encompassing practices such as "bait-and-switch" offers or false urgency claims that are already specifically addressed and prohibited in Annex I (the "blacklist" of the UCPD).[71]

Digital manipulative tactics have evolved into dynamic, personalized interfaces driven by artificial intelligence, algorithms and user data. Although all unfair commercial practices are in the scope of the UCPD regardless of the technology used, its principle-based rules are difficult to apply in such complex cases. Article 25 of the DSA uses broad terms like "design," "organise," and "operate" regarding online interfaces, which can be interpreted to cover these dynamic dark patterns. Importantly, the DSA's prohibition on the use of deceptive and manipulative design in online interfaces applies regardless of whether the recipient of the service, and likely the harmed entity, is a consumer or another trader and it applies regardless of the impact on the consumers' transactional decisions. For example, failing to make easily accessible the notice-and-action mechanism to remove illegal content can harm not only consumers but also competitors, who are traders. This means that the scope of Article 25 of the DSA is inherently broader than the protection offered under the UCPD, which applies to business-to-consumer relations.

It might be argued that where a commercial practice related to the use of deceptive or manipulative online design breaches the UCPD, Article 25 DSA would not apply. However, interpretation issues arise due to the lack of clear definitions of deceptive and manipulative design features covered by the UCPD and the DSA. This lack of clarity leaves room for interpretation regarding which dark pattern falls outside the scope of the UCPD and therefore should be addressed through the DSA. This creates practical enforcement challenges as elaborated below.

While the UCPD acts as "safety net" giving prevalence to more specific rules established in other Union law instruments (Article 3(4) UCPD), in the particular case of dark patterns, it is the DSA that acts as the "safety net" complementing the UCPD.

Academics have attempted to develop conceptual frameworks and methods to determine when deceptive and manipulative online design is in potential violation of the DSA, and national courts have addressed dark patterns applying the UCPD and DSA. However, there is so far no CJEU ruling specifically on dark patterns under the UCPD or DSA.

As regards relevant enforcement experience so far, recently the Consumer Protection Coordination (CPC) network, under European Commission's coordination, considered some of the commercial practices of Star Stable Entertainment AB as infringing prohibition of No. 28 of Annex I of the UCPD against direct exhortation to children as a result of "pressuring techniques encountered in the gameplay".[72] Further, "children through the design of the gameplay, combined with marketing in social media, are unduly influenced to buy in-game content, particularly during time-limited events". In the future, such findings

---

[70] See for example, the UCPD guidance (section 4.2.7) and *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report, Pu*blications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/859030.

[71] See section 4.2.7. Data-driven practices and dark patterns of the Commission's 2021 Notice on the interpretation of the UCPD.

[72] European Commission, 'Common position by competent authorities under Article 19(3) of Regulation (EU) 2017/2394 and concerning the commercial practices of Star Stable Entertainment AB' (21 March 2025) https://commission.europa.eu/document/download/030ff1d8-526e-4807-8a7e-1505f9e235d9_en?filename=Common%20Position%20on%20Star%20Stable%20Online%20.pdf.

could also give rise to actions under Article 25 of the DSA against manipulative interface design of online platforms.

Another example stems from the CPC case against Meta's "pay or consent" model started in 2023.[73] One of the claims raised in this case pertains to possible user confusion due to Facebook or Instagram apps forcing users to navigate through different screens and use hyperlinks sending users to different parts of their terms and conditions to discover how their personal data is used to personalise advertisements. Following the prohibition of deceptive online interface design, Article 25 of the DSA could now be invoked as well.

- **Ranking parameters for search results and recommender systems**: The DSA defines recommender systems as "a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed". As per the DSA Article 27, "Providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters." Furthermore, under Article 38 DSA, "In addition to the requirements set out in Article 27, providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679".

  The UCPD does not address recommender systems in the broad sense of the DSA but its Article 7(4a) UCPD requires traders, such as online platforms, that enable consumers to search for products offered by different traders (or consumers) on the basis of a search query, to provide consumers with information on the main parameters determining the ranking of search results.

  The two provisions overlap and complement each other. The UCPD provision requires stronger prominence for the information on search parameters. The DSA applies to all types of recommender systems, not only search parameters. This means that information on search parameters must be provided both in accordance with the UCPD (on the page where the search results are presented) and explained in the general T&Cs along with information on other recommender systems in accordance with the DSA.

  Accordingly, regarding the search parameters, platforms must comply with two complementary rules regarding the location and presentation of consumer information. Online platforms could face increased compliance burden having to duplicate the information about search parameters also in the T&Cs in addition to providing it directly on the search results pages

In sum, two overlaps have been identified, regarding dark patterns and recommender system transparency.

On dark patterns, Article 25 of the DSA prohibits manipulative design practices but explicitly excludes those already addressed by the UCPD (Articles 6 and 8), which is considered *lex specialis* and takes precedence in that area. Academic commentary and recent enforcement cases highlight the need for clearer guidance and coordination, as platforms may face parallel obligations. The DSA is intended to act as a "safety net" for dark patterns not covered by the UCPD, although without explicit clarification of the practices covered under the two legal instruments.

Regarding search ranking transparency, both the DSA (Article 27(1) and (2)) and UCPD (Article 7(4a)) complement each other, since the scope of DSA's obligations regarding recommender systems also covers the search parameters, whose transparency is specifically addressed by the UCPD.

[73] European Commission, 'Commission coordinates action by national consumer protection authorities against Meta on 'pay or consent' model'.

## Directive 2011/83/EU ([74]) – [Consumer Rights Directive]

*General Information*

The Consumer Rights Directive 2011/83/EU (CRD) of 25 October 2011 came into application on 13 June 2014. On 17 December 2021, the Commission adopted the current, updated CRD guidance - Commission Notice on the interpretation and application of the Consumer Rights Directive (hereinafter: "the CRD Guidance")([75]).

The Directive aims at achieving a high level of consumer protection by harmonising several key aspects of national legislation on contracts between consumers and traders and to facilitate the internal market, particularly for consumers buying, and traders selling, online. Its main focus is harmonising the traders' information obligations and the consumers' right of withdrawal. The Modernisation Directive (Directive (EU) 2019/2161), amended, among other consumer law directives, the CRD, to strengthen its enforcement and to update its rules in line with the market developments. Directive (EU) 2024/825 on empowering consumers for the green transition further amended the CRD to enhance consumer protection related to sustainability information. Finally, Directive (EU) 2023/2673 amended the CRD mainly to introduce provisions applicable to financial services contracts concluded at a distance.

*Personal scope*

The personal scope of the CRD is stipulated primarily in Articles 2 and 3. Article 3(1) establishes that the Directive applies to contracts concluded between traders and consumers concerning goods and services provided against remuneration, including contracts for water, gas, electricity, and heating. It applies to contracts for online digital content and digital services not only when they are provided to consumer against remuneration but also when the consumer provides personal data to the trader under the respective contract (Art. 3(1a)).

Pursuant to Article 2(1), a "consumer" is defined as any natural person who, in contracts covered by the Directive, acts for purposes outside his or her trade, business, craft, or profession. This definition imposes two cumulative conditions: first, the individual must be a natural person; second, the individual must be acting for non-professional purposes. The term "trader" is defined in Article 2(2) as either a natural or legal person acting for purposes related to their trade, business, craft, or profession, or acting in the name or on behalf of such a person. The definitions of both "consumer" and "trader" have been interpreted in case law of the Court of Justice of the European Union[76].

*Territorial scope*

In accordance with Regulation (EC) No 593/2008 (Rome I), which governs the applicable law for contractual obligations, the CRD applies where a trader established in a third country directs commercial activities towards consumers in one or more EU Member States[77]. Consequently, the CRD applies to both intra-EU transactions and transactions involving non-EU traders targeting EU consumers, thereby reinforcing consumer protection within the internal market.

---

[74] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[75] Commission notice Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights, *OJ C 525, 29.12.2021, pp. 1–85*, available at: https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive_en.

[76] For example, in *Kamenova* (C-105/17), *Tiketa* (C-536/20), *S.V.* (C-485/21), *YYY.* (C-570/21), *Pielatak* (C-410/23), *St Kliment Ohridski Primary Private School* (C-429/24).

[77] The CRD guidance, section 3.1.8.

*Material scope*

The material scope of the CRD covers any business-to-consumer ("B2C") contracts, with the exceptions specified in Article 3(3) CRD, e.g., gambling or healthcare contracts. If CRD provisions are in conflict with provisions of other EU legal acts governing specific sectors, the latter shall prevail as *lex specialis*, pursuant to Article 3(2) CRD.

The CRD imposes general pre-contractual consumer information obligations for contracts other than distance or off-premises contracts (Art. 5), and more detailed pre-contractual information requirements for distance and off-premises contracts (Art. 6), and additional information obligations for contracts concluded on online marketplaces (Art. 6a). Prior to contract conclusion, traders must provide clear and comprehensible information, amongst others, about their identity, product or service characteristics, payment terms, delivery, contract duration, and termination conditions. Article 6a addressed to providers of online marketplaces additionally require the disclosure of whether the supplier on the online marketplace is a trader or another consumer, information on the non-applicability of EU consumer protection rules when the supplier is not a trader, and explaining, where applicable, the allocation of contractual responsibility between the supplier and the online marketplace. The Directive also requires the traders to disclose the fact that the price they offer is personalised on the basis of automated decision-making (Art. 6(1)(ea)).

In case of distance or off-premises contracts, consumers have the right of withdrawal from the contract within 14 days (Art. 9), with certain exceptions (Art. 16). The CRD regulates how to exercise this right (Art. 11) and governs both the effects of withdrawal (Art. 12) and the respective obligations of traders (Art. 13) and consumers (Art. 14).

Chapter IV addresses other consumer rights, such as regarding delivery of goods (Art. 18) and prohibition of charging fees for the use of means of payment (Art. 19). It also regulates the passing of risk (Art. 20) and lays down specific provisions governing the post-contract communication by telephone (Art. 21).

*Enforcement*

Articles 23 and 24 CRD mandate Member States to ensure compliance and to establish penalties for infringements. Specifically, Member States must designate one or more competent bodies, such as public authorities, consumer or professional organisations, which are empowered to take actions before the national courts or the competent national authorities to enforce compliance with the CRD provisions (Art. 23). Accordingly, the Directive does not prescribe a uniform enforcement model, allowing Member States to assign enforcement powers to the courts and/or one or multiple administrative authorities as deemed appropriate under their national legal frameworks.

In contractual disputes concerning the CRD, the court jurisdiction is determined under Regulation (EU) 1215/2012 (Brussels I bis). According to Brussels Ibis Regulation, a consumer may bring proceedings against the trader either in the courts of the Member State in which the trader is domiciled or in the courts for the place where the consumer is domiciled, whenever the contract has been concluded with a trader who directs its activities to the Member State of the consumer's domicile. The DSA follows a country-of-origin principle, based on the Member State of establishment of the online intermediary services provider.

Member States must also lay down rules on effective, proportionate and dissuasive penalties for infringements of the Directive (Art. 24).

*Interactions with the DSA*

The CRD was adopted prior to the DSA and explicitly references the CRD in its Recitals 10, 72, 74. The DSA also establishes in Article 2(4)(f) that it 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 Union law on consumer protection and product safety, including Regulations (EU) 2017/2394 and (EU) 2019/1020 and Directives 2001/95/EC and 2013/11/EU. Article 3(2)

CRD provides that other EU legal provisions governing specific sectors, i.e. *lex specialis*, prevail in case of conflict with its provisions.

On **personal scope**, the DSA uses the notions of "consumer" and "trader" in the same meaning (Art. 3(c) and (f)) DSA) as the CRD, in accordance with the EU acquis. However, Recital 2 of the DSA clarifies that "consumers" are understood as only one of the categories of recipients of the service, resulting in a wider personal scope of application of the DSA, as it includes business-to-consumer (B2C), consumer-to-consumer (C2C) and business-to-business (B2B) relationships. "Trader" is defined by the CRD as any natural or legal person acting for business or professional purposes in relation to B2C contracts. The notion of "trader" includes the providers of "online marketplaces" which are defined in Article 2(17) of the Directive as services operated by or on behalf of a trader, allowing "*consumers to conclude distance contracts with other traders or consumers*". Therefore, the CRD applies to online marketplaces intermediating B2C or C2C contracts, but not to those intermediating solely B2B contracts and not engaging in B2C contracts. The notion of "online marketplace" in the CRD therefore is broader than the notion of "platforms allowing consumers to conclude distance contracts with traders" in Chapter III Section 4 of the DSA. On the other hand, Article 29(1) DSA provides that Chapter III Section 4 of the DSA does not apply to providers of online platforms that qualify as micro or small enterprises. The application of the CRD, by contrast and in particular of Article 6(a), is not subject to such an exemption. At the same time, the DSA also establishes relevant obligations on "online platforms" which also cover consumer-to-consumer relationships, but some of them also exempt small and micro enterprises.

The **territorial scopes** of the CRD and the DSA are similar. The CRD applies to both intra-EU and transactions involving third-country traders targeting EU consumers. Similarly, the DSA applies to intermediary services provided to recipients who are established or located within the EU, regardless of the service provider's place of establishment (Article 2(1) DSA). Therefore, both frameworks apply when consumers or users are located within the EU, including when external actors target the EU market.

With regards to **material scope**, significant part of the CRD provisions (e.g. Art. 6, 6a, 8, 9) applies to distance contracts, including distance contracts for the supply of digital content and digital services. The term "distance contract" is defined in the DSA (Art. 3(l) DSA) by referring to the definition under the CRD (Art. 2(7)), suggesting that both legal instruments apply at least to an extent to the same transactions. The CRD explicitly includes contracts for the supply of digital services and digital content within its scope (Art. 3(1a)). A "digital service" is defined in Art. 2(16) CRD by reference to Art 2(2) Directive (EU) 2019/770, and includes services that allow the consumer to "create, process, store or access data in digital form" as well as services that allow the "sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service". Consequently, B2C distance contracts concluded by providers of intermediary services as defined in Art 3(g) DSA fall within the CRD's scope.

On a more granular level, the CRD sets out information requirements that any distance trader must provide to consumers before they are bound by a distance contract (Art. 6 CRD). Moreover, both the CRD (in particular its Article 6a) and the DSA (in particular Section 4 of its Chapter III) set out certain information requirements for online marketplaces / online intermediary service providers allowing consumers to conclude distance contracts with traders. Specifically, when consumer concludes a contract on an online marketplace, its provider must inform the consumer, where applicable, how the contractual responsibilities are shared between the third-party trader and the provider of the online marketplace, pursuant to Article 6a(1) (d) of the CRD. Additionally, Article 6a(1)(b) and (c) of the CRD require the provider of the online marketplace to convey to consumers information on whether the third party offering the goods, services or digital content is a trader or not. Provision of this information is based on the declaration of the third-party suppliers to the online marketplace, which the provider of the online marketplace must accordingly collect from the suppliers that it hosts.

The DSA similarly requires providers of online platforms allowing consumers to conclude distance contracts with traders, to obtain certain information from a trader prior to the use of their service (Art. 30(1) DSA), and to make this information available on its platform, in a clear, easily accessible and comprehensible manner (Art 30(7) DSA).

There is, accordingly, a partial overlap. On the one hand, the CRD applies also to online marketplaces facilitating the conclusion of C2C transactions (not covered under DSA) and therefore requires also such marketplace providers to inform consumers about the non-professional character of their contractual counterparty. On the other hand, the information obligations under the DSA do not apply to micro or small enterprises (Art. 29 DSA). Further, the DSA seems to be more prescriptive in terms of the information that the online platform is required to obtain.

A further interlink exists with the compliance by design obligation of the provider of the online platform as set out in Art 31 DSA, which requires the provider to "ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information", such as the ones set out in Art 6 CRD. The DSA complements here the CRD. The obligations derived from Article 6a CRD remain applicable also to online marketplaces that fall outside of the scope of Article 31 DSA, namely, platforms qualifying as micro or small enterprises that are excluded from the scope of chapter III, section 4 of the DSA under its Article 29.

Additionally, Art. 6a(1)(a) CRD requires online marketplaces to provide information on the **main parameters used to determine the ranking of products and services** in search results. Such information must be made available in a specific section of the online interface that is directly and easily accessible from the page where the offers are presented. In this area, Art 27(1) DSA specifies that providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their **recommender systems**. The interplay between these two provisions is further discussed below in the overlap section.

Lastly, Article 6a(2) CRD prescribes that, without prejudice to Directive 2000/31/EC, Member States are not prevented from imposing additional information requirements for providers of online marketplaces, provided such rules are proportionate, non-discriminatory, and justified on grounds of consumer protection. However, Recitals 9 and 10 DSA provide important clarifications regarding the scope for Member States' intervention in this area.

Recital 9 explicitly states that Member States should not adopt or maintain additional national requirements relating to matters falling within the scope of the DSA, reflecting the full harmonisation effect intended by the Regulation. Recital 10 further elaborates that where other Union legal acts pursue the same objectives as the DSA, the DSA's rules apply to issues not fully addressed by those acts, as well as to issues where those acts allow Member States some discretion. This means that the DSA establishes a harmonised baseline that precludes the adoption of further national measures in areas covered by the DSA, even if other EU legislation permits minimum harmonisation or limited national discretion.

Importantly, Recital 10 covers not only aspects directly regulated by the DSA but also those where other EU legislation empowers Member States to go further. This ensures that the DSA's full harmonisation effect prevents fragmentation of legislation on intermediary services pursuing the same objectives, such as consumer protection. Consequently, while Article 6a(1) CRD is complementary to the specific obligations under the DSA, Article 6a(2) CRD's open clause does not grant Member States unlimited authority to impose additional information requirements on online marketplaces that would undermine the DSA's harmonised framework.

With regards to **enforcement**, as a consumer law instrument, the CRD is enforced by national authorities and courts in the Member States. In cross-border cases, national consumer authorities cooperate and coordinate their enforcement actions in the CPC Network in accordance with the cooperation mechanism established by the CPC Regulation. The DSA establishes a specific public enforcement framework for the enforcement of online intermediaries' obligations under the DSA. That public enforcement framework is distinct and separate from the public enforcement framework for consumer law. On the other hand, the DSA establishes an enforcement framework based on where the intermediary service/trader is established ("country of origin" logic), whilst the CRD is mainly focused where the affected consumers reside

*Special remarks on overlaps*

There are some overlaps that merit a detailed analysis:

- **Information obligations about ranking parameters for search results (CRD) and recommender system transparency (DSA)**: Article 6a(1)(a) CRD specifies that before a consumer is bound by a distance contract, or any corresponding offer, on an online marketplace, the provider of the online marketplace shall provide the consumer - in a clear and comprehensible manner and in a way appropriate to the means of distance communication - with general information on the main parameters determining ranking of offers presented to the consumer as a result of the search query and the relative importance of those parameters as opposed to other parameters. Such information must be made available in a specific section of the online interface that is directly and easily accessible from the page where the offers are presented.

  Article 27(1) DSA on recommender system transparency specifies that providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters. As per Art. 27(2) DSA these parameters shall explain why certain information is suggested to the recipient of the service and should include, at least: (a) the criteria which are most significant in determining the information suggested to the recipient of the service; (b) the reasons for the relative importance of those parameters. ([78])

  There is accordingly an overlap of information obligations for online marketplaces in this case. A question could arise whether the provider of an online marketplace providing information on the recommender systems in its terms and conditions, as required by Art. 27(1) DSA, also complies with the obligation under Art. 6a(1)(a) CRD to provide information about the search parameters (as an element of recommender systems) in a "specific section of the online interface that is directly and easily accessible from the page where the offers are presented".

  Pursuant to Articles 2(4) DSA and 3(2) CRD, where a DSA provision is more specific than that of the CRD and there is a conflict between them, the DSA shall prevail. However, where there is no conflict, both overlapping obligations can remain applicable, and both legislations can coexist. In the case at hand, the two provisions overlap and complement each other. The CRD provision requires stronger prominence for the information on search parameters. The DSA applies to all types of recommender systems, not only search parameters. Accordingly, regarding the search parameters, platforms must comply with two complementary rules regarding the location and presentation of consumer information. Consequently, online platforms could face increased compliance burden having to duplicate the information about search parameters also in the T&Cs in addition to providing it directly on the search results pages

- **Information obligations about single point of contact**: Further complexity arises in the relationship between Article 6 of the CRD and Article 12 of the DSA, with the latter requiring providers of intermediary services "*to make public the information necessary for the recipients of the service to easily identify and communicate with their single points of contact*", in addition to the obligations provided under Directive 2000/31/EC. This provision was added at the request of the European Parliament precisely to reinforce the protection of consumers in an intermediated environment. The complexity arises because the DSA states that its obligations apply "in addition to" the E-Commerce Directive, the E-Commerce Directive applies "in addition to other Community law (Article 1(3)), which includes the CRD, while the more specific provisions of DSA or e-Commerce Directive will prevail over those of the CRD in case of conflict (Article 3(2)). This layering creates ambiguity regarding the hierarchy and interaction of information obligations, particularly if intermediary service providers act as traders in B2C contracts governed by the CRD.

  The two provisions complement each other. On the one hand, Article 12(1) DSA establishes the obligation for online intermediaries to set a user-friendly electronic point of contact and Article 12(2) establishes that

[78] In addition to the requirements set out in Article 27, providers of very large online platforms and search engines that use recommender systems must offer at least one option for each system that does not use profiling, as defined in Article 4(4) of Regulation (EU) 2016/679.

this information should be made public, easily accessible and up to date, and it applies "in addition to the obligations provided under Directive 2000/31/EC". On the other, Article 6(1)(c) CRD requires traders to provide consumers with information about their geographical address and electronic mail and telephone number in a clear and comprehensible manner before the conclusion of the contract, to enable the consumer to contact the trader quickly and communicate with the trader efficiently. This requirement also applies to contracts concluded with consumers by online intermediaries in their role of traders that fall within the scope of the CRD. This overlap can be addressed by interpreting the CRD information requirement as *lex specialis* to the e-Commerce Directive since the CRD information requirement is more specific. Accordingly, this CRD requirements applies also "in addition" to Article 12(2) DSA.

This means that DSA and CRD information requirements apply in a complementary manner. Under the CRD, the online intermediary that enters into contract with the consumer must provide information about its address and contact details at the pre-contract stage whilst under the DSA the intermediary must display its contact details throughout the consumer's use of the platform.

In sum, as explained above, there are adjacent requirements in the CRD and DSA regarding information that online marketplaces must collect from the suppliers whose offers they host, information about ranking parameters for search results and recommender systems, and information regarding contact details.

# Regulation (EU) No 1215/2012 – [Brussels Ia Regulation]

*General Information*

Regulation (EU) No 1215/2012[79] ('the Brussels Ia Regulation') was adopted on 12 December 2012 and became applicable from 10 January 2015 onwards, except for its Articles 75 and 76 which applied from 10 January 2014 onwards. It replaced Regulation (EC) No 44/2001 ('Brussels I Regulation)', which continues to apply to judgments given in legal proceedings instituted, to authentic instruments formally drawn up or registered and to court settlements approved or concluded before 10 January 2015 which fall within its scope.[80] As established under Article 79 Brussels I (recast), the European Commission adopted a Report on the application of the Regulation on, 2 June 2025.[81]
The Brussels Ia Regulation seeks to facilitate access to justice, particularly by setting out clear, EU-wide and directly applicable rules on jurisdiction and on the recognition and enforcement of judgments in civil and commercial matters. Its objective is to promote the free circulation of judgments within the Union and to create uniform rules governing international jurisdiction and the recognition and enforcement of judgments in order to avoid obstacles to the efficient operation of the internal market.

*Territorial and material scope*

The Brussels Ia Regulation applies in civil and commercial matters whatever the nature of the court or tribunal and to "any judgment given by a court or tribunal of a Member State, whatever the judgment may be called, including a decree, order, decision or writ of execution, [a][82], [as well as] provisional, including protective, measures ordered by a court or tribunal which by virtue of this Regulation has jurisdiction as to the substance of the matter."[83]

The Regulation, as amended in 2014, has been applied since 10 January 2015 between all Member States, including Denmark[84].

The Brussels Ia Regulation governs the international jurisdiction of courts and enforcement of judgements in cross-border civil and commercial cases. The Regulation establishes specific provisions on jurisdiction in matters involving weaker parties, such as those relating to insurance (Section 3), jurisdiction over consumer contracts (Section 4) and jurisdiction over individual contracts of employment (Section 5). The Regulation also provides rules on the recognition and enforcement of judgements across EU Member States. For the purposes of facilitating recognition and enforcement it establishes two types of certificates: one for judgements (Article 53) and another one – for authentic instruments or court settlements (Articles 58, 60).

---

[79] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast); OJ L 351, 20.12.2012, p. 1–32.
[80] Judgments in civil and commercial matters - Brussels I Regulation. European Justice Portal. Available at: https://e-justice.europa.eu/topics/taking-legal-action/european-judicial-atlas-civil-matters/judgments-civil-and-commercial-matters-brussels-i-regulation_en#:~:text=Council%20Regulation%20%28EC%29%20No%2044%2F2001%20of%2022%20December,enforcement%20of%20judgments%20in%20civil%20and%20commercial%20matters%29. Last accessed on 17 July 2025.
[81] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast); COM(2025)268, 02.06.2025.

[83] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast); OJ L 351, 20.12.2012, p. 1–32, Article 2(a).
[84] Denmark applies the Regulation in line with the Agreement of 19 October 2005 between the European Community and Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 299, 16.11.2005, p. 62.

Article 1(2) of the Brussels Ia Regulation excludes certain civil and commercial matters from the scope of its application. Such matters include, amongst others, bankruptcy, proceedings relating to the winding-up of insolvent companies or other legal persons, judicial arrangements, compositions and analogous proceedings.

*Recognition and enforcement*

The Brussels Ia Regulation governs recognition and enforcement of judgments related to civil and commercial matters within the Union. Article 36(1) establishes that a judgment given in a Member State shall be recognised in the other Member States without any special procedure being required, while Article 39(1) specifies that a judgment given in a Member State which is enforceable in that Member State shall be enforceable in the other Member States without any declaration of enforceability being required.

*Interactions with the DSA*

The Brussels Ia Regulation does not contain any reference to DSA provisions in its text. By contrast, the DSA refers to Brussels Ia Regulation in its recitals and provisions.

First, First, Recitals 10 and 34, together with Article 2(4)(h) of the DSA, clarify that, as a matter of principle, the DSA does not alter the existing EU rules on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, the law applicable to contractual and non-contractual obligations, or judicial cooperation in civil matters. This follows the approach already taken in Article 1(4) of the ECD, which similarly excluded matters of private international law from its scope. However, Recital 8 of the DSA shows that in some cases DSA relies on notions in the EU private international law instruments. More concretely, for the purposes of establishing a "substantial connection", i.e., determining the territorial scope of the DSA. Article 17(1)(c) of the Brussels Ia Regulation could also be relied on and "a substantial connection' should also be assumed where a service provider directs its activities to one or more Member States within the meaning of Article 17(1)(c) of the Brussels Ia Regulation.

On **material scope,** the Brussels Ia Regulation establishes rules on jurisdiction and recognition and enforcement of judgments in civil and commercial matters. Therefore, when a civil or commercial dispute arises over a DSA obligation, for example between a consumer and an online intermediary service provider, or any other contractual dispute where there is a cross-border element, Brussels Ia Regulation determines the courts of which Member State have jurisdiction and thus can issue judgments, including certain orders under the DSA Articles 9 and 10 . and thereby ensure such orders can be recognised and enforced in another Member State.

*Special remarks on interplay*

Overall, the main interaction between the DSA and Brussels Ia Regulation consists in the fact that when a civil or commercial dispute arises following an alleged breach by a provider of an online intermediary service of DSA provisions, the Brussels Ia Regulation helps determining the courts of which Member State have jurisdiction. Another possible interplay between the DSA and the Brussels Ia Regulation concerns the recognition and enforcement of orders to act against illegal content (Article 9 DSA) and orders to provide information (Article 10 DSA) where these orders concern civil and commercial matters. Where such orders are 'judgments' within the meaning of Article 2(a) Brussels Ia Regulation, their cross-border enforcement and recognition is governed by the rules of Brussels Ia Regulation.

Articles 9 and 10 of the DSA lay out provisions on how service providers must respond to orders to act against illegal content and to provide information respectively. These provisions regulate the form and execution of such orders, but not the rules on jurisdiction to issue them or for their cross-border recognition, as clearly stated in Recital 31, which means that Brussels I Regulation fills this legal gap by setting out the rules on international jurisdiction, and subsequent cross-border enforcement of judgments issued by a competent court. As is clear in Recital 32, the DSA offers the legal basis for enforcing of the obligation *to inform the relevant authorities about the effect given* to Article 9 and 10 orders, as opposed to the enforcement of the orders themselves. The court competent to issue orders under Articles 9 and 10 DSA should be determined in accordance with the applicable rules on jurisdiction in national law, when those orders cover administrative matters, or in the Brussels Ia

Regulation, when they concern civil and commercial matters. The same rules should apply for the cross-border recognition and enforcement of such orders. For this reason, Recital 32 DSA defers the regulation of matters of cross-border enforcement and recognition of Article 9 and 10 orders to Brussels Ia Regulation rules when it comes to civil and commercial matters.

To conclude, the relationship between the DSA and the Brussels Ia Regulation is one of complementarity. While the DSA creates substantive obligations for intermediary services and empowers national authorities to issue binding orders under Articles 9 and 10, it does not regulate jurisdiction or cross-border recognition and enforcement of judgments in cross-border disputes over civil and commercial matters. These procedural questions are governed by Brussels Ia Regulation.

## Regulation (EU) 2015/2120 ([85]) – [Open Internet Regulation]

*General Information*

The Open Internet Regulation (OIR, also known as the Net Neutrality Regulation) was adopted in November 2015, and is applicable since 30 April 2016. The OIR has been amended on three occasions since its adoption

In line with Article 9, the next review (focused on Articles 3-6 only) should take place by 30 April 2027. The last OIR implementation report was published in April 2023.[86]

As per Article 1, the OIR has two key aims: (i) to establish common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights – Article 1(1); and (ii) to abolish retail roaming surcharges – Article 1(2). Only the obligations related to the first objective (the 'open internet provisions') are relevant in the context of the DSA.

The Open Internet Regulation (OIR), which has been applicable in all EU Member States since 30 April 2016, enshrines the open internet principle. The Regulation grants end-users the directly applicable right to access and distribute lawful content and services of their choice via their internet access service. It enshrines the principle of net neutrality: internet service providers must treat all internet traffic without discrimination, blocking, throttling or prioritisation. The end-users' rights cannot be limited by virtue of commercial agreements between them and their internet service providers, or by traffic management practices undertaken by the providers. The principle of the open internet has been included in the European Declaration on Digital Rights and Principles, which shows its continuing importance in the EU.

*Personal scope*

The OIR places requirements on providers of internet access services, which are defined in Article 2 as a "publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used". Additionally, Recital 5 of OIR provides additional explanation that '(…) However, for reasons outside the control of providers of internet access services, certain end points of the internet may not always be accessible. Therefore, such providers should be deemed to have complied with their obligations related to the provision of an internet access service within the meaning of this Regulation when that service provides connectivity to virtually all end points of the internet. Providers of internet access services should therefore not restrict connectivity to any accessible end-points of the internet.'

*Territorial scope*

The OIR applies to providers of internet access services to end-users in the EU/EEA.

*Material scope*

The OIR regulates the open internet by establishing rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights – Article 1(1). This is primarily done through provisions on:

---

[85] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

[86] Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120

- Safeguarding open internet access (Article 3), which: (1) establish the rights of end-users, including the right to access and distribute lawful content, applications and services and freedom of choice regarding devices and services; (2) ensure end-user rights are protected in commercial agreements; (3) set rules on traffic management; (4) address protection of personal data; and (5) permit the provision of specialised services that require enhanced quality, but not at the expense of general internet access quality.
- Transparency measures (Article 4), which require providers of internet access services to provide certain information and establish complaint management procedures.

*Enforcement*

Supervision and enforcement is governed by Article 5. National regulatory authorities (NRAs) in each Member State are tasked with closely monitoring and ensuring compliance with Articles 3 and 4, and promoting open internet access. They may impose requirements in that regard on providers and shall publish reports annually – Article 5(1). Under Article 5(2), NRAs have the power to require information relevant to the obligations set out in Article 3-4 from providers of electronic communications to the public (including providers of internet access services). To support consistent application of OIR, BEREC was tasked to issue guidelines for the implementation of the obligations of NRAs national regulatory authorities under Article 5.[87] Penalties are established by Member States in accordance with Article 6 and notified to the Commission.

*Interactions with the DSA*

As the OIR was adopted 10 years ago (2015), it includes no references to the DSA. It also does not contain any reference to the e-commerce Directive (2000/31/EC). However, regarding supervision and enforcement in Article 5 it includes as 'without prejudice clause', which provides that it is without prejudice to the tasks assigned by Member States to the national regulatory authorities or to other competent authorities in compliance with Union law e.g. stemming from DSA or the European Electronic Communications Code (EECC).

The DSA does not contain any references to the OIR.

On **personal scope**, the DSA interplay partially and to the extent that the EECC or other Union legal acts do not contain more specific provisions applicable to electronic communications services (internet access services are only one type of electronic communications services as per Art. 2 (4) (a) EECC), although different terminology is used as explained below.

The OIR applies to providers of internet access services, as defined above. Such a service could qualify as a 'mere conduit' service under the DSA – i.e. a service, "consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network" (Article 3(g)(i)).[88]

The "mere conduit" role is only one category of intermediary service under the DSA. Depending on its activities and the degree of control over transmitted data, an ISP does not always act as a mere conduit. An ISP is not a mere conduit when it goes beyond being a neutral, passive role of a transmitter of signals - for instance, when it alters or filters traffic, prioritises some content over others, stores or hosts content, or provides its own content services (e.g., ISP owns streaming platform, news service or provide cloud services). An ISP is not a mere conduit e.g. when it initiates the transmission (instead of just carrying what the user requests), selects or determines the recipient of the transmission, selects, modifies, or interferes with the information being

[87] See: BEREC, (2022) BEREC Guidelines on the Implementation of the Open Internet Regulation: BEREC Guidelines on the Implementation of the Open Internet Regulation

[88] See also Case C- 70/10, Scarlet Extended SA, 24 November 2011

transmitted or stores information for purposes beyond the transient technical transmission (that would fall under caching or hosting). In short, an ISP is not a mere conduit when it goes beyond being a neutral, passive transmitter of signals.

It follows that these definitions are not in conflict but overlap depending on the scope of activities of ISP as defined under OIR. An ISP's status as a mere conduit varies according to the nature of its activities and the level of control it exercises over the data it transmits (this approach was also explained in the Recital 10 EECC[89]).

With regards to **territorial scope**, both legal acts apply to the provision of services to users that are based in the EU/EEA; however, whereas the DSA specifically provides rules for territorial application (Article 2(1)), the OIR does not explicitly address its territorial application.

On **material scope**, while both Regulations aim to achieve similar objectives – e.g. safeguarding user (end-users for OIR) rights online – their core material scope is focused on different elements of internet governance. The DSA establishes a framework for conditional liability exemptions and imposes tiered due diligence obligations on providers of intermediary services concerning content, design and functioning of their services. In contrast, the OIR focuses on network-level treatment of traffic, enshrining the principle of net neutrality. This distinction is explicitly recognised in Articles 3(1) and (3) of the OIR, supplemented by Recitals 6 and 10-15.In establishing end-users' rights related to content, applications, services, and terminal equipment, Article 3(1) OIR states that 'this paragraph [on end-user rights] is without prejudice to Union law, or national law that complies with Union law, related to the lawfulness of the content, applications or services'.

Article 3(3) OIR complements this, establishing that 'internet access services shall treat all traffic equally' and, while permitting reasonable traffic management measures, it specifically notes that '[traffic management] measures shall not monitor the specific content' and 'shall be transparent, non-discriminatory and proportionate'. This is further supplemented by: Recital 6, which explicitly states that 'this Regulation does not seek to regulate the lawfulness of the content, applications or services, nor does it seek to regulate the procedures, requirements and safeguards related thereto'; Recital 10, which specifies that 'reasonable traffic management does not require techniques which monitor the specific content'; and Recital 11, which prohibits 'any traffic management measures which go beyond such reasonable traffic management measures' including blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services'.

However, the OIR does stipulate 'justified and defined exceptions' to this prohibition. Article 3(3) does provide for three exceptions where providers can go 'beyond such reasonable traffic management measures' (as explained further in Recitals 12-15). These include:

- Compliance with Union legislative acts or national legislation (and related measures implementing them). As stipulated in Recital 13, such legislation or measures must comply with the requirements of the Charter of Fundamental Rights of the EU. Orders to act against illegal content, as governed by Article 9 of DSA, could be the basis for the use of this exception, which would represent a complementary point of interplay between the two legal instruments.

---

98 'Certain electronic communications services under this Directive could also fall within the scope of the definition of 'information society service' set out in Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council. The provisions of that Directive that govern information society services apply to those electronic communications services to the extent that this Directive or other Union legal acts do not contain more specific provisions applicable to electronic communications services. However, electronic communications services such as voice telephony, messaging services and electronic mail services are covered by this Directive. The same undertaking, for example an internet service provider, can offer both an electronic communications service, such as access to the internet, and services not covered by this Directive, such as the provision of web-based and not communications-related content.'

- Preserving the integrity and security of the network, services or terminal equipment – for instance, to address attacks and threats such as hacking against network components or distribution of malicious software.[90] This is supported by Recital 14 of the OIR, Directive 2002/58/EU (e-privacy) and NIS2 Directive.

- Preventing impending network congestion or mitigating its effects. This is supported by Recital 15 of the OIR.

In line with the provisions of Article 3(3), the OIR also places explicit transparency obligations on providers of internet access services. Article 4(1) stipulates that such providers 'shall publish' and 'shall ensure that any contract which includes internet access services' includes information on traffic management. This is supplemented by requirements for establishing complaint-handling procedures in Article 4(2) OIR.

On the other hand, the DSA also establishes rules related to restrictions imposed by intermediary services – including 'mere conduit' services – on the use of their services, which could include traffic management measures. The DSA does not govern the legality of such restrictions, but it does set out transparency obligations should such (lawful) restrictions be implemented – Article 14 mandates that providers of intermediary services provide information in their Terms and Conditions on such restrictions; and Article 15 stipulates the need for public reporting on such restrictions (Article 15(1)(c)) if a provider engages in own-initiative content moderation.

These DSA transparency requirements complement the core OIR provisions on traffic management, but they remain distinct when an ISP does not act as mere conduit. Specifically, a provider of internet access services must provide information on traffic management to end-users through its contracts and publish it (under the OIR) and 'mere conduit' are obliged to provide similar information on 'restrictions' in their terms and conditions and, where relevant, annual transparency reporting (under the DSA). When this information is already publicly available, for example through terms and conditions, the obligations under the DSA and OIR do not conflict or duplicate each other.

Regarding the **enforcement**, the two laws implement similar enforcement structures, characterised by supervision and enforcement through national authorities (NRAs under OIR and DSCs under DSA), supplemented by EU level coordination (BEREC under OIR and the European Board for Digital Services (EBDS) under the DSA). The OIR also empowered BEREC to issue guidelines in close cooperation with the Commission on the obligations of the NRAs to monitor and ensure compliance with the provisions on open internet.[91]

While the DSA also foresees a supervisory function of the European Commission, this does not concern mere conduit providers, which are supervised at the MS levels. Within this context, the powers of these national authorities can intersect, as they may supervise and enforce against some of the same types of service providers. As such, they could impose similar enforcement measures (e.g. imposing requirements, information requests) in parallel. For instance, Article 5(1) OIR provides NRAs with the power to "impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures" and Article 5(2) OIR provides the basis for NRAs to request information from providers relevant to their obligations under Articles 3 and 4 OIR. Article 51 DSA provides DSCs with the power to require information 'relating to a suspected infringement of this Regulation' (a placeholder to explain DSA related details). However, the nature of the activities they are supervising and enforcing against differ significantly. Digital Services Coordinators under DSA have not only investigatory powers to require information from providers and related parties, but also request inspections of premises, and obtain explanations from staff or representatives to detect or address suspected infringements of the DSA within their Member State. Both types of authority also have public reporting obligations (Article 5(1) OIR foresees yearly reporting by NRAs on the monitoring and application of Art. 3 and 4, and Article 21(4), 35(2), and 55 DSA.

[90] BEREC, (2022) BEREC Guidelines on the Implementation of the Open Internet Regulation.
[91] BEREC published the first version of the guidelines in August 2016 and updated them in 2020 and 2022.

In addition, the DSA explicitly empowers DSCs to ensure cooperation at national level with other competent national authorities (NRAs under OIR included) to streamline supervision and enforcement (Article 49(2) as regards general cooperation; Article 53 as regards the right to lodge a complaint; supplemented by Article 57(2) on mutual assistance).

These enforcement mechanisms are thus not in conflict (parallel concurrent application).

*I. Special remarks on interplay*

While the same types of entities may be subject to both the laws, the interplay between the material scope of the two instruments is complementary – i.e. between orders to act against illegal content under Article 9 DSA and the exception to reasonable traffic management measures in Article 3(3) OIR, and between the DSA transparency requirements (Article 14 and 15) and the core OIR provisions on transparency measures for ensuring open internet access.

## Regulation (EU) 2016/679([92]) – [General Data Protection Regulation]

*General Information*

The GDPR was adopted on 27 April 2016, entered into force on 24 May 2016 and became applicable on 25 May 2018. The Commission published the first report on the application of the GDPR on 24 June 2020 and the second report on 25 July 2024. On 4 July 2023, the Commission adopted a proposal for a regulation on GDPR procedural aspects on which the Council and European Parliament reached a provisional agreement on 16 June 2025.

The main objectives of the GDPR are to protect personal dataand ensure the free movement of personal data within the EU by creating a harmonised set of rules applicable to all personal data processing by organisations (regardless of their size and whether they are public or private) established in the European Economic Area or targeting individuals in the EU.

The GDPR is adopted pursuant Article 16 TFEU, which mandates to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of such data. Compliance with these rules is subject to the control of independent authorities. The GDPR is further based on Article 8 of the Charter of the European Union, that lays down the fundamental right to personal data protection.

*Personal scope*

According to Article 1, the GDPR's personal scope encompasses natural persons as data subjects, with the overarching aim of harmonising data protection standards to uphold their rights throughout the EU. The Regulation lays down rules to safeguard the fundamental rights and freedoms of natural persons, particularly their right to the protection of personal data. Moreover, the GDPR seeks to ensure the free movement of personal data within the European Union, prohibiting any restrictions or prohibitions on such movement for reasons connected with the protection of natural persons with regard to the processing of their personal data.

Article 3 defines the GDPR's territorial scope. Firstly, the GDPR applies to the processing of personal data carried out in the context of the activities of an establishment of a controller or processor within the EU, irrespective of whether the actual processing occurs within or outside the EU. Secondly, the GDPR also covers processing of personal data of data subjects who are located in the EU by controllers or processors not established in the EU, provided that such processing is related either to the offering of goods or services to these data subjects within the EU, regardless of payment, or to the monitoring of their behaviour within the EU (typically, online). Finally, the Regulation applies to processing by a controller not established in the EU but situated in a location where Member State law applies under public international law.

*Material scope*

The GDPR's material scope, as set out in Article 2, applies to the processing of personal data by automated means and to non-automated processing forming part of a filing system or intended to do so. The Regulation is also without prejudice to Directive 2000/31/EC, in particular the liability rules for intermediary service providers (Art. 2(4)). The GDPR expressly excludes certain categories of processing from its scope. These exclusions include processing activities that fall outside the scope of Union law, processing carried out by Member States in exercising their responsibilities under Chapter 2 of Title V of the Treaty on European Union (TEU), and processing by natural persons for purely personal or household activities. For processing conducted by Union institutions and bodies, Regulation (EU) 2018/1725 applies, which is aligned with the GDPR's principles.

[92] Regulation (EU) 2016/679 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 (General Data Protection Regulation).

*Enforcement*

The enforcement mechanism of the GDPR is primarily governed by Chapters VI, VII and VIII (Articles 51 to 84). Chapter VI sets out the roles and powers of supervisory authorities in each Member State. Article 51 requires each Member State to establish one or more independent public authorities, known as supervisory authorities, responsible for monitoring the application of the GDPR to protect fundamental rights in relation to data processing. These authorities are empowered under Article 57 to perform a range of tasks, including conducting investigations, handling complaints, and promoting public awareness.

Article 58 confers extensive investigative and corrective powers upon supervisory authorities, such as the ability to carry out investigations in the form of data protection audits (Art. 58(1)(b)), issue warnings (Art. 58(2)(a)), reprimands (Art. 58(2)(b)), orders to comply with data subjects' requests to exercise their rights in conformity with the Regulation (Art. 58(2)(c) and impose a temporary or definitive limitation including a ban on processing (Art. 58(2)(f)). Moreover, Article 58(2)(i) empowers supervisory authorities to impose administrative fines in accordance with Article 83, which provides for significant financial penalties for infringements, ensuring effective, proportionate, and dissuasive sanctions.

Chapter VII of the Regulation also establishes mechanisms for cooperation and consistency among supervisory authorities to ensure uniform enforcement across the Union (Articles 60 to 66). Article 68 creates the European Data Protection Board, which is tasked to ensure the consistent application of the Regulation (Art. 70). GDPR Chapter VIII contains the remedies, liabilities and penalties (Arts. 77 to 84), which allow data subjects to lodge complaints with supervisory authorities and seek judicial review of decisions.

*Interactions with the DSA*

There is no reference to the DSA under the GDPR. However, Article 2(4) GDPR lays down that "[the regulation is] without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive". According to Article 89 of the DSA, the aforementioned provision in Article 2(4) GDPR must now be read as referring to the liability rules provided for in the DSA.

The DSA directly refers to the GDPR in recitals (10), (34), (67), (68), (69), (71) and (94), as well as in Articles 2(4)(g), 25(2), 26(3), 28(2), 38, 40(8)(g) and 40(13).

Regarding the **personal scope**, where the provision of intermediary services involves processing of personal data, the GDPR will apply to such processing. Art 2(4)(g) DSA lays down 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 this Regulation". The case-law on the GDPR stresses the ubiquitous application of that instrument in all matters relating to the internal market. For matters outside the scope of the GDPR, i.e. other than protection of personal data and its free flow, such as intermediary exemption liability rules, the DSA prevails.

Due to the broad scope of the GDPR's definitions of "controllers" (Art. 4(7)) and "processing of personal data" (Art. 4(2)), any provider of an intermediary service covered by the DSA acts as a controller under the GDPR in relation to any processing of personal data for which they establish the means and purposes. Intermediaries might also be "processors" (Art. 4(8)) under the GDPR. The role of a provider in a specific situation must be assessed on a case-by-case basis.

When it comes to the **territorial scope**, the GDPR applies i.a. to the processing of personal data in the context of an entity not established in the Union offering goods or services to data subjects in the Union or monitoring their behaviour in the Union. Similarly, the DSA is applicable to intermediary services offered to recipients established or located in the Union, regardless of the location of the providers of those intermediary services (DSA Art. 2(1)).

With regards to the **material scope**, some elements need to be highlighted:

- **Intermediary liability exemption (Art. 2(4) GDPR):** The basic relationship between the DSA and the GDPR in relation to the intermediary liability exemption is clear: the GDPR rules are "without prejudice" to the rules on such liability exemption in the e-Commerce Directive, which are to be construed to refer to the DSA (Art. 2(4) GDPR) and, for its part, the DSA is without prejudice to the GDPR rules regulating other aspects of the provision of intermediary services in the internal market (Art. 2(4)(g) DSA).

- **Points of contact for recipients of the service (Arts. 13(1)(a) and (b) GDPR, Arts. 14(1)(a) and (b) GDPR and Art. 12 DSA):** The transparency obligations under the DSA and the GDPR have a different scope. Under the DSA, intermediaries only need to make the information related to their single point of contact a public, while under the GDPR controllers must provide the data subjects with information of the controller and of their representative identity and contact details, if any, and of the contact details of the Data Protection Officer, where applicable. The DSA and the GDPR are in this respect complementary.

- **Legal representatives (Art. 27 GDPR and Art. 13 DSA):** The duty to appoint a representative where there is no establishment in the EU is seemingly the same, despite the DSA referring to "legal representative" while the GDPR uses “representative”. The DSA expressly stipulates in Art. 13(5) that "[t]he designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union." The DSA also does not contain the exception foreseen in the GDPR for "occasional", low-risk processing of non-sensitive data (cf. Art. 27(2)(a) GDPR).

  The DSA legal representative's mandate is limited to "efficient and timely cooperation with the Member States’ competent authorities, the Commission and the Board" in relation to "compliance with and enforcement of decisions issued in relation to this Regulation". That is more limited than the GDPR representative who must be "mandated [...] to be addressed by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation". Given the different purposes of both instruments in relation to designated representatives, the DSA and the GDPR are in this respect complementary.

- **The DSA take-down obligation and the GDPR "right to be forgotten" (Art. 17 GDPR and Art. 16 DSA):** The notice and action mechanism under the DSA applies to "illegal content", whereas the "right to erasure (or “right to be forgotten") requires "erasure" of personal data for a range of reasons, only some of which imply some illegality, i.e. that "the personal data have been unlawfully processed" (Art. 17(1)(d)), or that "the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject" (Art. 17(1)(e)). Article 17 GDPR applies only to that information for which the provider of an online intermediary service is considered controller. Obligation to erase personal data pursuant to Article 17 GDPR applies irrespectively if this article is invoked by the data subject or not if the condition of 17(1) GDPR is met. In practice, intermediaries who are subject to both the DSA and the GDPR will have to comply with both the notice and action mechanism of the DSA and the "right to erasure" under the GDPR.

- **Prohibition on profiling using special categories of personal data (Art. 4(4), Art. 9(1) and Art. 22 GDPR and Art. 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), GDPR using special categories of personal data referred to in Article 9(1) of said Regulation. The presentation of advertisements covered by Article 26 DSA might depending upon the particular characteristics of the case fall within the scope of automated individual decision making and profiling that fulfil the criteria of Article 22 GDPR. Article 22(1) GDPR prohibits the taking of decisions based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her, except in three special cases (consent, contract or law). Further, as per Article 22(4) GDPR, such decisions shall not be based on special categories of personal data, unless they fall under two exemptions (consent, necessary for reasons of substantial public interest based in law)In those cases "suitable measures" must be taken "to safeguard the data subject's rights and freedoms and legitimate interests". The DSA prohibits the

"presentation of adverts" on the basis of profiling using special categories of personal data, regardless of whether it involves decisions covered in Art. 22 GDPR and does not permit derogations.

The European Data Protection Board has issued guidelines on automated decision-making, including profiling, and targeting social media users to aid interpretation.[93] Intermediaries that are subject to the DSA and the GDPR should comply with both the GDPR requirements and take into account the interpretation of the GDPR notions used in the DSA as clarified in CJEU case-law when complying with the prohibition on the "presentation of advertisements" based on special categories of personal data in the DSA. They must take into account that the Court has stressed that personal data should be considered as falling within the categories listed in Art. 9(1) GDPR, not just when those characteristics are explicitly and directly used, but also when they can be "inferred"; and that the GDPR rules apply, not just to the end-result (the "presentation of the adverts") but also to the underlying processing and profiling leading to that result. The DSA and the GDPR are in this respect complementary, with extensive EU and Member State level case-law and guidance on the GDPR.

- **Transparency about advertising (Art. 5(1)(a), Arts. 13-14, subject to Art. 12 (modalities) GDPR and Art. 26(1)(d) and Recital 68 DSA):** The DSA requirements on the provision of "meaningful information" about "the main parameters used" in placing adverts should be interpreted in line with the GDPR, that requires to inform what categories of personal data are used and for which purpose, such as the case of advertising, and provide this information in a concise, transparent, intelligible and easy accessible form. The DSA and the GDPR are in this respect complementary.

- **Risk assessment (Art. 35(1)-(11) GDPR and Art. 34(1)-(3) DSA):** The DSA requires VLOPs and VLOSEs to conduct annual risk assessments identifying systemic risks arising from their service design and functioning, including algorithmic systems, at least once a year (Art. 34 DSA). As controllers, these entities are also subject to the obligation to carry out a Data Protection Impact Assessment (DPIA) prior to the processing, as per Art. 35 GDPR, particularly if automated processing, such as profiling or personalised advertising, is likely to pose high risks to individuals' rights and freedoms. The DSA mandates the inclusion of four systemic risks in the assessment: dissemination of illegal content; impacts on fundamental rights including privacy and data protection; effects on civic discourse, elections, and public security; and harms related to gender-based violence, public health, minors, and mental well-being.

  Both DSA risk assessments and GDPR DPIAs require evaluation of risks to individuals and implementation of mitigation measures. The EDPB has published guidelines on how to conduct DPIAs[94]. Any risk of discriminatory outputs or outcomes of the processing involved in the matters to be examined in a DSA risk assessment might be regarded as at least potentially a systemic risk. While the DPIA focuses on risks to fundamental rights prior to the envisaged data processing, the DSA's scope is broader, addressing systemic risks also beyond fundamental rights. However, the assessments overlap where personal data processing is involved, and DPIAs can inform the DSA's risk assessments. Both engagement with supervisory authorities. Overall, the DSA and GDPR risk assessment frameworks are complementary, and VLOPs and VLOSEs must comply with both.

- **Option to have profile-free recommender systems (Art. 38 DSA and Art. 4(4) and 22 GDPR):** Recommender systems might in specific cases relate to a decision based solely on automated processing in the meaning of Article 22 GDPR, notably when they can have serious consequences for individuals. Article 38 of the DSA adds to the GDPR requirements relating to profiling a right for the recipients of the services of VLOPs and VLOSEs to be offered "at least one option for each of their recommender systems which is not based on profiling". This is simply an additional right that must be offered to all recipients of services

[93] Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (wp251rev.01), 2018; Guidelines 8/2020 on the targeting of social media users. Guidelines 3/2025 on the interplay between the DSA and the GDPR are subject to comments until 31st October 2025.
[94] WP29 Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), endorsed by the EDPB.

of VLOPs and VLOSEs. The GDPR defines profiling in its Article 4(4). Therefore, the DSA and the GDPR are in this respect complementary.

- **Data access and security (Art. 40(1)-(13) and Recital 98 DSA and particularly Art. 89 GDPR):** Providing access to data held by online platforms involves the disclosure of personal data, thereby bringing such processing within the scope of the GDPR.

  Art. 5(1)(b) GDPR, read together with Art. 89 GDPR allows for special rules in relation to further processing of personal data for scientific research purposes. In contrast, Art. 40 DSA creates an obligation to disclose personal and non-personal data (subject to various requirements). On the other hand, Art. 40 lays down special purpose limitations on the use of the data to which access must be provided: Art. 40(2) stipulates that "Digital Services Coordinators and the Commission shall use the data accessed pursuant to paragraph 1 only for the purpose of monitoring and assessing compliance with this Regulation"; and Art. 40(12) stipulates that data must be made available to "researchers, including those affiliated to not for profit bodies, organisations and associations, who comply with [some of the core conditions that also apply to vetted researchers]", provided that these researchers will "use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Art. 34(1)".

  This applies to all the relevant data: it cannot be argued that when data that are provided to such researchers are anonymised, they can be used more widely because they are no longer personal data: that might be possible under the GDPR, but it is prohibited under the DSA. Relevant providers (i.e., VLOPs and VLOSs) must comply with the DSA requirements and disclose the data to vetted researchers and other researchers that qualify, subject to the procedures stipulated. But it should be noted that the relevant researchers must then comply with both GDPR, including Article 89 where applicable, and Art. 40 DSA. In particular, as noted earlier, they may only use the disclosed data for the specified purposes (respectively, "monitoring and assessing compliance with this Regulation" and "performing research that contributes to the detection, identification and understanding of systemic risks in the Union"); they may not use any data disclosed under Art. 40 DSA for any other purpose, not even if the data have been anonymised (either before disclosure by the provider or afterwards by the researchers).

  The DSA and the GDPR are in this respect complementary. The DSA mandates certain disclosures for specified research purposes, and then limits the use of the data, while the GDPR lays down general requirements that must be respected for processing of personal data for scientific research purposes, including when data are disclosed pursuant to Article 40 DSA.

- **Dark patterns (Art. 25 DSA and Art. 5 GDPR):** The prohibition of dark patterns in the DSA is applicable only to online platforms as defined in Article 3(i) DSA. However, as per Article 25(2) DSA practices that are already covered by the GDPR are not covered by Article 25(1) DSA. The GDPR only covers those dark patterns that relate to the processing of personal data and not to the provision of online intermediary services as such. The EDPB has provided recommendations and guidance for the design of the interfaces of social media platforms in compliance with the GDPR[95].

- **Compliance function (Art. 41 DSA and Arts. 37, 38 and 39 GDPR):** Under Art. 41 DSA, VLOPs and VLOSEs must establish a 'compliance function,' which may consist of multiple compliance officers. This function must be (i) independent from operational activities, (ii) endowed with sufficient authority, stature, and resources, and (iii) have access to the provider's management body to monitor compliance with the DSA. Additionally, the compliance function is required to cooperate with the Digital Services Coordinator of the establishment, ensure comprehensive risk identification through risk assessments, verify the effectiveness of mitigation measures, and inform and advise both management and employees on DSA obligations. Furthermore, VLOPs and VLOSEs that act as controllers must also appoint a data protection

95 EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces

officer, when the criteria under Art. 37 GDPR are met. The tasks of a data protection officer are laid down in Article 39 GDPR. They include monitoring the compliance with the GDPR, advising the controller, and cooperate with the data protection authorities. The DSA and the GDPR provisions on, respectively, the DSA "Compliance Function" and the GDPR DPO are complementary.

Finally, on **enforcement,** implementation, cooperation, penalties and enforcement arrangements in DSA Chapter IV (Arts. 49-55) and those in GDPR Chapter VI (Independent supervisory authorities in Arts. 51-67; EDPB in Arts. 68-76; Remedies, liability and penalties in Arts. 77-84) interplay: in relation to matters covered by the DSA, the DSA arrangements apply; in relation to matters covered by the GDPR, the GDPR arrangements apply. The two implementation, cooperation, penalties and enforcement systems are in principle (and in law) separate and distinct. In practice there will be an interplay between the DSA and the GDPR systems, when matters in a particular case that are covered by the DSA will have to take into an account the GDPR provision (as noted in the various entries, above). While the interplay between the DSA and the GDPR requires consistent interpretation and application, the DSA's enforcement and oversight framework does not formally recognise a role for cooperation or coordination with the DPAs or the EDPB. Nevertheless, all the regulatory actors are bound by the principle of sincere cooperation enshrined in Article 4(3) TEU, which has been elaborated on by the CJEU in particular in Case C- 252/21. Therefore, this absence should not hinder the establishment of cooperation and coordination mechanisms within their respective competencies in practice.

As noted, the DSA implementation, cooperation, penalties and enforcement arrangements interact with those laid down in the GDPR without providing for arrangements to address those interactions, and neither one nor the other constitute *leges specialis* in relation to the other. In practice, the principle of sincere cooperation applies and based on the *Bundeskartellamt* ruling, the respective authorities should liaise where e.g. the enforcement of the DSA requires interpretation of data protection concepts.

To aid with interpretation of the GDPR in the context of the DSA, the European Data Protection Board has issued "Guidelines 3/2025 on the interplay between the DSA and the GDPR".

### *VI. Special remarks on interplay*

A relevant interplay to be noted is referred to **online protection of minors** (Art. 28(1)-(4) and Recital 71 DSA, and Art. 4(11), 8 and Recital 38 GDPR)

The presentation of advertisements often involves the processing of personal data and profiling by online platforms, within the meaning of Art. 4(4) GDPR. Recital 38 of the GDPR stipulates that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child". The DSA enhances this protection when it comes to online platforms, prohibiting the presentation of ads on their interface based on profiling by using personal data of users "when they are aware with reasonable certainty that the recipient of the service is a minor" (Article 28(2)). In relation to VLOPs and VLOSEs, Article 35(1)(j) goes further and suggests that they should use "age verification" tools; and if these indicate that a user is a minor, they must of course comply with Article 28(2) and not present ads based on profiling of the minor. To this extent, the DSA extends the protection of minors beyond what is done in the GDPR.

The GDPR stipulates that personal data used for any purpose (i.e., also the use of age verification for the purpose of complying with article 28 DSA) must be "adequate" for that purpose and that the data must be "limited to what is necessary in relation to" the relevant purpose (Article 5(1)(c) GDPR). On its part, Article 28(3) DSA stipulates that "[c]ompliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor." There is therefore an interplay between GDPR and DSA requirements in this regard limited in application to Article 28 DSA that would not affect measures under Art 35 DSA. The recent EDPB Guidelines on the interplay between the GDPR and the DSA state that the provision in Article 28(3) DSA is 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.

In sum, the interplay in a complementary manner between Article 28(3) DSA and the principle of data minimization as enshrined in the GDPR is key ensuring protection of minors online, including when deploying age verification systems.

As detailed above, while a number of areas of interplay between the DSA and the GDPR have been identified, the provisions mutually reinforce each other and result in a complementarity between them.

## Regulation (EU) 2017/2394 ([96]) – [Consumer Protection Cooperation Regulation]

*General Information*

The Consumer Protection Cooperation (CPC Regulation) Regulation (EU) 2017/2394 was adopted in December 2017 and entered into force in January 2018. It entered into application in January 2020, replacing Regulation (EC) No 2006/2004. While there is no review clause in the CPC Regulation that obliges the Commission to review it, the Commission is currently reflecting about a review in order to ensure that the cross-border public enforcement cooperation framework established by it remains effective, also in light of the evolving digital landscape and the exponential growth of e-commerce.

The CPC Regulation lays down a cooperation framework to allow national authorities from all countries in the European Economic Area to work together to address breaches of consumer rules when the trader and the consumer are in different countries. Collectively, the national authorities form a European enforcement cooperation network, the "CPC Network".

*Personal scope*

The CPC Regulation concerns Member States, national competent authorities that have been designated by their Member State as responsible for the enforcement if Union laws that protect consumers' interests and the Commission as main actors under the cross-border public enforcement cooperation framework that it establishes. The Regulation also concerns specific other actors (such as European Consumer Centres, consumer organisations and associations or trader associations) on whom a Member State or the European Commission has conferred the power to issue a so-called external alerts to the CPC Network about suspected consumer law infringements covered by the Regulation.

*Material scope*

The CPC Regulation applies to cross-border infringements of the consumer law instruments listed in the Regulation's Annex. The Annex covers a broad range of substantive consumer law instruments covering, inter alia, consumer rights, unfair commercial practices, unfair contract terms, passenger rights, distance marketing of consumer financial services, cross-border portability of online content services, unjustified geo-blocking or the supply of digital content and digital services.

*Enforcement*

The CPC Regulation stipulates that each Member State needs to establish one or more competent authorities and a single liaison office responsible for the application of the Regulation (Article 5). The CPC Regulation provides the framework for mutual assistance (Chapter 3) and coordinated investigations and enforcement (Chapter 4) between these competent authorities. The Commission also plays a role in coordinating actions that relate to widespread infringements with a Union dimension (Chapter 5).

*Interactions with the DSA*

The CPC Regulation pre-dates the Digital Services Act and hence does not include any reference to it. Importantly, the DSA does not provide for its inclusion in the list of consumer law instruments in the CPC Regulation's Annex. As a consequence, CPC authorities are not competent to enforce the DSA's substantive obligations for online intermediaries. The DSA and CPC enforcement frameworks are distinct and separate from each other.

[96] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1–26).

In its Article 2(4)(f), the DSA provides that it is without prejudice to Union law on consumer protection including, *inter alia*, the CPC Regulation. Explicit references to the CPC Regulation are furthermore made in recitals 10 and 34 to the DSA.

On **personal scope**, both the DSA and the CPC Regulation provide that Member States designate national authorities as competent authorities under the relevant enforcement framework. While the two enforcement frameworks are distinct and separate from each other, neither the DSA nor the CPC Regulation prevents a Member State from designating a national authority as competent authority under both, the DSA and the CPC Regulation. Indeed, some Member States have made use of that possibility. Where a national authority has been designated as competent authority under both the DSA and the CPC enforcement frameworks ('double-hatted competent authority'), its actions are governed by the enforcement framework within which the specific action is taken. In other words: when a double-hatted competent authority acts as a DSA enforcer, its actions are subject to the requirements established by the DSA, when it acts as a CPC authority, its actions re subject to the requirements established by the CPC Regulation.

With regards to **territorial** and **material scope**, while the DSA is both a substantive and a procedural instrument (it establishes both, a responsibility framework with substantive law obligations for online intermediaries, and a specific framework for their public enforcement), the CPC Regulation is a procedural instrument only. This section therefore outlines the CPC Regulation's interplay with the DSA as a procedural instrument.

Referring to **enforcement**, both the CPC Regulation's enforcement framework and the enforcement framework established by the DSA concern enforcement within the EU. The CPC Regulation' territorial scope is broader than that of the DSA's enforcement mechanism in that the former also extends to enforcement in EEA countries. The relevant substantive DSA rules apply to EU-based and non-EU entities targeting EU consumers. The CPC Regulation' territorial scope is narrower than that of the DSA's enforcement mechanism in that the former only extends to enforcement in cross-border cases and not in domestic cases.

The CPC Regulation can be used for the cross-border enforcement of consumer law instruments as listed in the CPC Regulation's Annex and whose scope covers online intermediaries.

*Special remarks on interplay*

While the enforcement frameworks established in the DSA and the CPC Regulation are distinct and separate from each other, they are often applied in parallel where a certain conduct by an online intermediary concerns its obligations under the DSA and its obligations under consumer law (NB: for the interfaces between the DSA's substantive obligations and substantive consumer law see, for example the fiches on the UCPD and the CRD). The two enforcement frameworks are without prejudice to each other and designed to be complementary. The fact that the two enforcement frameworks often come into play in the context of a specific conduct by an online intermediary generates the need for cooperation between the competent authorities under the respective enforcement frameworks – in order to ensure coherent and complementary enforcement responses. As reported in the Commission's Communication on e-commerce[97] some Member States have taken the initiative of establishing cross-sectoral cooperation through e-commerce task forces at national level. The Commission encourages and is ready to support the creation of these task forces, that include Digital Services Coordinators, consumer protection authorities, market surveillance bodies, and customs authorities. Parallel investigations were launched under the CPC Regulation and the DSA in May 2025 identifying multiple breaches of EU consumer law[98]. Simultaneously, the European Commission launched a DSA investigation focused on whether SHEIN violated DSA obligations relating to risk assessment and mitigation, illegal content, recommender system transparency, and public ad-repository compliance 4. Similarly, in November 2024, the CPC Network launched a coordinated action against Temu for several consumer law violations while in parallel, on 31 October 2024 the Commission had Temu's interface design and content moderation systems (4).

[97] European Commission, A comprehensive EU toolbox for safe and sustainable e-commerce, 05.02.2025

[98] European Commission, February 2025, Online available at: Commission requests information from Shein on illegal products and its recommender system | Shaping Europe's digital future

These examples show that CPC and DSA enforcement mechanisms can apply in a complementary manner.

# Directive (EU) 2010/13/EU (as amended by Directive (EU) 2018/1808)([99])[Audiovisual Media Services Directive]

*General information*

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, known as the Audiovisual Media Services Directive (AVMSD), was adopted on 10 March 2010 and entered into force on 5 May 2010. Member States were required to transpose the Directive into national law by 19 December 2011. The Directive was subject to review by 19 December 2011 (Art. 33) to ensure it keeps pace with technological and market developments.

The 2018 revisions to the AVMSD were adopted on 14 November 2018 and entered into force on 18 December 2018. Member States were required to transpose the Directive into national law by 19 September 2020.An ex-post evaluation of the impact of the Directive and its added value is required by 19 December 2026. It will be accompanied where appropriate by proposals for its review.

The AVMSD[100] aimed to coordinate national legislation on audiovisual media services to create a single European market for such services. The AVSMD, as amended in 2018, seeks to create a safe, fair and diverse audiovisual media landscape in the EU while fostering an integrated market for content providers, balancing market freedoms with consumer protection and cultural policy goals.

*Personal scope*

The AVMSD applies to media service providers (linear broadcasters, and non-linear broadcasters, i.e. on-demand AV services / streaming platforms) (Art. 1(1)(d)) and video sharing platform (VSP) providers (Art. 1(1)(aa). In 2020, the European Commission issued Guidelines to support harmonisation and ensure a uniform interpretation by Member States when determining whether certain services qualify as video-sharing platform services under national law. These Guidelines focus on the practical application of the 'essential functionality' criterion in the definition of such services.[101]

*Territorial scope*

The AVMSD is generally limited to providers either established in the EU or considered under EU jurisdiction (Article 2(3)), for example because the provider uses a satellite link or satellite capacity pertaining to a Member State (Article 2(4)). However, the territorial scope of rules applicable to VSPs is set out in Art 28a. If a VSP is established in an EU Member State, then the rules in Article 3(1) Regulation 2000/31/EC (eCD[102]) apply, i.e. the country of establishment. The AVMSD rules also apply to VSPs not established in the territory of a Member State if they have (a) a parent undertaking or a subsidiary undertaking established on the territory of a Member State; or (b) is part of a group and another undertaking of that group is established on the territory of that Member State (Art. 28(a)(2)).

*Material scope*

The AVMSD establishes a comprehensive framework regulating traditional TV broadcasting, as well as on-demand audiovisual media services. For traditional media services, the AVMSD establishes the main legal

---

[99] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 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) (Codified version), OJ L 95, 15.4.2010, p. 1–24.

[100] The term "AVMSD" in this document should be construed as "the 2010 AVMSD, as amended in 2018".

[101] Communication from the Commission Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive 2020/C 223/02, OJ C 223, 7.7.2020, p. 3–9.

[102] 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.

framework, whereas for VSPs the AVMSD is only sector-specific legislation providing minimum harmonisation. In this context, the AVMSD introduced specific rules for audiovisual content displayed on VSPs, aimed at protecting users and minors from certain illegal and harmful content, as well as rules on audiovisual commercial communications.

The AVMSD focuses on the regulation of content available on VSP services (Art. 28a - 28b), in respect of protection of minors; incitement to violence and hate speech; and activities that constitute a criminal offence under Union law (as detailed in Art. 28b(1)).

In particular, VSP service providers must put in place appropriate measures to protect minors from content which could affect their physical, mental or moral development, and the general public from incitement to violence or hatred, or public provocation to commit a terrorist offence, offences concerning child pornography, and offences concerning racism and xenophobia. Such measures include, among others: mechanisms for users to flag non-compliant content and effective procedures for user complaints; providing effective media literacy measures and tools and raising users' awareness of those measures and tools; and age verification systems where content may impact minors. Importantly, Article 28a(5) clarifies that VSPs subject to the rules of the AVMSD are also subject (and therefore benefit from) the liability exemptions and prohibition on general monitoring obligations set out in Articles 12 to 15 of the ECD (now integrated in the DSA)[103]. In addition, Article 28b(1) clarifies that the content moderation obligations applicable to VSPs in that provision are without prejudice to Articles 12 to 15 of the ECD. Compliance with the AVMSD obligations by VSPs should be consistent with and not deprive them of the benefits of the hosting liability exemption and the prohibition on general monitoring obligations now in the DSA.

VSP service providers have obligations in respect of advertising and other content restrictions in audiovisual commercial communications, which take into account the limited control they can exercise over advertising on their platforms that is not marketed, sold or arranged by them (See Article 28b (2).

*Enforcement*

The AVMSD foresees enforcement at national level by the designation of independent national regulatory bodies by each Member State (Art. 30). It also includes a European coo peration and supervision dimension by the 'European Regulators Group for Audiovisual Services' (ERGA, currently replaced and succeeded by the 'European Board for Media Services'[104]) (Article 30b[105]). The European Commission does not have direct enforcement powers but can assess if national measures restricting freedom of reception of audiovisual media services, notified by Member States, are justified and compatible with EU law (Article 3 (5)). The Commission has the power to require the Member State to urgently put an end to the measure in question where it concludes that the measures are incompatible with Union law.

The national regulatory bodies have jurisdiction over audiovisual media service providers and VSPs in their territory, based on the country-of-establishment principle (as per Articles 2(3) and 28a, which includes a cross reference to Article 3 ECD)).

National regulatory bodies are responsible for the supervision, monitoring and enforcement of media service providers in the scope of the AVMSD. Article 3 of the AVMSD reflects the internal market principle by

---

[103] In addition, Recital 48 adds a safeguard to Articles 12-14 of the ECD, thereby preserving the limited liability exemption.
[104] ERGA was replaced and succeeded by the "Media Board" or "European Board for Media Services" after the entry into force of the Regulation (EU) 2024/1083, "European Media Freedom Act" (EMFA).
[105] The enforcement framework of the AVMSD primarily vests powers in national regulatory authorities or bodies designated by each Member State (Article 30). These authorities must be legally distinct from government and functionally independent, exercising their powers impartially and transparently in line with the Directive's objectives such as media pluralism, consumer protection and fair competition (Article 30(1)-(2)). Member States must clearly define the competences, powers and accountability mechanisms of these authorities in law, ensuring they have adequate financial and human resources and enforcement powers to effectively carry out their functions (Article 30(3)-(4)). These authorities collaborate through the currently European Board for Media Services, which provides technical expertise, facilitates consistent implementation, exchanges best practices, and cooperates on regulatory matters among Member States and with the European Commission (Articles 30a and 30b). Appeal mechanisms independent of the authorities exist at national level, and pending appeal outcomes, regulatory decisions generally stand unless interim measures are granted (Article 30(6)).

prohibiting Member States from restricting retransmissions on their territory of audiovisual media services from other Member States, subject to certain strictly framed derogations.

*Interactions with the DSA*

The DSA is not directly referenced, as the AVMSD predates the DSA. However, Article 28b(1) mentions that the AVMSD is without prejudice to Articles 12 to 15 of the ECD on the liability of intermediary service providers and Article 28b(3) mentions Article 15 of the ECD on the prohibition of any general monitoring obligations. As per Article 89 DSA, any references to Articles 12 to 15 ECD should be construed as references to Articles 4, 5, 6, and 8 DSA, respectively. Therefore, the AVMSD indirectly refers to the DSA.

Recital 10 and Article 2(4)(a) note that the DSA is without prejudice to other acts of Union law regulating other aspects of the provision of information society services, or specifying and complementing the harmonised rules under the DSA, and it includes in the list the AVMSD. For instance, Recital 68 DSA specifies that the DSA complements the application of the AVMSD which imposes measures to enable users to declare audiovisual commercial communications in user-generated videos.

Where the AVMSD pursues the same objectives of the DSA but does not fully address the issues, the rules of the DSA should apply in respect of such issues. This has been the position of the European Commission, confirmed for example in several of its reactions to draft national laws under Regulation 2015/1535. In any case, Member States retain competence to adopt legislative provisions determining what type of content is illegal or harmful.

Regarding the **personal scope**, both the DSA and AVMSD apply to intermediary services, but their scope differs. Whereas the DSA is horizontal and covers all online platforms, the AVMSD has a sector-specific scope. In particular, the AVMSD specifically regulates video-sharing platforms, and only as regards audiovisual content (so, it does not cover text, for instance). Video-sharing platforms can qualify as hosting services and online platforms under the DSA, including as Very Large Online Platforms (VLOPs) where relevant. This means that several VLOPs fall under the rules prescribed by both instruments.

When it comes to the **territorial scope**, the AVMSD applies to VSPs established in the EU or considered under the jurisdiction of a Member State. The AVMSD (Article 28a) also includes a rule extending the scope to those providers which are not established in the Union, with a relevant point of attachment to a Member State as per Article 28a(2). The country-of-establishment principle pursuant to Article 3 of the ECD also applies (Article 28a(5) AVMSD).

The DSA has a broader scope as it applies to all providers offering services to recipients in the EU, regardless of their actual place of establishment (Article 2 (1) DSA. Both instruments establish the competence of the authorities of the place of establishment of the provider.

On **material scope**, the core obligations for VSPs prescribed by the AVMSD are:

- Protection of minors (Article 6a, 28b(1)),
- Protection against incitement to violence/hatred, and certain criminal offences (Article 28b(1)),
- Advertising/commercial communications obligations (Article 9, 28b(2)),
- Age verification and parental controls (Article 28b(3)(h)),
- Media literacy (Article 28b(3)(f)),
- Complaint and redress systems (Article 28b(3)(i), (7)).

In general, the AVMSD and the DSA can be considered as complementary legislations for elements not covered equally in both instruments. VSPs must comply with both content rules (AVMSD) and platform rules (DSA). The following interactions in their respective material scopes are noteworthy:

- **Notice-and-action** and **feedback mechanisms** (AVMSD (Article 28b (3)(d) and (e)) and DSA (Articles 16, 17) (discussed in detail in the following section).

- **Internal complaint handling**: AVMSD (Article 28b(3)(i)) mandates "*transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints*" procedures; whereas the DSA

(Article 20) provides stricter obligations (free, electronic, with "human in the loop"). Here, the AVMSD remains relevant and applies to audiovisual-specific elements not covered in the DSA (e.g. content rating; reporting and flagging of content in breach of content standards set out in Article 28b(1)).

- **Out-of-court dispute resolution**: AVMSD (Article 28b(7)) requires impartial out-of-court (OOC) redress mechanisms; DSA (Article 21) establishes a certified OOC system. Here, the DSA prevails for content moderation disputes under its scope. AVMSD still applies for audiovisual-specific issues not covered under the DSA (e.g. content rating, reporting and flagging of content in breach of content standards set out in Article 28b(1), inclusion in terms and conditions of the content standards set out in Article 28b(1).

- **Advertising**: AVMSD rules on commercial communications (Articles 9, 28b(2)) and DSA provisions on transparency and profiling restrictions (Article 26, 28(2)) (discussed in detail in the following section).

- **Protection of minors**: Both instruments impose obligations; AVMSD has targeted rules (age verification, parental controls). The DSA (Articles. 28, 35) adds systemic risk assessment and mitigation (esp. for VLOPs) (discussed in detail in the following section).

- **Media literacy**: AVMSD mandates awareness-raising measures; DSA (Article 35) may require additional measures for VLOPs, with both provisions applying in parallel.

Finally, on **enforcement** both the DSA and AVMSD enforcement frameworks are harmonised across the EU but there are differences in their degree of centralisation and scope of authority. The AVMSD primarily relies on national enforcement through independent regulatory bodies designated by each Member State, which exercise jurisdiction over audiovisual media service providers and VSPs established in their territory. The DSA enforcement is based on the supervision by Digital Services Coordinators who supervise most providers at the national level, based on their place of establishment, coupled with direct enforcement powers vested in the Commission specifically for VLOPs.

*Special remarks on overlaps*

Certain specific provisions of the DSA and the AVMSD overlap. The prevalence of the DSA over the AVMSD depends on the individual provision, as discussed in the following section.

- **Protection of minors** (Article 28 DSA vs. Art. 6a AVMSD, Art. 28b(1) – (3) AVMSD. Both the DSA (Art. 28) and the AVMSD (Art. 28b(1)) contain provisions on the protection of minors. According to Article 28b(1) AVMSD, VSP providers shall "take appropriate measures to protect [...] minors from content which may impair their physical, mental or moral development." Article 28b(3), in turn, establishes targeted obligations on VSPs to protect minors, such as including and applying content requirements in the terms and conditions, establishing and operating age verification systems, or providing parental controls or content rating systems. With respect to Article 28(1) DSA, stipulates that there is an obligation for "providers of online platforms to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors". Both pieces of legislation are complementary and apply in parallel. Moreover, when VSPs are designated as VLOPs or VLOSEs, Articles 34 and 35 apply as well, imposing an additional set of obligations related to identifying systemic risks, including the respect for the rights of the child, and taking mitigation measures. In this regard, the two legislative frameworks do not overlap.

  Article 2(4)(a) DSA specifies that the DSA is without prejudice to other acts of Union law regulating the provision of information society services in general, such as the AVMSD. If such measures aim to protect minors, online platforms are required to comply with both sets of obligations. For those VSPs that are also VLOPs, an additional set of DSA obligations related to assessing systemic risks and taking mitigation measures apply. Consequently, compliance with the AVMSD does not exempt such VLOPs from these DSA obligations.

The latest European Commission' guidelines on the protection of minors,[106] consider that compliance with Article 28(1) DSA requires age verification methods to restrict access to adult content such as pornography and gambling, or when national rules set a minimum age to access certain services such as defined categories of online social media services. To this end, the European Commission's guidelines also point to the use of effective age assurance methods provided that they are accurate, reliable, robust, non-intrusive, and non-discriminatory. The EU Digital Identity Wallet, and before they become available, the blueprint for age verification on which applications can be built, will provide a compliance example and a reference standard for a device-based method of age verification."[107] The guidelines also clarify that they should not be interpreted as pre-empting obligations on protection of minors arising from other legal instruments, such as the AVMSD.

- **Notice-and-action and feedback mechanisms** (Article 28b (3) AVMSD vs. Articles 16 and17 DSA). AVMSD (Article 28b) requires the establishment of reporting mechanisms for illegal and harmful audiovisual content, which must be reflected in the VSPs terms and conditions; whereas the DSA harmonises: notice and action mechanisms solely for illegal content (Article 16) and obligations regarding the statement of reasons by the provider following restrictions imposed on the recipient of the service for content that is illegal or violative of their terms and conditions (Article 17). AVMSD (Article 28b) also requires mechanisms for feedback to users/reporters regarding illegal and harmful content; and the DSA, as mentioned, provides more detailed rules on notice-and-action and statement of reasons (Articles 16 and17); importantly, the DSA's notice and action obligations do not apply to content that is harmful or violative (of the provider's terms and conditions) but remains legal, but the feedback mechanism (statements of reasons) do cover also content moderation decisions based on terms and conditions. The AVMSD, in turn, requires feedback mechanisms to users who report illegal and harmful content, ensuring complainants are informed about the handling of their reports. Furthermore, the DSA expands on this by imposing more detailed rules on transparency, timelines for action and communication with users, enhancing accountability of online intermediary services providers.
  For notice-and-action procedures detailed in Article 16 DSA that apply to illegal content, the DSA prevails, as it is more specific. The AVMSD remains relevant and applies for the reporting, flagging and similar obligations related to harmful content. As regards feedback mechanisms on statement of reasons, the more detailed DSA's rules on these matters should prevail to the AVMSD.

  In practice, VSPs must integrate their reporting and feedback systems to comply with both the AVMSD and DSA. They need to ensure their mechanisms meet the more detailed DSA requirements while also fulfilling AVMSD obligations related to audiovisual content, such as the appropriate reporting, flagging and other measures related to harmful content. Furthermore, such compliance will be supervised by potentially different authorities (media regulators for the AVMSD, Digital Services Coordinators for the DSA).

- **Advertising** (Articles 9, 28b(2) and (3)) AVMSD vs. Articles 26, 28(2) DSA. AVMSD focuses on content standards and protection of vulnerable groups (especially minors) in audiovisual commercial communications. The DSA focuses on transparency (Article 26 DSA) including specific rules on how advertisements are presented to minors (Article 28(2) DSA). Both address protection of minors but from different angles: the AVMSD poses substantive content requirements (no harmful ads, no exploitation), whereas the DSA focuses on procedural (transparency). Both also include privacy safeguards: no advertisements based on profiling when the recipient is a minor in the DSA and no processing for commercial purposes of personal data of minors that are collected or otherwise generated through age verification or parental control systems in the AVMSD. Both instruments regulate VSPs when they serve audiovisual content or ads.

---

[106] ANNEX to the Communication to the Commission Approval of the content on a draft Communication from the 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; Brussels, 14.7.2025; Commission publishes guidelines on the protection of minors | Shaping Europe's digital future

[107] European Commission, Commission publishes guidelines on the protection of minors. Last accessed on 11 August 2025, Commission publishes guidelines on the protection of minors | Shaping Europe's digital future.

In the context of advertising, the AVMSD and the DSA apply in a complementary manner, as they address different aspects of audiovisual commercial communications. The AVMSD regulates what can be advertised and how minors are protected from harmful content, whereas the DSA governs how advertising must be presented on online platforms, ensuring transparency. In practice, video-sharing platforms must comply with both and ensure advertising content does not violate AVMSD requirements (e.g., no subliminal ads, no harmful ads targeting minors), as well as implement DSA transparency measures.

In sum, the AVMSD provides sector-specific rules for audiovisual content, including in relation to VSPs. The DSA establishes a horizontal framework covering all intermediary services. For audiovisual content on VSPs, both instruments interplay, but the DSA prevails where its harmonised and directly enforceable obligations are more specific, as it is the case for notice-and-action mechanisms for illegal content, feedback mechanisms on statement of reasons, complaint handling mechanisms or out-of-court dispute settlement bodies related to DSA-specific issues, or obligations related to assessing systemic risks and taking mitigation measures to protect minors . AVMSD remains crucial and applies for targeted obligations that are not covered under the DSA.

VSPs must comply simultaneously with both frameworks. For VSPs that are designated as VLOPs or VLOPs/VLOSEs, compliance with AVMSD does not exempt them from Articles 34 and 35 DSA obligations. In this respect, where overlaps occur, these DSA's obligations prevail.

## Directive (EU) 2019/790 ([108]) – [Directive on Copyright in the Digital Single Market]

*General information*

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 (CDSMD) was adopted on 17 April 2019 and came into force on 7 June 2019.

The Directive does not replace the 11 directives which together comprise the EU's copyright legislation or Copyright *acquis*, including Directive 2001/29/EC on the harmonisation of copyright in the information society (InfoSoc) and Directive 2004/48/EC on the enforcement of intellectual property rights (IPRED) (please refer to dedicated fiches).

The CDSMD's primary objective is to modernise copyright rules by adapting certain exceptions and limitations to copyright and related rights to digital and cross-border environments, ensuring fair remuneration for rights holders and better regulation of content-sharing services providers.

*Personal scope*

The CDSMD applies to a wide range of actors, including authors, performers and rightsholders who hold copyright or related rights. Some specific actors to which exceptions to copyright are applied are defined in Article 2: 'research organisations' (Articles 2(1)) and 'cultural heritage institutions' (Article 2 (3)). The Directive also applies to online content-sharing service providers (OCSSPs), defined in Article 2(6) of the CDSMD as "provider of an information society 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", as well as collective management organisations (Articles 8-12). The CDSMD also extends certain rights of the InfoSoc Directive to press publishers if their content is used by an information society service providers (Article 15), although it does

[108] 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; PE/51/2019/REV/; OJ L 130, 17.5.2019, p. 92-125.

not directly regulate them. The CDSMD refers to Directive (EU) 2015/1535 Article 1 (1) (b) for the definition of information society services.[109]

*Territorial scope*

The CDSMD applies to the use of copyright protected content within the EU and may apply also to OCSSPs established outside the EU, who make protected content uploaded by their users accessible in the Union. The application of the CDSM in a particular case also relies on the Brussels Ia[110] and Rome II Regulations, the latter having specific rules for copyright law in Article 8. The DSA explicitly applies to online intermediary services providers regardless of establishment, provided they offer services to users in the EU (Article 2(1) and Recital 7 DSA) and introduces the concept of a "substantial connection" to the Union, which may arise through targeting EU markets or having a significant EU user base.

*Material scope*

The CDSMD covers copyright and related rights in the digital environment focusing on the use, licensing and protection of works and other subject matter online. It also introduces due diligence obligations for OCSSPs who communicate or make available to the public protected works and other subject uploaded by their users (Article 17).

*Enforcement*

The CDSMD itself contains limited direct enforcement provisions, as enforcement primarily relies on existing national laws and the IPRED (2004/48/EC) (please refer to dedicated fiche), and, to a limited extent, the InfoSoc Directive (Article 8). It also requires certain platforms – OCSSPs under Article 17 – to implement a number of measures (namely in paragraph 4) and several substantive and procedural safeguards (paragraphs (7) to (9)). These rules are enforced in the Member State where the copyright relevant act takes place – therefore the "country-of-destination" principle applies.

*Interactions with the DSA*

As the CDSMD precedes the DSA, no reference to the latter is possible. The CDSMD though makes explicit reference to Directive 2000/31/EC111 (e-Commerce Directive –ECD-) in Recitals 4 and 65 and in Article 1(2).[112] There is also an implicit reference to Article 15 ECD in Article 17(8), which sets out that the application of Article 17 shall not lead to any general monitoring obligation. As per Article 89 DSA, any references to Articles 12 to 15 ECD should be construed as references to Articles 4, 5, 6, and 8 DSA, respectively.

The DSA contains an implicit reference to the relationship between that Regulation and Article 17 CDSMD: Recital 11 DSA notes that the DSA is without prejudice to Union law on copyright and related rights, including

---

[109] b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
For the purposes of this definition:

- 'at a distance' means that the service is provided without the parties being simultaneously present;
- 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.'

[110] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007, pp. 40–49.

[111] 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.

[112] Article 17(3) CDSM also refers to the e-Commerce Directive. This is discussed in more detail in the section on overlap in the liability regime for hosting service providers and OCSSPs (para. 18 ff).

the CDSMD, "which establish specific rules and procedures that should remain unaffected". Recital 97 specifies that the DSA provides a framework for compelling access to data from VLOPs and VLOSEs to vetted researchers affiliated to a research organisation within the meaning of Article 2 CDSMD. Moreover, following the aforementioned Recitals, Article 2(4)(b) DSA also specifies 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* this Regulation, in particular,[...] Union law on copyright and related rights." [...]. Finally, Article 40(8)(a) DSA refers to CDSM's definition of "research organisation".

Regarding the **personal scope**, both apply to OCSSPs, which are regulated under Article 17 CDSM and as online platforms under Article 3(i) DSA. Online platforms which are not OCSSPs are not covered by Article 17 CDSM, but rather by the pre-existing copyright acquis, and in particular Article 3 and 8(3) InfoSoc Directive. For instance, an online platform that does not "store and give the public access to a large amount" of copyright-protected works or other protected subject matter uploaded by its users, or an online platform without profit-making purposes, will not be in scope of Article 17 CDSM, but will still generally be covered by the DSA. Specific categories of hosting services that are excluded for the OCSSPs definition are identified in the second part of Article 2(6) CDSMD.

On **territorial scope**, both DSA and CDSM have the same territorial scope. The DSA applies to providers of intermediary services that offer their services to recipients in the EU (Article 2(1) DSA). The CDSMD also captures non-EU platforms targeting the EU market as it applies to services that operate within the EU (Cf. Article 17(1) CDSM which requires OCSSPs to obtain authorisation when performing an act of communication to the public or making available to the public).

Referring to the **material scope**, there is an interplay in the material scope of the CDSMD and the DSA in as far as they both regulate the responsibilities of online platforms in managing user-generated content and protecting fundamental rights. While the CDSM imposes obligations related to copyright enforcement and licensing (notably in Article 17), the DSA introduces a more horizontal regime which includes rules on the liability regime and due diligence obligations for online intermediary services providers, particularly regarding measures on illegal content, that would include copyright-infringing material which qualifies as such. Article 15 CDSMD on the other hand imposes an obligation on all information society service providers, including intermediaries, to obtain an authorisation from press publishers for the online use of their publications (except for private use, hyperlinking or very short extracts). In practice, this obligation may apply in particular to providers of online search engines and online platforms. Press publications used by these providers without authorisation would qualify as "illegal content" under the DSA, and therefore the horizontal due diligence obligations regarding illegal content under the DSA apply and provide a complementary layer to the actual enforcement of the ancillary copyrights of press publishers.

In particular, Article 17 CDSM imposes several obligation on OCCSPs that find some parallelisms in the DSA, such as having a specific notification system, a complaint mechanism, the obligation to make best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided the service providers with the relevant and necessary information, or even transparency obligations (*vis-à-vis* rightsholders) as regards their content moderation practices. Member States should also ensure the availability of out-of-court redress mechanisms.

For services in scope, the CDSMD establishes a specific liability regime, including a specific "safe harbour", that acts as *lex specialis* to the general safe harbour under the DSA for those services in scope.

On **enforcement**, under the CDSMD is primarily handled by national courts, based on a "country-of-destination" principle, whereas the DSA introduces a dual oversight system, with powers given to national DSCs and the European Commission (Articles 49-56 DSA), based on a "country-of-origin principle".

*Special remarks on overlaps*

Some relevant elements need to be highlighted as follow:

- **Liability regime for hosting service providers and OCSSPs**: Article 17 of the CDSMD and Articles 6 of the DSA both regulate the exemption of liability of online platforms for user-uploaded content. Article 6 DSA replaces the previous Article 14 ECD safe harbour for hosting service providers, setting out a liability exemption conditional on lack of actual knowledge of illegal content and prompt removal upon notice. Article 17 CDSM, in contrast, establishes a *lex specialis* regime specifically for OCSSPs.

  Article 17 states that OCSSPs carry out acts of communication to the public when they give access to works/subject matter uploaded by their users. As a result, these providers become directly liable for their users' uploads. They are also expressly excluded in paragraph (3) from the hosting safe harbour for copyright relevant acts, previously available to many of them under Article 14(1) ECD. Arguably, this makes Article 17 *lex specialis* to the ECD.

  The provision then introduces a set of rules to regulate OCSSPs, including a liability exemption mechanism in paragraph (4), and a number of what can be referred to as mitigations measures and safeguards. The liability exemption mechanism is comprised of best efforts obligations for preventive measures, including those aimed at ensuring the unavailability of unauthorised content ex ante, at notice and stay-down, and at notice and takedown.

  Importantly, unlike the liability exemption for hosting services under Article 6 DSA, which requires lack of knowledge and prompt removal upon notice, Article 17(4) mandates proactive preventive measures and licensing best efforts to avoid liability.

  The Guidance[113] confirms that Article 17 CDSM serves as a *lex specialis* liability regime specifically addressing copyright-protected content on OCSSPs (Section II). It supplements the broader hosting liability framework under Article 6 DSA by creating a specific rule to regulate copyright-protected content hosted and made available to the public on OCSSPs (Section V). Article 17(3) CDSMD states that if an act of an OCSSP is covered by Articles 17(1) and (2), then the hosting liability exemption in Article 14(1) – and therefore Article 6 DSA – does not apply to that act. Thus, the OCSSP is directly liable without the possibility of benefiting from the liability exemption for hosting service providers in the DSA. For acts of those same online platforms that do not fall under the scope of Article17(1) and (2) – especially the hosting of illegal content that is not copyright infringement – Article 6 DSA remains applicable.

  The DSA provides a general liability exemption framework for hosting services. By contrast, Article 17 imposes a stricter, copyright-specific liability regime on OCSSPs. The DSA's general hosting liability rules thus remain applicable to other illegal content, or for copyright infringements by other providers or under circumstances not covered by Article 17, but copyright enforcement on OCSSPs is governed by Article 17's *lex specialis* regime.

- **Notice-and-action**: Article 16 DSA establishes general procedural rules for hosting service providers to receive, process, and respond to notices about illegal content, including requirements for notice precision and timely decisions. Article 17(4) CDSM, in turn, sets a specific liability regime for OCSSPs regarding unauthorised copyright-protected content uploaded by users, notably requiring providers to act expeditiously upon "sufficiently substantiated notices" from rightsholders.

  As explained above, Articles 17(4)(b) and (c) CDSMD set out a specific notice-and-action regime, which includes in paragraph (c) obligations regarding notice-and-takedown as well as notice-and-stay-down. At the same time, however, Article 17 CDSMD does not specify the concrete details of the notice-and-action mechanism and some components of the notice-and-action regime, such as the minimum elements that should be contained in a notice to a platform, which is where Article 16 DSA adds a level of specificity not found in the *lex specialis* rules of the CDSMD.

---

[113] Communication From The Commission To The European Parliament And The Council, 4.6.2021, COM(2021) 288 final. Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market.

While the rules under the DSA apply to all types of illegal content, Article 17 CDSMD establishes a specific liability and notice-and-action regime tailored to copyright content. Practically, this means OCSSPs must design notice-and-action systems that meet both frameworks, ensuring notices coming exclusively from rightsholders comply with the specific standards of substantiation under the CDSMD, while also aligning with the DSA. The DSA's list of elements that need to be included in the notice and the standard for notice are very similar to what the CDSMD requires for illegal content to be taken down, which in turn is based on the indications given by the Court of Justice in its case-law. The standard that notices should meet in order to give rise to actual knowledge is exactly the same in its intermediary liability case law.

Given that Article 17 CDSMD does not include any trusted flagger mechanism, Article 22 DSA applies to OCSSP covered by Article 17 CDSMD, as they fall into the DSA category of "online platforms", defined under Article 3(h). In this case, OCSSP covered by Article 17 would need to process with priority and "without undue delay" the notices submitted by trusted flaggers in relation to unauthorised copyright content, however only if they are submitted through the mechanism which the provider has established in accordance with the requirements under Article 16 DSA.

Certain DSA provisions, notably those linked to actual knowledge and the hosting safe harbour, do not apply to OCSSPs with regards to copyright-infringing content due to the *lex specialis* status of Article 17 CDSMD. Additionally, users' rights to receive statements of reasons for content removal under Article 17 DSA and the complaint mechanism under the DSA complement the complaint and redress mechanisms mandated by Article 17(9) CDSM, requiring platforms to extend their reporting and communication systems accordingly. Overall, this overlap demands integrated compliance strategies that respect the specificities of copyright enforcement.

CDSMD In practice, service providers may decide to implement a single notice and action mechanism, including for cases falling within the scope of Article 17 of the CDSMD.

- **Internal complaint-handling system**: In various forms, both Article 20 DSA and Article 17 CDSMD stipulate that such internal complaint mechanisms need to be effective, to be processed within a reasonable timeframe (undue delay/timely manner) and to involve some form of human review. Article 20 DSA, however, is fullly harmonised (in a Regulation) and more detailed. It requires providers to allow access to an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge, against any content moderation decision. Furthermore, it imposes an obligation on platforms to reverse unfounded or unwarranted decisions where complaints present sufficient grounds. It also includes a requirement of user-friendliness and a minimum period for filing such complaints of six months following the restrictive moderation decision, listed in Article 20(1). These obligations are clearly more specific and detailed than the corresponding Article 17(9) of the CDSMD, that merely obliges Member States to "provide that online content-sharing service providers put in place an effective and expeditious complaint and redress mechanism", with reference to a narrower set of copyright content moderation restrictions ("disabling of access to, or the removal of, works or other subject matter uploaded by" users). Furthermore, Article 20 DSA's broader scope extends beyond reinstatement of content to cover measures such as account terminations, suspensions, and demonetisation related to copyright-infringing material, areas not addressed by Article 17 CDSM.

  Article 17(9) of the CDSMD establishes a baseline regime for OCSSPs to implement effective and expeditious complaint and redress mechanisms for users disputing the removal or disabling of copyright-protected content. This provision ensures that users have access to internal processes to challenge copyright content moderation decisions, with the expectation of human review and the possibility of content restoration where appropriate. However, the Article leaves detailed procedural requirements and enforcement mechanisms largely to Member States. Article 20 DSA supplements and expands upon this framework in a fully harmonised manner by imposing more detailed and specific requirements for internal complaint-handling systems and does not allow national laws to deviate from it. It mandates that providers allow electronic, free-of-charge complaints against different types of content moderation decisions and obliges them to reverse unjustified actions when complaints have merit. Furthermore, Article 20 DSA's

scope extends beyond content reinstatement to include other moderation actions such as account suspensions and demonetisation.

The Guidance elaborates on the complaint and redress mechanism under Article 17(9), requiring human review of content removal decisions and enabling users to contest blocks (Section VI).

Platforms must navigate the requirement under Article 20 DSA to reverse unfounded or unwarranted content moderation decisions, which extends beyond the content reinstatement focus of Article 17(9) CDSM to include account terminations, suspensions, and demonetisation relating to copyright-infringing material, areas which are not explicitly covered by the CDSMD[114]. The DSA requires providers of online platforms to reverse unfounded or unwarranted decisions where the complaint contains sufficient grounds for this. The Guidance on Article 17 similarly states that under the complaint and redress mechanism the OCSSP should decide whether to make available or to restore the content which has been blocked or taken down.

However, the DSA establishes one single obligation, to be enforced by the country of establishment of the platform, while the CDSM empowers the authorities in all 27 Member States to potentially establish different conditions for the compliance with this obligation. Therefore, a given platform may be subject to 27 different specifications of this obligation under the CDSM, while the DSA is fully harmonising the obligation.

- **Out-of-court mechanisms**: Article 21 DSA establishes a framework for certified out-of-court dispute settlement (ODS) bodies to resolve disputes arising from platform content moderation decisions, including removals or disablement of access to content. Article 17(9) CDSM requires MS to ensure that such out-of-court redress mechanisms, including impartial dispute resolution are available. Both provisions address the possibility of out of court dispute resolution to challenge content moderation decisions by online platforms, although with significant differences of detail on how this possibility in regulated.

  Article 17(9) CDSMD mandates MS to ensure ODS mechanisms are available to users. Article 21 DSA establishes a detailed ODS mechanism that allows users to challenge a platform's content moderation decisions before an independent third-party body certified by national regulators.

  The DSA does not per se require Member States to set up ODS bodies. In contrast, Article 17(9) CDSMD requires that this option is available for disputes on OCSSPs. In theory, the ODS bodies that are certified under Article 21 DSA could also settle disputes under Article 17 CDSMD. However, in practice, this possibility only materializes if a specific ODS body obtains certification also for this type of content in their areas of expertise. If this is not the case, these systems will in practice run on parallel tracks and no overlap appears between both legislations

- **Transparency obligations**: Article 15 and 24 DSA mandates comprehensive transparency reporting by providers of online platforms regarding content moderation activities, including decisions related to copyright content removals and cooperation with rightsholders. Article 17(8) CDSM requires OCSSPs to provide rightsholders, at their request, with adequate information on the functioning of their practices with regard to two aspects: (1) the cooperation referred to in paragraph 4 (i.e. the best efforts obligations mentioned therein) and; (2) where licensing agreements are concluded between OCSPPs and rightsholders, information on the use of content covered by the agreements.

  The transparency reporting obligations in Articles 15 and 24 DSA - which require providers to make information publicly available – are broader and require more information than the transparency obligation in Article 17(8) CDSMD; the latter applies only at the request of rightsholders and concerns the practical application of Article 17 CDSMD. Therefore, the DSA transparency obligations should be seen as complementary to the transparency obligation of the CDSMD, to the extent that they require information

[114] The Guidance on Article 17 recommends that only manifestly infringing content stays down during the human review performed under the redress mechanism, in line with the CJEU's ruling in C-401/19 - Poland v. Parliament and Council.

that is in addition to that required under Article 17 CDSMD. As such, the platforms covered by Article 17 would need to comply with Articles 15 and 24 of the DSA, including for copyright-protected content (e.g. information on the number of notices sent under Article 17 CDSM).

On this topic, the Guidance highlights that OCSSPs must provide rightsholders with adequate information on the functioning of content recognition technologies, and on the use of content under licensing agreements as required by Article 17(8) (Section VII). This complements the broader transparency reporting obligations under Articles 15 and 24 DSA (Section VII).

The interaction mandates that OCSSPs maintain detailed internal records and reporting systems enabling timely and accurate disclosures both to rightsholders and to the public and regulators.

- **No general monitoring obligations:** Article 17(4)(b) CDSMD introduces an obligation of best efforts to ensure the unavailability of protected content for which the rightsholders have provided the service providers with the relevant and necessary information, and Article 17(4)(c) CDSMD requires a so-called "notice and stay down procedure" (best efforts to prevent their future uploads in accordance with point (b)). However, Article 17(8) CDSM, consistently with Article 8 DSA, explicitly prohibits the imposition of a general monitoring obligation on service providers. The internal consistency of these provisions has been clarified and confirmed by the CJEU (C-401/19 - Poland v. Parliament and Council). In particular, the Court recognises that Article 17 CDSM is formulated "in terms similar to those employed in Article 15(1) of Directive 2000/31" and applies, by analogy, the jurisprudence interpreting the ECD to modulate the obligations under the CDSM: "*That clarification means that the providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright.*"

  Accordingly, the preventive obligations under Article 17(4)(b) and (c) CDSM must be qualified to exclude content where determining illegality mandates such an independent, case-by-case assessment by the OCSSP, including consideration of copyright exceptions and limitations. This means that according to the Court's interpretation, Article 17 CDSM does not impose a general or indiscriminate monitoring obligation; rather, it requires "best efforts" limited to content that can be identified as infringing based on the relevant and necessary information provided by rightsholders, without necessitating an independent legal or factual evaluation by the platform. Following this interpretation, Article 17's obligations are to be understood as targeted, proportional and subject to the fundamental rights safeguards recognised by the Court.

  Article 17 CDSMD is construed as a *lex specialis* to the horizontal liability regime in the ECD (replaced by the DSA), and as Recital 11 DSA stresses, its "specific rules and procedures [...] should remain unaffected". Moreover, the Court in C-401/19 (Poland v Parliament and Council), at paragraph 91, explicitly references its prior ruling in the YouTube case (C682/18 and C683/18), which interprets Article 14 ECD on the requirements for notices to trigger actual knowledge—now codified under Article 16 DSA. The Court emphasises that, as recital 66 of Directive 2019/790 states, availability of unauthorised content may only be avoided upon notification by rightsholders. Further, such notification must contain sufficient information enabling the online content-sharing service provider to ascertain, without detailed legal examination, that the content is illegal and that removal complies with freedom of expression and information.

  Consistent with the CJEU interpretation, the Guidance reiterates the prohibition of any general monitoring obligation imposed on service providers (Section VI). It clarifies that preventive measures must be proportionate, targeted and based on relevant and necessary information provided by rightsholders, ensuring platforms are not required to engage in indiscriminate surveillance (Sections V.2 and VI).

  Articles 34 and 35 of the DSA require VLOPs/VLOSEs to conduct comprehensive systemic risk assessments and implement proportionate mitigation measures addressing risks—including the dissemination of illegal content such as copyright-infringing material. Practically, this means these platforms must analyse how their design, algorithms, content moderation and advertising systems might facilitate such dissemination, and adopt targeted measures to reduce these risks. However, the interplay with

Article 8 DSA and Article 17(8) CDSM is crucial in defining the boundaries of these preventive obligations. Article 8 DSA explicitly prohibits imposing a general monitoring obligation on intermediaries to actively seek illegal content, while Article 17(8) CDSM similarly forbids a general monitoring obligation in the copyright context.

Importantly, Article 17(5) CDSM requires that the preventive obligations imposed on OCSPPs be proportionate and take into account factors such as the service's size, audience, and the availability and cost of appropriate technologies. In practice, this ensures that preventive measures do not translate into a blanket monitoring duty, aligning with the prohibition on general monitoring under Article 17(8) CDSM and Article 8 DSA.

In sum, while the DSA introduces a harmonised, horizontal regime for intermediary services the CDSMD, and in particular Article 17, establishes *a lex specialis* liability regime for copyright-protected content on OCSSPs. In areas of overlap, the DSA's provisions often supplement or complement the CDSM's requirements, while the CDSM continues to govern copyright-specific issues.

## Regulation (EU) 2019/1020 ([115]) – [Market Surveillance Regulation]

*General Information*

The Market Surveillance Regulation (MSR) entered into force on 25 June 2019. It has been applicable since 16 July 2021. It must be evaluated by 31 December 2026, and every five years thereafter.

The MSR is based on Articles 33 and 114 TFEU. It seeks to establish a common framework for ensuring that products placed on the EU market comply with Union harmonisation legislation and therefore fulfil requirements providing a high level of protection of public interests, including safety. It aims to strengthen the enforcement of Union harmonisation legislation by enhancing cooperation between national authorities, improving controls on imported goods, and addressing challenges posed by online and cross-border trade. The Regulation requires market surveillance authorities to perform appropriate checks on the characteristics of products on an adequate scale, empowers them to take corrective actions, including ordering the removal of dangerous products, and ensures that products without a responsible EU-based economic operator cannot be sold to EU consumers.

*Personal scope*

The MSR is chiefly concerned with national market surveillance authorities and custom authorities but also sets obligation on the relevant economic operators involved in the supply chain of products subject to Union harmonisation legislation placed or made available on the internal market (see Articles 4 to 7 MSR). Amongst these, the MSR sets out specific obligations for information society service providers which it defines by referencing Article 1(1)(b) of the Information Society Directive (2015/1535).[116]

*Territorial scope*

The MSR applies to "products that are subject to the Union harmonisation legislation listed in Annex I" (which refers to more than seventy instruments of EU law on product safety), and its Recital 6 establishes that 'if new Union harmonisation legislation is adopted in the future, it will be for that legislation to specify whether this Regulation is also to apply to that legislation' (Artificial Intelligence Act, e.g.). As a general rule, these pieces of legislation apply to products that are placed or made available on the internal market. With regard to online sales, Article 6 MSR stipulates that "products offered for sale online or through other means of distance sales shall be deemed to be made available on the market if the offer is targeted at end users in the Union. An offer for sale shall be considered to be targeted at end users in the Union if the relevant economic operator directs, by any means, its activities to a Member State."

*Material scope*

The MSR focuses on ensuring that products placed on the EU market comply with Union harmonisation legislation and therefore fulfil requirements providing a high level of protection of public interests, including safety , and it grants national authorities the power to take enforcement actions, including requiring the removal of non-compliant products from online interfaces.

In more detail, market surveillance provisions generally apply to non-food products that are subject to EU harmonization legislation i.e., to more than seventy pieces of legislation listed in the mentioned Annex I MSR and to legislation adopted after the Regulation's entry into force, but only in so far as there are no specific

[115] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ 2019 L 169, 1–44.

[116]Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ 2015 L 241, 1-15.

market surveillance and enforcement provisions in the EU harmonization legislation *(lex specialis*). Besides, specific provisions on controls at the external borders (Chapter VII MSR) apply to all products subject to Union law; finally, specific provisions on economic operators (Article 4 MSR) only apply to products subject to 19 pieces of EU legislation referred to in Article 4(5) MSR.

*Interactions with the DSA*

The MSR contains no direct references to the DSA. However, it clarifies that it is without prejudice to Articles 12 to 15 of Directive 2000/31/EC (E-Commerce Directive) which as per Article 89(2) DSA shall be construed as references to Articles 4, 5, 6 and 8 DSA.

The DSA states in Article 2(4)(f) and Recitals 10 and 34 DSA that it 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, such as the rules laid out in the MSR. Moreover, the DSA refers to the MSR on the definition of an economic operator, which is a key category that sets the distinction from an online intermediary service provider. According to Article 31(1) of the DSA, providers of online platforms must ensure that their online interface enables traders to provide information on the name, address, telephone number and email address of the economic operator.

On **personal scope**, the MSR is broader than the DSA, as it applies to providers of all information society services, which refer to services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535. The DSA, in contrast, applies to providers of a subset of information society services, namely those known as "mere conduit", "caching" and "hosting" services.

With regards to **territorial scope**, as mentioned, the MSR applies to a wide range of products covered by Union harmonisation legislation that are placed on or made available on the EU market, irrespective of where they are manufactured. By contrast, under Article 2(1) DSA, the DSA applies to online intermediary services offered to recipients that have their place of establishment or are located in the Union, irrespective of the provider's place of establishment.

When it comes to **material scope**, the legal framework organised by the MSR complements the system of the DSA without interference.

While the MSR does not directly regulate online intermediary services, it does impose certain obligations and enable enforcement actions that affect them, particularly in relation to the online sale of products. The most notable provision is Article 14(4)(k) MSR which, where no other effective means are available to eliminate a serious risk, grants enforcement powers to market surveillance authorities:

- to require the removal of content referring to products from an online interface or the explicit display of a warning to end users when they access an online interface; or
- where the above request has not been complied with, to require information society service providers to restrict access to the online interface, including by requesting a relevant third party to implement such measures.

While the MSR does not define or categorize online intermediary services as a distinct group of addressees, it indirectly involves them by targeting the interfaces through which non-compliant products are marketed or sold. In cases where a product has no responsible economic operator in the EU, the MSR strengthens controls on fulfilment service providers, which may include actors operating in a platform-like capacity.

The MSR explicitly underlines the importance of enforcement in the online environment in Article 11, by emphasising that market surveillance authorities shall ensure "effective market surveillance within their territory of products made available online and offline with respect to products that are subject to Union harmonisation legislation." The MSR also enacts, in Article 7(2), a sequence of obligations for the providers of information society services, who must "cooperate with the market surveillance authorities, at the request of the market surveillance authorities and in specific cases, to facilitate any action taken to eliminate or, if that is not possible,

to mitigate the risks presented by a product that is or was offered for sale online through their services." Article 9 DSA specifies this obligation, as it requires the providers of intermediary services to act on orders of judicial or administrative authorities. These providers, once an order is received, must inform the issuing authority without undue delay, of how, when and when they complied with the order.

The MSR addresses the **enforcement** of product safety laws in the digital context. Other instruments such as the DSA set detailed procedural and transparency obligations for online intermediaries. The DSA thus interacts with the MSR by complementing it.

Nonetheless, the enforcement mechanisms between the MSR and the DSA differ. Under the MSR, national market surveillance authorities are competent to monitor and enforce compliance with EU product legislation. These authorities can inspect products, order recalls or withdrawals, and, under Article 14(4) MSR, require the removal of illegal or unsafe product listings from online interfaces. Enforcement is thus primarily decentralised and targets economic operators (including, manufacturers, authorised representatives, importers, distributors and fulfilment service provider) rather than intermediary service providers. Under the DSA, specific independent authorities at national level (Digital Services Coordinators) and, for very large online platforms (VLOPs) and very large online search engines (VLOSEs), the European Commission, are responsible for all matters relating to supervision of providers of intermediary services and enforcement of the DSA (Article 49 DSA). A number of other mechanisms must also be put in place, which require online platforms to set up internal complaint handling systems (Article 20 DSA) and to give priority to the notices of trusted flaggers who detect, identify and notify illegal content (Article 22 DSA). These measures are not envisaged in the Market Surveillance Regulation.

*Special remarks on interplay*

The MSR and DSA have complementary provisions.

## Regulation (EU) 2019/1148 ([117]) – [Explosives Precursors Regulation]

*General Information*

Regulation (EU) 2019/1148 on the marketing and use of explosives precursors (EPR) was adopted on 20 June 2019 and became applicable as of 1 February 2021. It repealed and replaced Regulation (EU) No 98/2013, strengthening the EU framework for preventing the misuse of certain chemical substances in the illicit manufacture of explosives. The EPR sets harmonised rules across Member States to restrict access to high-risk substances and to enhance detection, reporting, and enforcement mechanisms.

The next scheduled review of the Regulation is an evaluation by the European Commission, to be carried out by 2 February 2026. This evaluation will assess efficiency, effectiveness, relevance, coherence, and EU added value, forming the basis for possible future amendments.

The EPR aims to limit the availability of substances or mixtures that could be misused for the illicit manufacture of explosive to members of the general public with a view to ensuring the appropriate reporting of suspicious transactions throughout the supply chain (Article 1). Therefore, Regulation (EU) 2019/1148 is a content-specific act that follows a specific objective with regard to explosive precursors aligned with the broad DSA aim of contributing 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 are effectively protected.

*Personal scope*

The EPR applies to a defined set of actors involved in the making available, use, and monitoring of explosives precursors within the EU internal market. Its personal scope includes three main categories of regulated actors: economic operators (Article 3(10)) who make regulated explosives precursors available on the market, whether offline or online, and are directly subject to obligations concerning the sale, transfer, verification of licenses, and reporting of suspicious transactions (Articles 5-9); professional users (Article 3(9)) who acquire explosives precursors for purposes connected to their trade, business, or profession and for their own use only and Members of the general public (Article 3(8)) who are not permitted to acquire restricted explosives precursors above specified concentration thresholds unless authorised under a national licensing regime. Finally, the Regulation also includes in its personal scope online marketplaces (Article 3(11)) that act as mere intermediary services and are subject to specific obligations, such as informing users who aim to make regulated explosives precursors available through the use of their services of their obligations under the Regulation, and to implement technical and organisational measures that support compliance regarding verification of licenses (Articles 7(3) and 8(3))). Moreover, pursuant to Article 9, given the increasing significance of online marketplaces for all kinds of supply (including for terrorist purposes), they are subject to detection and reporting obligations, but detection procedures should be "properly adapted to the specific online environment". Recital 16 clarifies that this obligation should not amount to a general monitoring obligation on online marketplaces and exempts online marketplaces from liability for transactions that were not detected despite the online marketplace having in place appropriate detection procedures.

*Territorial scope*

The territorial scope of the EPR covers all Member States insofar as the activity in question takes place within or targets the internal market of the EU.
According to Article 1 EPR, also companies established outside of the EU are obliged carry out the monitoring and control measures (verification upon sale, inform the supply chain, and not make restricted explosive

[117] Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 - http://data.europa.eu/eli/reg/2019/1148/oj.

precursors available to the member of the general public) if they sell restricted explosives precursors to a customer that resides inside the EU.

*Material scope*

The EPR establishes a harmonised regulatory framework governing the availability, introduction, possession, and use of chemical substances and mixtures that may be used in the illicit manufacture of explosives. Its primary aim is to enhance public security while ensuring that legitimate professional and industrial uses of such substances are not unduly impeded.

The Regulation applies to both individual substances and mixtures that contain one or more explosives precursors above defined concentration thresholds, set out in Annexes I and II.
The core provisions are found in Articles 5 to 9, which outline licensing and prohibition regimes for sales to the general public (Article 5); obligations on economic operators and online marketplaces to inform users about regulatory requirements (Article 7); requirements for verifying customer identity and, where applicable, licenses (Article 8) as well as mandatory reporting of suspicious transactions, thefts, or disappearances (Article 9).

*Enforcement*

The enforcement mechanism under the EPR relies primarily on national-level implementation, inspection, and control in the "country of destination" (i.e. where the infringement is detected, regardless of the place of establishment of the marketplace). Member States are required to designate competent national inspection authorities (Article 11) and to ensure that those authorities have sufficient powers and resources to carry out effective enforcement. Member States are tasked with setting up 24/7 contact points for reporting and must ensure adequate training for enforcement actors (Article 10). Article 13 requires Member States to lay down effective, proportionate, and dissuasive penalties for infringements. Although the Regulation sets EU-level restrictions and requirements – such as the prohibition of sales of restricted precursors to the general public (Article 5) and licensing regimes (Article 6), the monitoring and sanctioning of compliance remain national. The Regulation establishes a safeguard clause (Article 14), which allows Member States to adopt emergency restrictions. Member States must also report annually to the Commission on enforcement metrics (Article 19), distinguishing between online and offline activity.

*Interactions with the DSA*

There is no mention of the DSA in the EPR. In the DSA, there is reference to the EPR in Recital 10 and Article 2(4)(d).

There is an interplay in **personal scope** between the EPR and DSA in that the EPR covers "online marketplaces", defined as "provider(s) of an intermediary service that allows economic operators on the one side, and members of the general public, professional users, or other economic operators, on the other side, to conclude transactions regarding regulated explosives precursors via online sales or service contracts, either on the online marketplace's website or on an economic operator's website that uses computing services provided by the online marketplace(s)" (Article 3(11); see also Recital 15). While the DSA does not provide a formal definition of "online marketplaces" in Article 3, the concept is functionally delineated in Recitals 23 and 24 and substantiated through obligations in Section 4, Chapter III. These provisions apply to providers of online platforms allowing consumers to conclude distance contracts with traders.

In terms of **material scope**, the interplay is one of the EPR effectively "plugging into" the DSA as the substantive illegality trigger by defining when certain products / transactions are unlawful (placing on the market or making available regulated precursors without compliance) and thus making them "illegal content" in the sense of the DSA Article 3(h). At the same time, the EPR preserves the DSA's liability regime and explicitly avoids general monitoring obligations – Recital 16 EPR and Article 9(2) EPR make clear that having "appropriate, reasonable and proportionate procedures" for suspicious transaction detection shields marketplaces from liability for what they failed to detect. This echoes the liability safe harbour of the DSA as per Articles 4-6 and 8 DSA.

Finally, unlike the DSA, which mandates harmonised **enforcement** standards under Article 51 in the country of establishment of the marketplace ("country of origin" principle), particularly in terms of coherence and coordination among national authorities, the EPR does not prescribe specific penalty levels, leaving enforcement frameworks entirely to Member States under Article 13. This divergence does not amount to a normative inconsistency but reflects the subsidiarity-based approach of the EPR, which targets product-specific risks and relies on national inspection authorities for enforcement.

*Special remarks on interplay*

Complementarity can be noted as regards Article 9(1, 4-6) EPR, which requires economic operators and online marketplaces to report suspicious transactions or attempted transactions, and thefts or disappearances of explosive precursors within 24 hours of detection to the national contact point of the Member State where the transaction was concluded or attempted, or where the disappearance or theft took place. This is also reflected under Article 18 DSA, which obliges providers of hosting services to inform competent authorities when they become aware of information giving rise to a suspicion of serious criminal offence involving a threat to life or safety. However, Article 9 (1, 4-6) EPR provides for specific types of conduct, the recipients of reports, and a strict 24-hour deadline. The EPR functions here as *lex specialis:* compliance with Article 9 EPR will typically satisfy Article 18 DSA where explosives precursors are involved.

Interplay occurs as regards Article 8(1) EPR, which governs the verification of prospective customers of the general public in terms of proof of identity and license, and Article 8(2) EPR, that relates to the information to be requested for the purpose of verifying that a prospective customer is a professional user or another economic operator.

By contrast, Article 30 DSA regulates trader traceability. Thus, both provisions may apply to the same online marketplace, but they regulate distinct relationships – one focusing on buyers of explosives precursors, the other on traders in digital marketplaces. Article 8(5) further requires providers of online marketplaces to take measures to help ensure that their users, when making restricted explosives precursors available through their services, comply with their verification obligations. This requirement complements the "compliance by design" obligation imposed on providers of online marketplaces under Article 31(1) DSA, which focuses on the provision of information by traders but does not concern the verification obligations of traders. In addition, unlike Article 31(1) DSA, Article 8(5) is formulated more broadly and is not limited to the design of the online interface of the marketplace. As emphasised in Recital 16 EPR, however, no obligation on online marketplaces under the EPR shall amount to a general monitoring obligation for the provider.

## Regulation (EU) 2019/1150 ([118]) – [Platform-to-Business Regulation]

*General Information*

The Platform-to-Business (P2B) Regulation was adopted on 20 June 2019 and applies since 12 July 2020. The first review was published in September 2023. The next review is expected to take place 3 years later (2026).

As per Article 1 P2B, the regulation lays down rules to ensure that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities, thereby contributing to the proper functioning of the Single Market. It aims to create a more predictable and balanced business environment by addressing power imbalances and ensuring business users have clear, transparent, and enforceable rights.

*Personal scope*

Online intermediation services mean services which meet all of the following requirements (Article 2(2) P2B):

- They constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 (any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services);
- They allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded;
- They are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers.

Online search engines are defined as a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found (Article 2(5) P2B).

Some rules for online intermediation services do not apply to small enterprises (i.e. rules on setting up internal complaint-handling systems (Article 11(5) P2B) and indicating two mediators in the terms and conditions (Article 12(7) P2B)).

*Territorial scope*

As per Article 1(2) P2B, the regulation applies to online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website users, respectively, that: Have their place of establishment or residence in the Union, and through those online intermediation services or online search engines, offer goods or services to consumers located in the Union, irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable.

*Material scope*

The P2B Regulation lays down rules for providers of online intermediation services on: their terms and conditions (e.g. they must be transparent, drafted in simple and understandable language and be easily available to business users); the restriction, suspension and termination of their services (providers must give a statement of reasons to the business concerned); and resolution of disputes (there is a requirement to set up internal

[118] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance).

complaint management systems to resolve disputes). For online search engines specifically, the regulation requires they disclose the main ranking parameters used for determining the ranking of indexed websites.

*Enforcement*

As per Article 15 P2B, each Member State is required to ensure adequate and effective enforcement of the regulation, leaving a certain flexibility for Member States to define the authority in charge.

In practice, the Court of Justice of the European Union (CJEU) has ruled that the country-of-origin principle applies, in two separate rulings: Joined Cases C-662/22 and C-667/22;[119] and Case C-665/22.[120]

*Interactions with the DSA*

The P2B Regulation was adopted before the DSA and does not contain any references to it. It also does not contain any references to Art. 12-15 e-commerce Directive (2000/31/EC).

The DSA makes reference to the P2B Regulation in several instances. In particular, the DSA clarifies that it is without prejudice to the P2B Regulation when it comes to other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA (Recital 10, Article 2(4e)).

Furthermore, the DSA provides that it is without prejudice to the P2B Regulation when it comes to providers of an online platform allowing consumers to conclude distance contracts with traders, refusing to allow a trader to use their service or suspending the provision of their service (Article 30(4) DSA), and the subsequent right for the trader to lodge a complaint pursuant to the DSA.

Regarding the **personal scope**, there is a full overlap in terms of personal scope: all services covered by the P2B Regulation are covered by the DSA. Both the DSA and P2B apply to online intermediary services (including online search engines), with the P2B applying only in a B2B context ("platform-to-business"), whereas the DSA applies both to B2B and B2C relationships. But the DSA applies also to other intermediary services such as mere conduits and caching services, or technical hosting services, which are not in scope of the P2B. The scope of the DSA is wider, with the P2B applicable only to a specific sub-set of intermediary services that allow business users to offer goods or services to consumers, and that are provided to these business users on a contractual basis. The definition of online search engine in P2B largely corresponds to the one contained in the DSA, which takes inspiration from and follow the one from the P2B Regulation.

On **territorial scope** the P2B Regulation, like the DSA, applies to online intermediary services and online search engines offering services in the EU, regardless of whether they are established inside or outside the Union.

On its **material scope**, the P2B Regulation focuses on the obligations of online intermediation services when businesses use them to offer goods and services to consumers. As such, overlaps include:

- Article 3 P2B and Article 14 DSA on terms and conditions,
- Articles 4 and 10 P2B and Article 17 and 23 DSA on restriction, suspension and termination of services,
- Article 5 P2B and Article 27 on transparency of ranking or recommender systems,
- Article 11 P2B and Articles 20 and 53 DSA on complaint-handling, and
- Article 15 P2B and Article 49 DSA on enforcement.

Article 12 and 13 P2B on mediation and Article 21 DSA on out-of-court dispute settlement contain separate provisions related to the settlement of disputes out of court. Whereas the P2B stipulates that providers of online

[119] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0662.
[120] https://eur-lex.europa.eu/eli/C/2024/4295/oj/eng.

intermediation services must identify in their terms and conditions two or more mediators they can engage with, and specifies the requirements that mediators must fulfil, the DSA states that service recipients can choose any certified out-of-court dispute settlement body, outlines the criteria for DSCs to certify out-of-court dispute settlement bodies, sets out the timeframes to settle disputes and stipulates that online platforms shall pay fees, with the dispute settlement either free of charge to service recipients, or at a nominal fee. As such, there is no duplication regarding mediation services, and both legal texts can co-exist. In general, the P2B would be considered a *lex specialis* in cases specifically concerning online intermediation services providing services to business users.

As regards **enforcement**, there is largely overlap between both instruments, both when it comes to Member States in appointing a national authority to enforce the P2B and the DSA, but also when it comes to the Commission as enforcement authority vis-à-vis the VLOPs/VLOSEs under the DSA. However, since the enforcement powers of the European Commission are not limited to Chapter V DSA but concern all due diligence obligations of VLOPs, there might be a conflict where a competent authority under the P2B enforces an overlapping obligation vis-à-vis a VLOP. For example, considering transparency of recommender systems (Article 27 DSA) and ranking provisions in the P2B (Article 5), the Commission could run an investigation in relation to Article 27 DSA, while the national authority would be looking at transparency of ranking criteria under Article 5 P2B.

*Special remarks on overlaps*

There are several overlapping points with regards DSA which should be noted:

- **Terms and Conditions**: When it comes to terms and conditions, the P2B provides for information obligations of the intermediary vis-à-vis the business user in order to prevent any unfair business relationships or abusive changes. In particular, the P2B requires providers of online intermediation services to set out the grounds for the suspension, termination or any other kind of restriction on the provision of their service to a business user. This overlaps with the general requirement for intermediary services under Article 14(1) DSA to provide in their terms and conditions information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service. In addition, business users must be notified about any changes to the terms and conditions on a durable medium and with a notice period of at least 15 days, otherwise such changes shall be null and void. This goes beyond the requirements in Article 14 DSA which does not include a similar obligation.

  The P2B Regulation is to be seen as lex specialis to the DSA, applying to intermediaries as defined in the P2B Regulation in their relationships with business users. The P2B rules should remain applicable insofar as the P2B regulates other aspects of the provision of intermediary services than the DSA or specifies or complements the rules of the DSA.
- **Information requirements following the restriction, suspension and termination of service**: Both the P2B (Article 4) and DSA (Article 17) set out information requirements following the restriction, suspension and termination of the service. Whereas however Article 4 P2B applies only to restrictions on business users, Article 17 DSA applies to all users. The content requirement of both statement of reasons partly overlaps. Both require information on the facts and circumstances relied on in taking the decision. The statement of reasons under the P2B however must explicitly also include the contents of third party notifications, that led to the decision whereas under Article 17 DSA, only the information that the decision was taken pursuant to a notice submitted in accordance with Article 16 must be included (without disclosing the content) and the identity of the notifier only added "where strictly necessary". In addition, Article 17 DSA requires information on the use of automated means, the available redress mechanisms and a reference to the relevant legal or contractual ground relied on, whereas Article 4 P2B more generally requires a reference to the relevant section in the terms and conditions. Furthermore, Article 4 P2B sets out a 30-day notice period for the termination of the service and requires that the statement of reason is provided on a durable medium, an obligation which is absent from the DSA. Similarly, the P2B complements the DSA when it comes to informing business users of any restriction, suspension or termination of B2B services, such as defined notice periods. The out-of-court dispute settlement provisions in the DSA (Article 21) relate to such restriction, suspension or termination whereas the obligation relating to out-of-court mediation in

the P2B (Article 12 and 13) is broader and applies to any dispute arising between the platform and its business user in relation to the service provided.

The P2B Regulation is to be seen as lex specialis to the DSA, applying to intermediaries as defined in the P2B Regulation in their relationships with business users. The P2B rules should remain applicable insofar as the P2B regulates other aspects of the provision of intermediary services than the DSA or specifies or complements the rules of the DSA.

- **Ranking transparency**: The DSA (Article 27) and P2B (Article 5) overlap in their provisions related to transparency around the parameters determining the ranking of goods or services offered through online intermediation services and online platforms, which are required to be set out in the terms and conditions and in a publicly available description, respectively. Article 5 P2B stipulates that, where the parameters include the possibility of payment to influence ranking, the service provider must detail the impact of payment on ranking. The information provided on ranking parameters should enable business users and corporate website users to understand how the ranking takes account of the characteristics of the goods and services, the relevance of those characteristics for consumers, and the design characteristics of online search engines used by corporate website users.

  Article 27 DSA on recommender system transparency states that providers of online platforms must set out in their terms and conditions, in plain and intelligible language, the main parameters used, options to influence the parameters, as well as the criteria determining ranking and the reasons for their relative importance. Article 39 DSA contains additional provisions on online advertising transparency related to VLOPs and VLOSEs, who are required to maintain a public repository containing details on advertisements they present.

  Both legal texts contain overlapping requirements related to ranking transparency, though the P2B contains more specific information regarding how specific criteria impact ranking, including payment. The P2B targets the specific needs of business users where the recommender system transparency obligations in the DSA cover both B2B and B2C. However, the DSA contains provisions specific to VLOPs and VLOSEs that present advertisements. The two legal instruments are designed to operate in parallel, without contradiction, since both instruments foresee that the terms and conditions of the platform shall contain the main parameters used, making the individual requirements complementary. The P2B rules apply insofar as tit regulates other aspects of the provision of intermediary services than the DSA or specifies or complements the rules of the DSA.

- **Internal complaint handling**: The internal complaint-handling system imposed for online platforms by the DSA (Article 20) relates to decisions taken by the platform on restriction, suspension or termination of services, whereas the obligation relating to internal complaint-handling system in the P2B (Article 11) is broader, in particular covering alleged non-compliance by the intermediary with any obligation laid down in the P2B.

  Article 11 P2B and Article 20 DSA relate to the internal complaint-handling system available to business users of online intermediation services and users of online platforms, respectively. Article 11 P2B provides that this system is required to be easily accessible and free of charge for business users, with responses provided within reasonable timeframes and based on the principles of transparency, equal treatment and proportionality. Providers of online intermediation services are required to process complaints swiftly and effectively, and communicate the results in a clear manner. Additionally, they must publish information on their internal complaint-handling system every year. This publicly available information must include the total number of complaints lodged, the main types of complaints, the average time period needed to process the complaints and aggregated information regarding the outcome of the complaints.

  According to Article 20 DSA, the internal complaint-handling system must be easily accessible and free of charge to users who have submitted a notice pertaining to a prior decision made by the online platform (e.g. suspension/termination of account/service due to illegal content or incompatibility with its terms and conditions). It should be available for at least six months following this decision. Providers of online

platforms are required to handle complaints in a timely, non-discriminatory, diligent and non-arbitrary manner, and inform of their decision without undue delay. As per Article 15 DSA, providers of intermediary services are required to make publicly available information on the number of complaints received, at least once a year. Online platforms, additionally, must provide the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed.

Both legal texts contain similar provisions, apply in different but complementing situations and can co-exist. The P2B should be considered a lex specialis in its treatment of complaints submitted by business users specifically and beyond decisions taken by the platform on restriction, suspension or termination of services. The P2B rules apply insofar as tit regulates other aspects of the provision of intermediary services than the DSA or specifies or complements the rules of the DSA.

- **Enforcement**: Article 15 P2B **s**tipulates that Member States shall ensure adequate and effective enforcement of the P2B, with national authorities appointed as the primary enforcement authority. Article 49 DSA provides that Member States appoint Digital Services Coordinators as a competent authority, and also foresees an enforcement role for the Commission with regard to VLOPs and VLOSEs.

  There is no contradiction given the sufficient flexibility for Member States to organise national enforcement under the P2B Regulation. However, since the enforcement powers of the Commission are not limited to Chapter V DSA but concern all due diligence obligations of VLOPs, there might be a conflict where a competent authority under the P2B enforces an overlapping obligation vis-à-vis a VLOP. For example, considering transparency of recommender systems (Article 27 DSA) and ranking provisions in the P2B (Article 5), the Commission could run an investigation in relation to Article 27 DSA, while the national authority would be looking at transparency of ranking criteria under Article 5 P2B. As mentioned before, the Court of Justice of the European Union (CJEU) has ruled that the country-of-origin principle applies, in two separate rulings: Joined Cases C-662/22 and C-667/22;[121] and Case C-665/22.[122]

[121] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0662.
[122] https://eur-lex.europa.eu/eli/C/2024/4295/oj/eng.

# Regulation (EU) 2021/784 ([123]) – [Terrorist Content Online Regulation]

*General Information*

Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online ("Terrorist Content Online Regulation" or "TCO") was adopted by the European Parliament and the Council on 29 April 2021 and entered into force on 6 July 2021. The Regulation became applicable as of 7 June 2022. It was introduced as part of the Union's broader counterterrorism and digital security strategy, aimed at enhancing the effectiveness and coordination of efforts to remove terrorist content from online platforms while safeguarding fundamental rights, particularly freedom of expression and access to information.

The TCO Regulation establishes directly applicable obligations on hosting service providers ("HSPs") who disseminate information to the public and empowers national competent authorities to issue removal orders to ensure the removal or disabling of access to terrorist content. The Regulation also sets out harmonised rules on transparency reporting, complaint mechanisms, preservation of evidence, and cooperation among Member States. A review of the Regulation's effectiveness is foreseen under Articles 21-23, which obliges the Commission to assess its implementation and functioning by 7 June 2024, and report to the European Parliament and Council. In February 2024, the Commission published a report on the implementation of the Regulation.[124]

*Personal scope*

The TCO Regulation applies to HSPs, defined under Article 2(1) TCO as any provider of services consisting of the storage of information provided by and at the request of a content provider. In addition, according to Article 1(2) TCO the obligations under the Regulation apply only whenever such HSPs disseminate content to the public at the request of the content provider., The TCO Regulation does not apply to interpersonal communication services as defined in Article 2(5) of Directive (EU) 2018/1972 ("European Electronic Communications Code") such as email or private messaging services.

*Territorial scope*

The territorial scope of the TCO Regulation extends beyond the borders of the European Union and applies to all HSPs that offer services in the European Union, irrespective of their place of establishment. This means that even providers established outside the Union fall within the Regulation's territorial scope if they make their services available within the EU. This extraterritorial reach is explicitly set out in Article 1(2). HSPs without a main establishment in the Union have to designate a legal representative in the Union to ensure the enforcement of the Regulation (Article 17 TCO).

*Material scope*

The TCO's material scope is defined to apply specifically to terrorist content, which is defined in Article 2(7), and mirrors the definition in the EU Directive on Combating Terrorism (Directive (EU) 2017/541)[125]. The Regulation establishes the legal basis for removal orders on terrorist content (Article 3 and 4) and sets out the respective obligations of HSPs, it further includes provisions for HSPs exposed to terrorist content (Article 5), on preservation of data linked to removed content (Article 6), transparency and redress obligations (Articles 7-11), and cooperation between national authorities and with the Commission (Sections IV and V).

---

[123] Regulation (EU) 2021/784, on addressing the dissemination of terrorist content online.

[124] COM(2024) 64 final.

[125] Under the TCO, "terrorist content" includes material that incites the commission of terrorist offences, solicits the participation in a terrorist group, provides instruction on how to commit terrorist offences, and/or encourages the contribution to such activities.

*Enforcement*

The enforcement structure of the TCO Regulation is primarily decentralised. Under Article 12, each Member State must designate one or more competent authorities responsible for issuing removal orders, scrutinising cross-border removal orders, overseeing specific measures, and imposing penalties. These authorities must act independently, objectively, and with full respect for fundamental rights (Article 13). Each must establish a contact point to handle clarifications related to removal orders. As required by Article 14, competent authorities must cooperate with each other (particularly to avoid duplication and interference on investigations across different Member States), with Europol (especially where coordinated efforts are needed), and through secure communication mechanisms (by using tools such as Europol's platforms to facilitate exchanges and feedback on removal orders).

Under Article 15, hosting service providers must designate a contact point for the receipt of removal orders and ensure communication can be handled in official EU languages, including at least that of the Member State of main establishment or legal representation. Additionally, providers without an EU establishment must designate a legal representative in the EU (Article 17), who may be held liable for compliance failures.

The Member State of main establishment has jurisdiction over enforcement, including penalties and proactive measures (Article 16). For providers without an EU establishment, the Member State where their legal representative is based assumes jurisdiction. If no representative is designated, all Member States may assert jurisdiction.
Per Article 18, Member States must adopt effective, proportionate, and dissuasive penalties for non-compliance. Specific infringements covered include failures to act on removal orders (Article 3), implement specific measures (Article 5), preserve data (Article 6), fulfil transparency or redress obligations (Articles 7, 10, 11) and appoint or empower legal representatives (Article 17). In cases of systematic or persistent failure to comply with obligations pursuant to removal orders (Article 3(3)), financial penalties may reach up to 4% of global annual turnover.

Articles 21–22 establish that Member States must report to the European Commission annually on removal orders issued, content taken down, proactive measures and complaint outcomes, and data access and enforcement actions.

*Interactions with the DSA*

As per Article 2(4)(c) DSA, the DSA is without prejudice to provisions of the TCO regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing this Regulation.

The TCO does not refer to the DSA directly because it was adopted in April 2021, before the adoption of the DSA in October 2022. It therefore builds on the e-Commerce Directive (Directive 2000/31/EC), with Article 1(5) and Recital 7 confirming that any measures taken by a HSP in compliance with the TCO Regulation should not in themselves lead to a loss of the exemption of liability established under the e-Commerce Directive. Similarly, Article 5(8) TCO echoes Article 15(1) of the Directive by prohibiting general monitoring or fact-finding obligations, while allowing the voluntary use of automated tools in line with Recital 25. With entry into force of the DSA, these references to the e-Commerce Directive now refer to the DSA as Article 89 DSA provides that references to Articles 12-15 of the e-Commerce Directive are to be read as references to Articles 4-6 and 8 DSA. Accordingly, the safeguards on liability exemptions and the ban on general monitoring obligations in the TCO are now interpreted consistently with the corresponding DSA framework. The DSA explicitly references the TCO in Recital 10, Recital 34, and Article 2(4)(c).

On **personal scope**, while the DSA applies to all providers of "intermediary services", as defined in Article 3(g) DSA, including providers of "mere conduit", "caching" and "hosting" services, the TCO covers only "hosting service providers", and only insofar as they disseminate information to the public (Article 1(2) TCO). This distinction implies that not all hosting service providers as defined under Article 3(g)(iii) DSA are subject to the TCO Regulation. Instead, the Regulation mainly applies to hosting service providers that qualify as "online platforms" under Article 3(i) DSA, a definition that did not exist when the TCO Regulation was first adopted,

as it predates the DSA. Beyond online platforms, the TCO Regulation however also covers HSPs for whom the dissemination of information to the public constitutes only an ancillary feature of another service or a minor functionality of the principal service. These services are excluded from the definition of an "online platform" under the DSA and fall within its broader category of HSPs. Therefore, the personal scope of the TCO Regulation overlaps fully with, but is more limited than, the personal scope of the DSA.

Regarding **territorial scope**, both instruments apply to providers not established in the EU if they offer services within the Union, creating alignment in terms of territorial scope

As regards as **material scope**, the TCO establishes a sector-specific regime exclusively for the removal of terrorist content. As such it sets out the legal basis for competent authorities to issue removal orders to HSPs under Articles 3 and 4 and requires hosting service providers to act within one hour of receiving a removal order. Article 17 further obliges HSPs not established in the Union to designate a legal representative for the receipt of such orders.

The DSA, under Article 9, sets out general requirements for orders to act against illegal content, but explicitly states in Recital 34 that these requirements are without prejudice to other Union acts which confer specific powers to order the removal of content - including the TCO Regulation. Orders issued in accordance with Article 3 and 4 TCO Regulation therefore do not have to fulfil the requirements set out in Article 9(2) DSA but must be issued using the template provided in Annex I TCO Regulation. In other words, if a removal order concerns terrorist content, this will trigger the application of the provisions under the TCO, as *lex specialis.* If a removal order however does fulfil all the requirements set out in Article 9(2) it triggers the information obligation of the HSP under Article 9(1) DSA. In addition, while the DSA under Article 13 obliges providers of intermediary services (including all HSPs) without an establishment in the Union to designate a legal representative, this representative does not serve to receive orders issued in accordance with Article 9. Instead, such orders must be sent to the electronic point of contact designated by that provider in accordance with Article 11 DSA. This point of contact is however intended primarily for operational communication and does not require a physical presence.

Articles 7 to 11 of the TCO introduce due diligence obligations regarding transparency, complaint mechanisms and redress, specific to the removal of terrorist content, which apply in addition to the DSA's horizontal requirements. Article 7(2) TCO requires hosting service providers to publicly report on their actions against terrorist content, Article 10 obliges HSPs to establish an effective and accessible internal complaint mechanism and Article 11 TCO sets out an obligation for service providers to inform content providers after removal of terrorist content about the reasons and available redress options. The DSA imposes horizontal, but detailed, mechanisms and safeguards for the removal of any type of illegal content: Article 17 DSA requires HSPs to provide a statement of reason for removals based on the providers' own decisions or user notices, Article 9(5) requires any provider of an intermediary service, including HSPs, to inform users about content which has been taken down pursuant to an order under Article 9, and Article 20 obliges online platforms to provide an internal complaint-handling system for decisions taken on the grounds that information constitutes illegal content or violates the providers terms and conditions.

Both frameworks rely on Member State-level authorities and territorial establishment or legal representation to assert jurisdiction, but they differ in their **enforcement** structures. The TCO designates national competent authorities to issue and monitor removal orders (Articles 3-5) and relies more on a decentralised model without an EU-level coordinating body, whereas the DSA centralises oversight through Digital Services Coordinators and the European Commission. The TCO imposes narrow, time-bound obligations, such as the one-hour removal deadline, due to the higher security risks related to terrorist content. The DSA instead applies broader systemic supervision related to risk mitigation, transparency, and due diligence, due to its horizontal nature. Both instruments foresee significant sanctions of up to 4% of global turnover under Article 18(3) TCO for systemic non-compliance with removal obligations, and up to 6% under Article 52 and 74 DSA for violations across the Regulation's scope. Recital 34 and Article 2(4)(c) DSA clarify that the DSA is without prejudice to other instruments regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA, such as the TCO. Simultaneous enforcement actions may however arise where an HSP fails to comply with its obligations regarding the dissemination of terrorist content under

the TCO, which at the same time indicates a breach of due diligence obligations in terms of illegal content under the DSA.

*Special remarks on overlaps*

Both the DSA and the TCO Regulation therefore provide for similar systems of due diligence obligations, with similar safeguards and mechanisms, but sector-specific in the case of the TCO. Some relevant aspects could be highlighted:

- **Transparency reporting:** Both the DSA and the TCO impose transparency reporting obligations on HSPs, but with different scopes, formats and timelines. Article 15 DSA requires all intermediary service providers, including HSPs, to publish annual transparency reports covering content moderation activities, taken with regards to any form of content, including the number of removal orders received, types of illegal content, and other relevant metrics. In contrast, Article 7(2) TCO imposes a more sector-specific and time-sensitive obligation: if a provider has taken action against terrorist content or received a removal order, it is required to publish a transparency report by 1 March of the following year, regardless of whether it already complies with the DSA's reporting schedule. The TCO report is thus limited to actions against terrorist content, and requires detailed breakdowns of compliance with TCO obligations, in particular with regards to removal orders.

  Since the reporting requirements are different in timelines, content, structure and function, they apply simultaneously and providers who are subject to both instruments are required to produce two reports one general under the DSA and one specific under the TCO. However, the absence of an explicit reference to the TCO transparency reporting obligations in the DSA may create uncertainty as to whether the same information disclosed under Article 15 DSA can also satisfy Article 7(2) TCO, or whether two reports must be separately prepared to comply with both instruments.

- **Statement of reasons**: Both the DSA and the TCO Regulation require HSPs to inform users when their content has been taken down. Under Article 11 TCO Regulation, the HSP must at first only notify the content provider by indicating that the content has been removed or access to it has been disabled in accordance with the Regulation. Further information about the reasons for the removal or disabling as well as the remedies for the removal or disabling must be provided only upon request of the content provider (Recital 34). Article 17 DSA on the other hand introduces a more proactive approach. It obliges HSPs to issue a detailed statement of reasons to any affected recipient whenever content is restricted, whether based on their own decisions or on user notices. These statements must also be made publicly available through the Transparency Database established under Article 24 DSA. For content removals following a removal order issued in accordance with Article 9 DSA, the provider of an intermediary service, including a HSP, must inform the affected user about the order received and the effect given to it, including a statement of reasons, information about the available redress options as well as a description of the territorial scope of the order.

  For the removal of terrorist content based on a provider's own decisions or user notices, both Article 11 TCO Regulation and Article 17 DSA apply simultaneously for HSPs subject to both Regulations. However, the detailed statement of reasons required under Article 17 DSA also satisfies the more general information obligations set out in Article 11 TCO Regulation, and therefore one notification in accordance with Article 17 DSA would fulfil both obligations. On the other hand, when terrorist content is removed following a removal order, both frameworks only require a general user notification, including a statement of reasons.

- **Complaint mechanism**: Article 10 TCO Regulation as well as Article 20 DSA require online platforms to establish an internal complaint handling mechanism for content removals. Neither provision applies however to content removals pursuant to orders, as these follow their own redress structure. While Article 10 TCO Regulation applies specifically to the removal of terrorist content, Article 20 DSA covers the removal of all types of content. Consequently, when an online platform removes terrorist content pursuant to specific measures under Article 5 TCO Regulation, the obligations under Article 10 TCO Regulation and Article 20 DSA apply simultaneously, since terrorist content also qualifies as illegal content under the DSA.

An online platform can potentially be subject to both regimes if exposed to terrorist content. In this case it must therefore comply with both provisions, which are largely aligned and can operate complementarily. For example, Article 20 DSA requires the complaint handling mechanism to be provided free of charge, a requirement not explicitly stated in Article 10 TCO Regulation but compatible with it. In cases where the requirements under Article 20 DSA are contradictory to Article 10 TCO Regulation, the latter prevails.

- **Notification of suspicions of criminal offences**: Under Article 14(5) TCO Regulation, if a HSP becomes aware of terrorist content involving an imminent threat to life, it must promptly inform the authorities competent for investigating and prosecuting criminal offences in the Member States concerned or Europol. The DSA establishes a similar but broader obligation. Under Article 18 DSA, HSPs must promptly inform the law enforcement or judicial authorities of the Member State concerned when they become aware of any information that gives rise to a suspicion of a criminal offence involving a threat to the life or safety of a person.

  Accordingly, the reporting obligation under Article 14(5) TCO Regulation is narrower in scope, both in terms of the type of content, being limited to terrorist content, and the protected interests, covering threats to life but not to personal safety. The competent authority to be notified may be the same or different under the two regimes, depending on how competencies are distributed within the respective Member State. When an HSP becomes aware of terrorist content indicating an imminent threat to life Article 14(5) TCO Regulation would prevails as the more specific obligation for the notification of terrorist content.

In conclusion, although some aspects are addressed in both Regulations (statement of reasons, complaint mechanisms, transparency reports), the two regimes apply in a complementary way, with the DSA providing a horizontal framework to address illegal content online and the TCO Regulation adding additional, sector-specific requirements for terrorist content.

# Regulation (EU) 2022/1925 ([126]) – [Digital Markets Act]

*General Information*

The Digital Markets Act (DMA) was adopted on 14 September 2022 and applied from 2 May 2023 (certain Articles applied from 1 November 2022 and 25 June 2023). The first review will take place by 3 May 2026.

As per Article 1 DMA, the Regulation lays down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users. The DMA lays down obligations that apply to the designated gatekeepers as regards relevant core platform services, thereby aiming to create more fair and contestable digital markets.

*Personal and territorial scope*

As per Article 1(2) DMA, the Regulation applies to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service. The DMA provides an exhaustive list of such core platform services in Article 2(2) DMA. Gatekeepers are those undertakings that:

- have a significant impact on the internal market (EU turnover of at least EUR 7.5 billion in each of the last three financial years, or an average market capitalisation or market value of at least EUR 75 billion in the last financial year, and provides the same core platform services in at least three MS);
- provide a core platform service which is an important gateway for business users to reach end users (at least 45 million monthly active end users established or located in the EU and at least 10,000 yearly active business users established in the EU, in the last financial year);
- enjoy an entrenched and durable position, in their operations, or it is foreseeable that they will enjoy such a position in the near future.

However, the DMA does not apply to: electronic communications networks as defined in Article 2, point (1), of Directive (EU) 2018/1972; and electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972, other than those related to number-independent interpersonal communications services.

*Material scope*

The DMA outlines the obligations placed on gatekeepers. For example, gatekeepers are required to: allow third parties to inter-operate with the gatekeeper's own specific core platform services (e.g. number-independent interpersonal communication services; operating systems); allow their business users to access the data that they generate in their use of the gatekeeper's platform; provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper; allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform. Furthermore, gatekeepers are prohibited to: process consumers' personal data collected from third-party services for the purpose of providing online advertising services, without prior consent; prevent business users from offering their products and services under different prices and conditions on their own sales sites, as well as on third-party platforms; and rank gatekeeper products or services higher than those of other businesses.

[126] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance).

The DMA prohibits the practice of self-preferencing (Article 6(5) DMA) by gatekeepers, meaning a more favourable treatment in indexing and ranking of their own products and services. In this context, the DMA also requires gatekeepers to apply transparent, fair and non-discriminatory conditions to such ranking. At the same time, the DSA requires all online platforms to describe the main parameters of their recommender systems in their terms and conditions (Article 27 DSA). Both the DMA and DSA address opacity issues with online advertising: the DMA requires real-time, cost-free access for advertisers, publishers, and third parties to ad portfolio information, enabling ad verification and performance assessment (Article 6(8)). The DSA complements the DMA by increasing digital advertising transparency. VLOPs and VLOSEs must maintain a public advertisement repository for the duration of advertisement presentation and one year after (Article 39).

The DMA and DSA are complementary to each other when it comes to transparency of ranking and recommender system respectively, as both instruments pursue the general objective of transparency, but from the perspective of specific complementary objectives that the two Regulations pursue. In particular, while the DMA aims to ensure that there is no-self preferencing by the gatekeeper of its own services in ranking and requires transparency of ranking conditions to preserve contestable core platform services, the DSA aims to provide for a transparent online environment by requiring online platforms to inform recipients of their service of the main criteria and reasons in determining the information shown to the recipients of the service.

*Enforcement*

The Commission is the sole authority empowered to enforce the DMA (Recital 91 DMA). It has, among others, the power to designate gatekeepers, conduct market investigations and inspections, adopt non-compliance decisions in absence of effective compliance and impose fines for non-compliance (Chapters IV and V).

*Interactions with the DSA*

Both instruments were negotiated and adopted in parallel, but they do not contain any cross-reference, as they were designed as purely complementary.

Regarding the **personal scope**, the DMA applies to core platform services as defined in Article 2(2) DMA some of which coincide with intermediary services covered by the DSA. Out of the core platform services defined in the DMA, these services could include: online intermediation services; online search engines; online social networking services; video-sharing platform services; number-independent interpersonal communications services; loud computing services; and online advertising services. The DMA primarily focuses on fostering a fair and contestable digital markets where "gatekeepers" are present. In contrast, the DSA aims to ensure safe online environment, by providing framework for tackling illegal and harmful content and applies to a broader range of providers of intermediary services. The DSA also sets out a similar threshold for recipients of the relevant services for determining Very Large Online Platforms and Very Large Online Search Engines as it is the one of end users of a core platform service under the DMA, with both referring to 45 million monthly active recipients of the service and end users respectively. The DSA contains provisions specific to VLOPs and VLOSEs. Section 5 of the DSA outlines the additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks.

On **territorial scope** the DMA, like the DSA, applies to core platform services provided or offered by gatekeepers to business users established in the EU or end users established or located in the EU, regardless of where the gatekeepers are established.

With regards to **material scope**, both the DSA and DMA apply to intermediary services. However, they have different focuses and objectives. The DMA primarily focuses on fostering fair and contestable digital markets, targeting "gatekeeper" platforms with considerable market power. The DSA aims to tackle illegal and harmful content and applies to a broader range of online platforms and services. Both instruments thereby pursue different and primarily complementary objectives and there is no material overlap between the obligations imposed on platforms in both instruments, which does not mean that in certain cases these obligations may not deal with similar issues but from the perspective of the respective complementary objectives.

On **enforcement,** whereas the Commission is exclusively responsible for enforcing the DMA, the enforcement of the DSA is the competence of the national Digital Service Coordinators and the Commission with regards to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs).

*Special remarks on interplay*

Both the DSA and DMA apply to intermediary services regarding their personal and territorial scope. However, they have different focuses and objectives when it comes to their material scope.

The DMA primarily focuses on fostering fair and contestable digital markets, targeting "gatekeeper" platforms with considerable market power. The DSA aims to tackle illegal and harmful content and applies to a broader range of online platforms and services. Both instruments thereby pursue different and primarily complementary objectives and there is no material overlap between the obligations imposed on platforms in both instruments, which does not mean that in certain cases these obligations may not deal with similar issues but from the perspective of the respective complementary objectives.

## Regulation (EU) 2023/988 ([127]) - [General Product Safety Regulation]

*General Information*

The General Product Safety Regulation (GPSR) was adopted on 10 May 2023 and applies since 13 December 2024. It has different evaluation dates on various issues, with a general evaluation foreseen by the 13 December 2029.

The GPSR lays down the general safety framework for consumer products placed or made available on the Union market in order to improve the functioning of the internal market while providing for a high level of consumer protection (Article 1).

*Personal scope*

The GPSR formulates obligations for a series of economic operators: manufacturers (Article 9 GPSR), authorised representatives (Article 10 GPSR), importers (Article 11 GPSR), distributors (Article 12 GPSR) other parties who can be deemed to be manufacturers for the purposes of the Regulation (Article 13 GPSR) and other economic operators, including the EU responsible person or fulfilment centres. In addition, Chapter IV GPSR establishes specific obligations for providers of online marketplaces.

A single entity may fall under multiple categories depending on their business model, and economic operators bear specific duties when their products are sold on the market online or other means of distance sales. Of relevance here are the obligations that the GPSR prescribes on providers of online marketplaces. Such a provider is defined in Article 3(14) GPSR as "a provider of an intermediary service using an online interface which allows consumers to conclude distance contracts with traders for the sale of products." An online interface is defined in Article 3(15) GPSR as "any software, including a website, part of a website or an application, including mobile applications." The Regulation does not define the concept of intermediary service.

*Territorial scope*

Article 1 GPSR determines that the Regulation applies to consumer products placed or made available on the internal market. Distance selling, including online sales, fall into the scope of the Regulation.[128] The GPSR applies therefore also to economic operators and providers of online marketplaces established outside of the European Union who target EU consumers and place or make available products on the EU market.

*Material scope*

The GPSR prescribes multiple obligations relating to risk assessment and documentation, labelling, traceability and corrective actions. It also specifies obligations directed at providers of online marketplaces, which build on the obligations addressed to providers of intermediary services set out in the DSA.

*Enforcement*

The GPSR is enforced primarily by national market surveillance authorities in each EU Member State, who are responsible for monitoring compliance, investigating unsafe products, and ordering recalls or removals where necessary. These authorities are part of the Consumer Safety Network, which is coordinated by the Commission. They can also require online marketplaces to take down dangerous product listings and cooperate through designated contact points. The European Commission supports enforcement through tools like the Safety Gate

[127] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, OJ 2023 L 135, 1–51.
[128] Recital 20 GPSR.

Rapid Alert System and the Safety Gate Portal, which facilitate rapid alerts and coordination across the EU and also via innovative market surveillance tools (interoperability solution and the EU eSurveillance tool). The Safety Business Gateway is a channel for economic operators to comply with their obligation to inform authorities and consumers of dangerous products and accidents. Nevertheless, some obligations of Chapter IV of the GPSR fall under the DSA enforcement regime.

*Interactions with the DSA*

The DSA is referred to in the preamble of the GPSR (Recitals 47, 50, 51, 53, 56, 57, 58) and in Article 22. As per Article 2(4)(f) DSA, the DSA is without prejudice to the General Product Safety Directive, which the GPSR replaced.

On **personal scope**, the DSA (which regulates intermediary services) and the GPSR (which is a product safety legislation) define their respective personal scope on the basis of different concepts. There is an interplay, since both apply to some providers of intermediary services within the meaning of the DSA.

Article 22 GPSR applies to providers of online marketplaces, which are a subcategory of providers of online platforms as defined in Art 3(i) DSA. There is no reference or definition of an "online marketplace" under the DSA, but the text of the Regulation refers multiple times to "online platforms that allow consumers to conclude distance contracts."

Regarding the **territorial scope**, the GPSR applies to consumer products that fall under its scope as a safety net, which are placed on or made available in the EU market, regardless of where they are manufactured or where the business involved is based. Meanwhile, the DSA regulates services that are offered to recipients in the EU, regardless of their place of establishment.

With regards to **material scope**, in most instances, the GPSR complements and specifies the DSA. The main nexus between the two instruments is Article 22 GPSR, which is detailed as follows:

- Article 22(1) and (2) GPSR stipulate that providers of online marketplaces must implement two contact points (one for consumers, one for market surveillance authorities) for the purpose of notifying orders and direct communications relating to product safety. These obligations are introduced without prejudice of the obligation on providers of intermediary services provided for by Articles 11 and 12 DSA to set up contact points for national authorities, the Commission and the European Board for digital services, and for the recipients of intermediary services. The DSA demands these contact points to be easily accessible, up to date, user-friendly, and to be provided in some language spoken in the Union. These aspects are absent from the GPSR. There is no conflict or inconsistency between the DSA and the GPSR in respect of these requirements. Rather, the single point of contact under the GPSR might be the same as the point of contact under Articles 11 and 12 DSA (Recital 50, 51 GPSR).

- Article 22(1) GPSR requires providers of online marketplaces to register with the Safety Gate Portal, which is part of the Safety Gate Rapid Alert System for non-food products that is set up in Articles 25 to 27 GPSR. This registration is essential in order to regularly receive information on dangerous products notified by the market surveillance authorities. No such obligation exists under the DSA. The GPSR therefore imposes an additional obligation on online marketplaces. Under Article 31(3) DSA, providers of online marketplaces are however subject to an obligation of due diligence, which require them to "make reasonable efforts to randomly check in any official, freely accessible and machine-readable online database or online interface whether the products or services offered have been identified as illegal." The GPSR, in its Article 22(7), specifies that for providers of online marketplaces these databases must include the Safety Gate Portal.

- Article 22(3) GPSR requires providers of online marketplaces to put "internal processes for product safety in place in order to comply without undue delay with the relevant requirements of this Regulation." This duty is similar to one of the potential risk mitigation measures reserved to very large online platforms by

the DSA (Article 35(1)(f) DSA). Here too, the GPSR merely stipulates an obligation that complements the obligations of the DSA with not being limited only to VLOPs.

- Under Article 22(4) GPSR, market surveillance authorities should be empowered, as regards specific content referring to an offer of a dangerous product, to issue an removal orders, in accordance with the minimum conditions set out in Article 9(2) DSA; providers of online marketplaces have to process such orders and act without undue delay, and in any event within two working days from receipt of the order. Paragraph 5 further states that such orders could also require the marketplace to prevent the reappearance of a given offer, to the extent that it does not require require the provider of an online marketplace to carry out an independent assessment of that content, and that the search and the removal can be carried out in a proportionate manner by reliable automated tools.

- Under Article 22(8) GPSR, providers of online marketplaces are required to process product safety notices "without undue delay and in any event within three working days" of receipt. This obligation complements Article 16 of the DSA, which obliges providers of hosting services – of which online marketplaces are a sub-set - to establish notice and action mechanisms for illegal content, without however determining a particular deadline to respond, regulating only that such notices must be processed "in a timely, diligent, non-arbitrary and objective manner".

- According to article 22(11) GPSR, providers of online marketplaces – for the purpose of compliance with Article 23 DSA - are required to suspend their service, for a reasonable period of time and after prior warning, to economic operators who frequently offer non-compliant products. This obligation therefore specifies the due diligence obligation under Article 23 DSA for providers of online marketplaces in the area of product safety.

- The GPSR further develops the obligations of providers of online platforms in respect of compliance by design (Article 22(9)). Article 31(1) DSA requires providers to make sure that their interface "is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information under applicable Union law." The interface must, on the ground of Article 31(2) DSA allow traders to provide information that allows the unambiguous identification of the product, the identification of the trader, and the information on marking and/or labelling. Article 22(9) GPSR further elaborates these requirements for product-related information on both the manufacturer and the product itself. The GPSR here complements the DSA.

- Article 22(12) GPSR formulates obligations of cooperation with national authorities for the proper enforcement of product safety rules. Here too, the GPSR complements the DSA, whose provisions on cooperation focus on specific institutional mechanisms distinct from the rules of the GPSR.

Finally, on **enforcement**, the DSA includes direct enforcement powers for the European Commission at European level and Digital Services Coordinators at national level, whereas the GPSR relies on national enforcement by Member States. However, some of the new obligations established under the GPSR merely "plug in" to the DSA and are to be enforced also by Digital Services Coordinators and the Commission, where appropriate.

*Special remarks on interplays*

The DSA and the GPSR are mutually supportive and complementary in respect of traceability.

The DSA provides for a system that ensures the traceability of traders to increase transparency and accountability in online marketplaces. Under Article 30 DSA, platforms that allow consumers to conclude distance contracts with traders must ensure that those traders provide essential information before being permitted to list products or services. This includes the trader's name, contact details, company registration information, and payment details, as well as confirmation that the product complies with applicable EU rules. Platforms are required to make reasonable efforts to verify the reliability of this information and must display

it clearly to consumers. These obligations are intended to help identify rogue sellers and enhance consumer trust in online transactions. The GPSR on the other hand requires economic operators, such as manufacturers, importers, and distributors, to ensure that products can be traced through the supply chain. This includes clear labelling with information such as the product type, batch or serial number, and the name and contact details of the responsible economic operator. When products are sold online, the GPSR mandates that this traceability information be made available to consumers at the time of purchase, just as it would be in a physical store. Online marketplaces are required to design their interface to enable traders to provide this information, ensure that the information is provided by the trader before the listing is published and make best effort checks whether the information has been provided. These traceability rules are designed to support effective recalls, improve market surveillance, and ensure that unsafe products can be quickly identified and removed. They are complementary in that the DSA provisions focus on the traceability of traders whereas the GPSR focuses on the information on manufacturers and other relevant economic operators and traceability of products. Moreover, the DSA provides for procedural obligations which are absent from the GPSR. A trader benefits from a right to lodge a complaint against measures of suspension implemented by providers of intermediary services under Article 30(4) DSA, which is not provided for in the context of the GPSR.

Last but not least, the GPSR also interacts with the DSA when it requires online marketplaces (along with economic operators) to inform consumers on safety recalls and safety warnings. Under Article 35 GPSR, in the event of a product safety recall or a safety warning, providers of online marketplaces are obliged to directly notify all affected consumers who purchased the relevant product through their interfaces, without undue delay. Online product listings must also contain safety instructions, warnings, and the identity/contact details of the responsible economic operator (manufacturer, importer, authorised representative). This information must be visible on online interfaces before the consumer buys the product. In case of recall, product registration and loyalty systems must be used to reach consumers. When direct notification to affected consumers is impossible, the providers of online marketplaces (as well as the economic operators) must disseminate a clear and visible recall notice or safety warning through appropriate communication channels. Article 35 GPSR complements Article 32 DSA, on the right of information of consumers who purchased an illegal product or service, but, unlike Article 32 DSA, without establishing a specific timeframe.

# Regulation (EU) 2023/1115 ([129]) – [Deforestation and Forest Degradation Regulation]

*General Information*

The Regulation was adopted in 2023, and will become applicable on 30 December 2025 following an amendment of the entry into application by Regulation (EU) 2024/3234[130]. An additional legislative proposal was tabled by the Commission on 21 October 2025, aiming to amend certain obligations of operators and traders[131].

Based on Article 192(1) TFEU, Regulation (EU) 2023/1115 (EUDR) sets out the legal framework aiming to combat global deforestation and forest degradation. As a measure of environmental protection, its purpose is to minimise the European Union's contribution to deforestation and forest degradation worldwide, and to reduce the Union's contribution to greenhouse gas emissions and global biodiversity loss.

*Personal scope*

The EUDR applies to operators and traders involved in the supply chain of specific commodities and products outlined in Annex I of EUDR. Article 2 EUDR provides the following definitions related to the personal scope:

- 'Operators' are natural or legal persons who, commercially, place relevant products on the Union market or export them. Their main obligation is to exercise due diligence to ensure products are deforestation-free and comply with the country of production's relevant laws. Non-SME operators must also report annually on their due diligence system, while SME operators have simplified obligations if due diligence has already been performed by a previous operator
- `Traders` are persons in the supply chain, other than operators, who commercially make relevant products available on the market without further manufacturing
- Non-SME traders have the same obligations as non-SME operators. SME traders must collect and keep information about their suppliers and those they supply products to, providing it to competent authorities upon request
- Regarding online platforms, the Recital 30 EUDR explicitly states that the obligations for operators and traders apply regardless of whether products are made available on the market through traditional or online means.

*Territorial scope*

The EUDR's territorial scope covers the placing and making available on the Union market and the export from the Union of relevant products. It applies to commodities and products produced within the Union as well as those imported to the Union (Article 1(1)).

*Material scope*

The EUDR prohibits the placement, making available or export of certain commodities and products (including cattle, cocoa, coffee, oil palm, rubber, soya, and wood) within or from the EU unless they are 'deforestation-

[129] Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation and repealing Regulation (EU) No 995/2010, OJ 2023 L 150, 206–247.
[130] Regulation (EU) 2024/3234 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2023/1115 as regards provisions relating to the date of application.
[131] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2023/1115 as regards certain obligations of operators and traders, COM(2025) 652 final.

free', produced legally and covered by a due diligence statement. It establishes a mandatory due diligence system for operators, requiring them to collect information, assess risks, and implement mitigation measures, with simplified requirements for products produced in countries classified as low-risk.

*Enforcement*

The Regulation is enforced by Member States through their designated competent authorities in cooperation with customs authorities. Competent Authorities are, among others, mandated to carry out checks on operators and traders, and apply corrective actions and penalties for non-compliance (See Articles 16 and 24 EUDR).

*Interactions with the DSA*

The EUDR does not contain any references to the DSA or the E-commerce Directive (2000/31/EC). The DSA does not contain any references to the EUDR.

On **personal scope**, as long as providers of online marketplaces only facilitate distance contracts to be concluded between two other parties and do not intervene in the actual supplu of the product to the client, they are considered as intermediary service providers with no obligation under the EUDR. Where such providers play other functions such as supplying products themselves or offering services aimed at delivering products, the decision as to whether they are considered as operators or traders under the EUDR or intermediary service providers under the DSA must be made on a case-by-case basis, taking into account their concrete functions in the supply of the individual sale in question.

Regarding **material scope**, the EUDR and the DSA have a different material scope. Only where online marketplaces would qualify as operators or traders, the EUDR would apply in respect of the specific services it provides that extend beyond acting solely as an intermediary. Consequently, there is no overlap on **enforcement**.

In sum, there are no overlaps or contradictions between the EUDR and the DSA.

# Regulation (EU) 2023/1542 ([132]) – [Batteries Regulation]

*General Information*

The Batteries Regulation (BR) was adopted on 2 July 2023. It became applicable on 18 February 2024 with the first review planned by 30 June 2031. It repealed Directive 2006/66/EC.

The BR is based on both Article 114 TFEU and Article 192(1) TFEU. It is thus a measure aimed both at ensuring the efficient functioning of the internal market and at protecting the environment. More specifically, the Regulation seeks to ensure the sustainability, safety, and circularity of batteries throughout their entire life cycle within the EU. It aims to reduce the environmental and social impacts of batteries by setting requirements on design, performance, due diligence, carbon footprint, labelling, and waste management. The Regulation supports the EU's transition to a low-carbon economy and the development of a competitive and responsible battery value chain.

*Personal scope*

The Regulation applies to various economic operators involved in the battery supply chain, including manufacturers, authorised representatives, importers, distributors, and fulfilment service providers. This encompasses any natural or legal person who is subject to obligations related to the manufacture, preparation for re-use, preparation for repurposing, repurposing, or remanufacturing of batteries, or making them available or placing them on the market (including online) or putting them into service. The Regulation also applies to providers of online platforms that allow consumers to conclude distance contracts with producers (i.e. manufacturers, importers and distributors) offering batteries (including those incorporated in appliances, light means of transport, or other vehicles), directly referencing the same term used in Section 4 of Chapter III DSA.

*Territorial scope*

The BR applies to batteries placed or made available on the EU internal market (Article 1(1) BR), irrespective of where the economic operator is established.

*Material scope*

The BR requires that all batteries placed on the EU market meet strict standards for sustainability, safety, and circularity. This includes requirements for carbon footprint disclosure, minimum recycled content, performance and durability, removability and replaceability, and proper labelling, including a QR code linked to a digital battery passport. It also introduces obligations for due diligence on raw material sourcing and sets targets for collection, recycling efficiency, and recovery of critical materials.

These rules apply across the battery life cycle—from production to end-of-life. With regard to providers of online platforms that allow consumers to conclude distance contracts with producers, the Article 62(6) BR establishes that for the purposes of compliance with Article 30(1)(d) and (e) DSA, providers shall obtain certain information from producers, namely the register of producers referred to in Article 55 and the producers' registration number and a self-certification committing compliance with the extended producer responsibility requirements laid down in the Regulation. The BR is therefore aligned and specifies Article 30(1), points (d) and (e) DSA, to the extent that it can be interpreted as applying only to producers who sell directly through those platforms. Furthermore, information on the prevention and management of waste batteries should be made available as a minimum, at the point of sale in a visible manner and through online platforms (Article 74 BR). Distributors selling products through online platforms also have obligations to provide certain information.

---

[132] Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC, OJ 2023 L 191, 1–117.

*Enforcement*

The enforcement of the BR lays in the competence of national market surveillance authorities. While the BR sets out certain enforcement measures, it also relies on the mechanisms of the Market Surveillance Regulation. The BR requires the providers of online platforms to cooperate with national market surveillance authorities.

*Interactions with the DSA*

The Regulation refers to the DSA in the definition of an "online platform" (Article 3(1)(67) BR) and the provision on traceability (Article 62(6) BR). The DSA does not make any references to the BR.

On **personal scope**, the BR covers providers of online platforms that allow consumers to conclude distance contracts with producers of batteries as per Article 62 (6) BR. As online platforms are intermediary services under Article 3 DSA, there is an interplay between the DSA and the BR.ç

Regarding **territorial scope**, the DSA applies to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services are established. The BR applies to batteries placed or made available on the EU internal market.

Referring to the **material scope**, all producers offering batteries via distance contracts to consumers shall be considered traders under the DSA (Recital 132). Prior to the use of their services, providers of online platforms therefore must obtain from traders who are producers the information set out in Article 30(1) DSA.

As mentioned, Article 62(6) BR further specifies the information which providers of online platforms must obtain from battery producers, including details from the register of producers and a self-certification of compliance with extended producer responsibility requirements. It is worth to note that, being the BR a sector-specific piece of legislation with general and direct effect, no additional national requirements are allowed, unless otherwise expressly provided.

Finally, on **enforcement**, the implementation of the rules on the traceability of traders for the sale of batteries online are subject to the enforcement rules laid down in the DSA as per Recital 104 of the BR.

*Special remarks on interplay*

The instruments interplay, as they both apply to online marketplaces for the purposes of identifying the seller of products, but apply in a complementary manner. Article 62(6) BR complements Article 30(1)(d) and (e) by specifying the information a provider of an online platform must obtain from producers offering batteries for the purpose of compliance with the DSA.

However, it is important to note that Article 62(6) can only apply where the producer sells directly through the online platform – if a distributor mediated such sale, the online marketplace would only be obliged to receive the information –and make best efforts to check it- from the distributor, but not from the producer, who would not be in that case a "business customer" of the platform, but of the distributor.

## Regulation (EU) 2023/1543 ([133]) - [e-evidence Regulation]

*General information*

The e-evidence Regulation was adopted on 12 July 2023 and is applicable from 18 August 2026. The Commission will carry out an evaluation of this Regulation by 18 August 2029.

The purpose of the e-evidence Regulation is to facilitate and improve access to electronic evidence in criminal judicial proceedings within the EU in cross border situations. The Regulation creates the legal basis for two types of orders: the European Production Order for the production of electronic evidence stored by or on behalf of a service provider, and the European Preservation Order for the preservation of electronic evidence for the purposes of a subsequent request for production.

*Personal scope*

Article 3(3) provides a detailed definition of the type of service providers falling within its scope namely: (a) electronic communications services, (b) internet domain name and IP numbering services or (c) other information society services enabling their users to communicate with each other or otherwise store or process data on their behalf, provided that the storage of data is a defining component of the service. Financial services as defined in Article 2(2)(b) Directive 2006/123/EC are explicitly excluded from the scope.

The e-evidence Regulation applies to service providers which offer the above-mentioned services in the Union (Article 2(1) e-evidence Regulation)[134]. As per Article 3(4), "offering services in the Union" is defined as (a) enabling natural or legal persons in a Member State to use the services listed in the Regulation and (b) having a substantial connection based on specific factual criteria to a Member State. Such substantial connection requires either an establishment in a Member State or in the absence of such may be based on the fact that there is a significant number of users in one or more Member States, or that there is targeting of activities towards one or more Member States'.

*Material scope*

The e-evidence Regulation provides rules on the issuance and enforcement of European Production Orders and European Preservation Orders as well as the transmission and execution of European Production Order Certificates (EPOC) and European Preservation Order Certificates (EPOC-PR) for the purposes of criminal proceedings.

*Enforcement*

Chapter III of the e- e-evidence Regulation provides rules on the enforcement of European Production Orders and European Preservation Orders. Article 15 requires Member States to lay down rules for penalties applicable to the infringements of Articles 10 (execution of an EPOC) and 11 (execution of an EPOC-PR) and Article 13(4) (confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or

[133] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings; OJ L 191, 28.7.2023, p. 118–180.

[134] Article 1(1) of the e-evidence Regulation also states that "This Regulation lays down the rules under which an authority of a Member State, in criminal proceedings, may issue a European Production Order or a European Preservation Order and thereby order a service provider offering services in the Union and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or to preserve electronic evidence regardless of the location of the data." However, we don't understand this as a narrowing of the scope, but rather an intentional reference to the e-evidence Directive (EU) 2023/1544, which requires an establishment and legal representative in the EU.

preserved), and to take all measures necessary to ensure these are implemented. Article 16 provides for the procedure for enforcement in cases the addressee does not comply with an EPOC or EPOC-PR. In cases of non-compliance, the enforcing authority can impose penalties, which can be up to 2 % of the total worldwide annual turnover of the service provider's preceding financial year. The enforcing state is defined as the Member State in which the designated establishment of the service provider or its legal representative is established. (Article 3(16)).

*Interactions with the DSA*

There are no references to the DSA in the e- e-evidence Regulation. The DSA does refer to the e-evidence Regulation in Recitals 10 and 34 as well as Article 2(4)(i), noting the DSA shall be without prejudice to the provisions set out in the e- e-evidence Regulation,, regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA.

Regarding **personal scope**, both the DSA and the e- e-evidence Regulation apply to the following types of services:

- Mere conduit services which are electronic communications services (see Art 3(3)(a) e-evidence Regulation and Article 3(g)(i) DSA, such as internet access services, email services, messenger services and VoIP services[135];
- Domain name system (DNS) services and top-level domain name registries (see Art 3(3)(b) e-evidence Regulation and recital 28 of the DSA;
- Intermediary services (other than electronic communication services) that enable their users to communicate with each other (see also Recital 27 and Article 3(3)(c)(i) e-evidence Regulation and Article 3 (g) DSA);
- Hosting Service Providers (see Art 3(3)(c)(ii) and Recital 27 e-evidence Regulation and Art. 3(g)(iii) DSA).

It follows that most providers of online intermediary services under the DSA are covered by the E-evidence Regulation as well.

On **territorial scope**, both the DSA and the e-evidence Regulation apply to service providers offering services in the EU, which they both define in a similar way in Article 3(d) and (e) DSA and Article 3(4) e-evidence Regulation (i.e. enabling users in the EU to use its services and having a substantial connection to the Union, which can be demonstrated by either an establishment in a Member State, a significant number of users in one or more Member States, or where the service is targeted towards one or more Member States).

With regards to **material scope,** the DSA and the e-evidence Regulation interplay, in that they both regulate orders to provide certain information (Article 10 DSA and Articles related to the European Production Order), however in different ways. Article 2(4)(i) DSA states that the DSA is without prejudice to Union law regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA in the field of judicial cooperation in civil or criminal matters, including the e-evidence Regulation. and Recital 31 of the DSA specifies that the DSA does not provide the legal basis for the issuing of orders to provide certain specific information, the e-evidence Regulation provides such legal basis.

The following elements need further attention:

- **Type of order:** The e-evidence Regulation covers orders to produce or to preserve electronic evidence (regardless of the location of the requested data), in the specific context of criminal proceedings. Article

[135] The e-evidence Regulation refers to "electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972". However, it remains unsure whether broadcasting transmission services and machine-to-machine services (also listed in the definition of Article 2(4)(c) of the Directive (EU) 2018/1972, would also fall under the DSA.

3(8) e-evidence Regulation defines "electronic evidence" as subscriber data, traffic data or content data in electronic form, stored by or on behalf of a service provider at the time of the receipt of an EPOC or EPOC-PR. This could thus include data on the recipient of a service including from traders selling products or services on online platforms. The DSA on the other hand generally covers "orders to provide information" in Article 10. While the DSA does not provide a definition of the term "order" in Article 3, Article 10(1) refers to orders "to provide specific information about one or more specific individual recipients of the service". Moreover, Article 10(2)(a)(iv) of the DSA states that the requested information must be necessary "to determine compliance by the recipients of the intermediary services with applicable Union law or national law." Therefore, European Production Orders issued under the e-evidence Regulation could qualify as orders under Article 10 DSA, if those European Production Orders concern subscriber data, traffic data or content data in electronic form, stored by or on behalf of a service provider at the time of the receipt of such an order, and if all the conditions set out in Article 10(2)(a) of the DSA are fulfilled. However, Article 10 DSA should only apply to orders not falling under the scope of the e-evidence regulation as complementary orders.

- **Issuing authority:** As per Article 4(1) e-evidence Regulation, a European Production Order for subscriber data and data requested for the sole purpose of identifying the user may only be issued by a judge, court, or a public prosecutor competent in the case concerned as well as any other competent authority as defined by the issuing State. Pursuant Article 4(2), a European Production Order to obtain traffic data and content data needs to be issued or validated by a court or judge. Article 10(1) DSA on the other hand, given its horizontal nature, does not define the competent issuing authority but rather states that such orders are *"issued by the relevant national judicial or administrative authorities on the basis of the applicable Union law or national law in compliance with Union law",* covering therefore all authorities competent to issue EPOCs under the e-evidence Regulation.

  An EPOC under the e-evidence Regulation could therefore qualify as an order to provide information under article 10 DSA, insofar the EPOC requests information about an individual service user, for the purpose of their identification and to determine their compliance with applicable laws. However, Article 10 DSA should only apply to orders not falling under the scope of the e-evidence regulation as complementary orders.

- **Obligations for service providers**: The DSA does not create a legal basis to issue orders and no corresponding obligation for service providers to disclose, store or preserve data for the purpose of criminal investigations or prosecutions. However, there are a number of obligations which are similar (i.e. where the material scope overlaps). Article 10(1) DSA regulates how intermediary services should inform the authority issuing the order of its receipt and effect given to it. On the other hand, the e-evidence Regulation sets out in Article 10 (5-8) specific and detailed obligations of the service provider to inform the issuing authority if the service provider cannot comply with the EPOC under different circumstances.

  Article 10(2) DSA sets out **minimum conditions** for orders to provide information to give rise to the information obligation (Recital 31). Article 5 (5) of the e-evidence Regulation also specifies the information that must be included in an EPOC.

  Furthermore, Article 10(3) and (4) DSA specify **how the order should be transmitted** from the issuing authority to the DSC of that same Member State, and from this DSC to all DSCs in the Member States. On the other hand, Article 19 of the e-evidence Regulation covers the method of transmission of the order to the addressee and the enforcing authority, which should take place through the decentralised IT system. Finally, both instruments include **obligations to inform the recipient of the service whose data are being requested in the order** (Article 10(5) DSA and Article 13(1) e-evidence Regulation), but the e-evidence Regulation prohibits the information of the user by anyone other than the issuing authority and in the case of overlaps between the two instruments, pursuant to Article 2(4)(i) and 10(6) DSA, only the requirements of the e-evidence Regulation apply.

Finally, on **enforcement** and similar to the e-evidence Regulation, the DSA appoints the Member State of the establishment of the provider of intermediary services with the powers to supervise and enforce the DSA (Article

56(1) DSA), but also provides enforcement powers to the European Commission, with regards to VLOPs and VLOSEs. However, the enforcement actions foreseen under each instrument do not cover the same obligations (and therefore do not overlap): the DSA includes provisions on the enforcement of the obligation to inform the relevant authorities about the receipt and effect given to those orders (Article 51 DSA, Recital 31 and 32) whereas the e-evidence Regulation includes provisions which relate to the enforcement of the orders themselves (Article 15 and 16 e-evidence Regulation).

*Special remarks on interplay*

Some particular elements need to be highlighted:

- **Orders to provide information & their enforcement** (Article 10 DSA):
  - Information to be included in the order (Article 10(2) DSA vs Article 5 (5) e-evidence Regulation): The information requirements for the orders under the DSA and e-evidence Regulation are slightly different.

  - Obligation to inform recipient of service (Article 10(5) DSA vs 13(1) e-evidence Regulation): While the DSA requires the provider of the intermediary services to inform the user whose data is requested about the order (with certain caveats pursuant Art.10(6)), Article 13 e-evidence Regulation requires the service provider to ensure confidentiality and secrecy of the EPOC and EPOC-PR and puts the obligation to notify the user on the issuing authority. This is to take into account the specific confidentiality needs of criminal investigations. The EPOC template as well notes that "the addressee shall in any event refrain from informing the person whose data are being requested. It is the responsibility of the issuing authority to inform that person, without undue delay, about the data production".[136] Moreover, as regards the content of the user notification, the DSA requires the user to be informed of the order received and the effect given to it, as well as a statement of reasons and the possibilities for redress that exist, while the e-evidence Regulation requires informing the person "about the production of data on the basis of an EPOC", as well as available remedies (Article 13(1) and (3) Regulation). In terms of timing, the DSA specifies this should be done "when effect is given to the order, or, where applicable, at the time provided by the issuing authority in its order", while the e-evidence Regulation requires this to be done "without undue delay". Article 13(2) e-evidence Regulation also provides for specific exemptions to this obligation, as does Article 10(6) DSA[137].

  - Obligation to provide information on the receipt and effect given (Article 10(1) DSA and Article 10 e-evidence Regulation): Article 10(1) DSA requires that the provider of the intermediary service receiving an order for information, informs the issuing authority about the receipt and of the effect given to the order "without undue delay". In case an order sent under the e-evidence Regulation would qualify as an order under Article 10 DSA, the DSA could "top up" the obligations to provide information, under the e-evidence Regulation), under which the information itself should be provided. The e-evidence Regulation includes the obligation to transmit the requested data to the issuing authority within 10 days (Art 10(1-3), or to inform "without undue delay" the issuing authorities of its reasons why it cannot provide the requested data within this timeline (Article 10(5-8) e-evidence Regulation). Moreover, the issuing authority will also receive notifications through the decentralised IT system, which will be used to transmit EPOCs to service providers. Since the e-evidence Regulation provides for a comprehensive regulation in this regard, it has to be considered *lex specialis*, without leaving space for the application of Article 10(1) DSA.

[136] See section H, Annex I of the e-evidence Regulation.

[137] Recital 34 DSA states that "the obligation on the providers of intermediary services to inform the recipient of the service might be delayed in accordance with applicable Union or national law, in particular in the context of criminal, civil or administrative proceedings".

- **On the applicable norm regarding the obligation to inform the recipient of the service,** the DSA contains a few references stating that the DSA is without prejudice to Union law regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA in the field of judicial cooperation in civil or criminal matters, including the e-evidence Regulation, as well as criminal procedural law (e.g. Recital 10, 34, Article 2(4)(i) and Article 10(6) DSA). Moreover recital 34 further notes that, where those laws in the context of criminal or civil proceedings provide for conditions that are additional to or incompatible with the conditions provided for in the DSA, the conditions provided for in the DSA might not apply or might be adapted.

  This is further confirmed by the carve-out in Article 10(6) DSA. The recital highlights two examples in particular in this regard: the obligation under Article 10(4) of the DSA for the Digital Services Coordinator from the Member State of the issuing authority to transmit a copy of the orders to all other Digital Services Coordinators, and the obligation in Article 10(5) DSA on the providers of intermediary services to inform the recipient of the service. The confidentiality requirement under Article 13(1) e-evidence Regulation therefore prevails as the *lex specialis* over the obligation to inform the recipient of the service under Article 10(5) DSA.

- **On the applicable norm regarding the enforcement provisions,** the preamble of the DSA, in recital 32, clarifies that the applicable EU law under which the orders are issued might require additional conditions and should be the basis for the enforcement of the respective orders. Recital 31 of the DSA further confirms that the DSA "does not […] regulate their cross-border enforcement" primarily serving to clarify the limitations of Article 10 DSA and emphasising that the DSA is without prejudice to the rules under the e-evidence Regulation related to the enforcement of the orders themselves (Article 15 and 16 e-evidence Regulation). This means the e-evidence Regulation should be the basis for the enforcement of the EPOC and EPOC-PRs, not the DSA.

  As noted above, Article 10(2) DSA does not in general stipulate requirements for orders to provide information, but harmonises information requirements which - if fulfilled - trigger the information obligation under Article 10(1) (see Recital 31). Article 5(5) e-evidence Regulation on the other hand sets out the requirements which a European Production Order must fulfil in order to give rise to the obligation of the provider to disclose information. Even though these formal requirements are complementary (e.g. the DSA adding redress mechanisms available), the e-evidence Regulation would take precedence in case of misalignment.

In sum, because of its specific scope and specific provisions reflecting the needs of criminal proceedings, the provisions of the e-evidence Regulation should be considered as *lex specialis* to Article 10 DSA, that applies without prejudice to national criminal law. A parallel application would undermine the efficiency of the e-evidence rules and could conflict with the needs of criminal proceedings.

## Directive (EU) 2023/1544([138]) - [e-evidence Directive]

*General Information*

The e-evidence Directive (EED) was adopted in 2023 and is applicable from 18 February 2026. As per Article 8 EED, the Commission will carry out an evaluation of the Directive by 18 August 2029.

The EED aims to ensure that for decisions and orders for the purpose of gathering electronic evidence on the basis of several Union instruments, in particular the e-evidence Regulation[139] there is an addressee of the newly created instruments of European Production or Preservation Orders, against whom such orders can be enforced. Together with the e-evidence Regulation, the EED should facilitate the cross-border obtaining of electronic evidence in criminal proceedings.

*Personal scope*

The EED applies to service providers that provide the following categories of services per Article 2(1) EED: (a) electronic communications services, (b) internet domain name and IP numbering services, or (c) other information society services enabling their users to communicate with each other or that make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user. It explicitly excludes providers of financial services[140].

*Territorial scope*

As per Article 1(5) EED, the EED applies to service providers that offer the above-mentioned services in the Union. As per Article 2(2) EED, offering services in the EU is defined as (a) enabling natural or legal persons in a Member State to use the services listed in the EED or (b) having a substantial connection based on specific factual criteria to a Member State where the service can be used.

Such a substantial connection may be based on the fact that 'there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States'. The Directive does not apply to service providers established on the territory of a single Member State that offer services exclusively on the territory of that Member State (recital 8 and Article 1(5) EED).

*Material scope*

The EED lays down the rules on the designation of designated establishments and the appointment of legal representatives of certain service providers that offer services in the Union, for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States, for the purposes of gathering electronic evidence in criminal proceedings.

---

[138] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings; OJ L 191, 28.7.2023, p. 181–190.

[139] The EED applies to to decisions and orders for the purpose of gathering electronic evidence on the basis of Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings; Directive 2014/41/EU and of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between Member States of the Union. The EED equally applies to decisions and orders for the purpose of gathering electronic evidence on the basis of national law addressed by a Member State to a natural or legal person acting as legal representative or designated establishment of a service provider on the territory of that Member State.

[140] As referred to in (Art 2(2)(b) Directive 2006/123/EC, on services in the internal market.

*Enforcement*

As per Article 6 EED, it is the Member States' central authority(ies) that need to ensure the EED is applied in a consistent and proportionate manner, In addition, Article 5 EED requires Member States to lay down rules on penalties and to take all measures necessary to ensure that they are implemented. The EED does not provide further substantive rules on enforcement. In particular, it does not assign the responsibility to enforce to one Member State, but to several (i.e. the Member States where the provider has a legal representative or is established, and/or where the services are provided, depending on the case). Article 6(3) EED requires Member States to ensure that their central authorities coordinate and cooperate with each other, which it notes "should cover, in particular, enforcement actions". Recital (21) EED foresees additional coordination mechanisms to be set up in this regard and anticipates the involvement of the Commission where relevant for the coordination of enforcement action.

*Interactions with the DSA*

The EED does not contain any references to the DSA. The DSA does refer to the EED in several provisions:

- Recital 10 DSA: "This Regulation should be without prejudice to [...] provisions of Union law set out in [...] a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings".
- Recital 34 DSA: "However, this Regulation should be without prejudice to Union law in the field of judicial cooperation in civil or criminal matters."
- Art 2(4) DSA: "This Regulation 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 this Regulation, in particular, the following: (...) (j) a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings."

With regards to the **personal scope**, both the DSA and the EED apply to the following types of service providers or intermediary services, namely:

- Mere conduit services which are electronic communications services (see Art 2(1)(a) EED and Article 3(g)(i) DSA, such as internet access services, E-Mail services, messenger services and VoIP services.
- Domain name system (DNS) services and top-level domain name registries (see Art 2(1)(b) EED and recital 28 of the DSA.
- Intermediary services (other than electronic communication services) that enable their users to communicate with each other (see also (Article 2(1)(c)(i) EED and Article 3 (g) DSA;
- Hosting Service Providers (see Recital 14 and Art 2(1)(c)(ii) EED and Art. 3(g)(iii) DSA).

On **territorial scope**, the DSA and the EDD apply to service providers offering services in the EU, which they both define in a similar way in Article 3(d) DSA and Article 2(3) EED (i.e. enabling users in the EU to use its services and a substantial connection to the EU/a Member State).

With respect to **material scope**, although the EED and the DSA generally have different objectives (see above), they do interact in one particular area, namely that both the DSA and the EED require service providers without establishment in the Union to designate a legal or natural person to act as their legal representative where they offer their services for their respective areas of application - for the purpose of receiving and complying with orders issued by competent authorities of the Member States, for the purposes of gathering electronic evidence in criminal proceedings, and for the enforcement of the due diligence obligations under the DSA, respectively.

Regarding the **enforcement**, in the event the provider does not appoint a legal representative (as required under Article 13 DSA) and lacking a legal establishment in one of the Member States, according to Article 56 DSA all Member States or the Commission (in case of a VLOP) would be empowered to supervise and enforce. The

EED provides that all Member States on whose territory the service provider offers services are responsible for enforcement, if a service provider without an establishment in the EU fails to appoint a legal representative.

*Special remarks on overlaps*

Some elements need to be highlighted with regards the identified overlaps:

(1) **Appointment legal representative (Article 13 DSA):** The DSA replicates the obligation to appoint a legal representative under the e-evidence Directive, where both apply for the purpose of their respective enforcement in their personal and material scope. The legal representative designated under Article 13 DSA would be liable for the enforcement of the service provider's respective obligation under Article 10(1) DSA with respect to orders, where applicable, which adds an obligation to provide "feedback" on the follow-up given to the received orders. However, Article 10 DSA should only apply to orders not falling under the scope of the e-evidence regulation as complementary orders. Both legal instruments have obligations to ensure that service providers provide their legal representatives with the necessary powers and resources (Article 13(2) DSA vs Article 3(4) EED). The legal representatives under each framework (DSA and EED) have distinct but somewhat overlapping roles concerning receipt of decisions/orders.

- **Legal representative**: The legal representative under the DSA serves the "receipt of, compliance with and enforcement of decisions issued in relation to the DSA" (Article 13(2)) whereas the legal representative under the EED serves "the receipt of, compliance with and enforcement of decisions and orders […] for the purposes of gathering electronic evidence in criminal proceedings " including under the e-evidence Regulation (Article 1(1) and (2) EED). The provisions contained in Articles 10(5) to 10(8) of the e-evidence Regulation prevail as *lex specialis* over Article 10(1) DSA. The interplay of this obligation with similar obligations under the e-evidence Regulation is further addressed in the report on the e-evidence Regulation.

- **Sending orders**: Orders under Article 10 DSA must be sent to the electronic point of contact designated by that provider, in accordance with Article 11 DSA (Art. 10(2)(c) DSA)) whereas EPOCs under the e-evidence Regulation must be sent to the designated establishment or legal representative established under the EED through the de-centralised IT-system.

  On the other hand, both the EED and DSA require notification of information on the legal representatives (Article 13(4) DSA and Article 4(1) EED). However, the DSA is more specific in the types of information to be notified (name, postal address, email address and telephone number), while the EED uses more general language which leaves room for interpretation. Also the EED and the DSA both require the notified information to be made public and to be updated. The DSA goes further in that it requires it to be accurate and easily accessible, while the EED only states that "information may be further disseminated to facilitate access by competent authorities."

In sum, the EED should be considered *lex specialis* in relation to the DSA due to its focus on criminal proceedings. Moreover, in various places, the DSA specifies that the DSA should be applied without prejudice to Union law in the field of judicial cooperation in civil or criminal matters, to national civil and criminal procedural law and without prejudice to the e-evidence Regulation and EED (recital 10, recital 34 and Article 2(4)(i) and (j); Art. 10(2)(iv) and Art. 10(6) DSA).

# Regulation (EU) 2024/900 ([141]) – [Regulation on the transparency and targeting of political advertising]

*General Information*

Regulation (EU) 2024/900 on the transparency and targeting of political advertising (TTPA) was adopted by the Council and the Parliament on 13 March 2024 and published in the Official Journal of the European Union on 20 March 2024. It entered into force on 9 April 2024 and fully entered into application from 10 October 2025, with the exception of Article 3 and Article 5(1) which were already applicable since 9 April 2024 (Article 30).

On 8 October 2025, the Commission adopted comprehensive guidelines to support the implementation of the Regulation[142] in the context of its full entry into application. These Guidelines represent the Commission's official interpretation of the Regulation (in particular of its Chapter I and II) with a view to ensuring its consistent, effective and uniform application. The European Data Protection Board will issue guidelines regarding the use of targeting and ad-delivery techniques under Chapter 3 of the Regulation, as referred to in Article 22(2) thereof.

The TTPA introduces transparency and accountability requirements covering both online and offline activities. It has a double legal basis, i.e. internal market and data protection. The Regulation is indeed part of the EU's broader internal market agenda, providing for common standards for transparency and related due diligence obligations linked to political advertising, to increase legal certainty and reduces the fragmentation of the obligations that service providers meet in the context of political advertising, therefore easing compliance efforts and reducing costs.

As provided in Article 2(1), the Regulation applies where "the political advertisement is disseminated in the Union, is brought into the public domain in one or several Member States or is directed to Union citizens, irrespective of the place of establishment of the provider of political advertising services or of the place of residence or establishment of the sponsor, and irrespective of the means used."

The common EU standards laid down in the Regulation reinforce fundamental rights including electoral integrity, free voting rights and data protection, addressing opaque influence in electoral, legislative and regulatory process, both online and offline, and empower citizens to make informed choices, in support of their democratic rights. It also contributes to the prevention of illegal behaviour including corruption.

As reiterated among others in Recital 5 and 49, fundamental rights, including freedom of expression and information, the right to hold political opinions, to receive and impart political information and share political ideas are protected in line with the Charter of fundamental rights in line with its article 2(3), the TTPA is without prejudice to the rules laid down in the DSA.[143] As such, the TTPA complements existing legislation, particularly the GDPR and the DSA.

*Personal scope*

[141] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L, 2024/900, 20.3.2024.
[142] Communication from the Commission – Guidance to support the implementation of Regulation (EU) 2024/900 on the transparency and targeting of political advertising, C(2025) 6829 final, of 6.10.2025.

The Regulation provides for EU common standards which applies to both online and offline political advertising. The scope of the Regulation goes beyond the scope of activities relevant to political advertising covered by the DSA, whose content is not affected by the Regulation.

Specific obligations under the Regulation on political ads apply to "sponsor[s]" as defined in Article 3(10), namely "the natural or legal person at whose request or on whose behalf a political advertisement is prepared, placed, promoted, published, delivered or disseminated."

Different concepts are relevant for the application of Chapter 2 of the Regulation (transparency and due diligence obligations for political advertising services). The concept of "provider[s] of political advertising services" is defined in Article 3(6), as "natural or legal person[s] engaging in the provision of political advertising services, with the exception of purely ancillary services." The term "political advertising service" is defined in Article 3(5) as "a service consisting of political advertising with the exception of an online 'intermediary service', as defined in Article 3, point (g), of Regulation (EU) 2022/2065, that is provided without consideration, for the preparation, placement, promotion, publication, delivery or dissemination for the specific message." The concept of "political advertising publisher(s)," which are a sub-category of political advertising services providers, defined in Article 3(13) covers "provider(s) of political advertising service that publish(es), deliver(s) or disseminate(s) political advertising through any medium."

According to Article 3, point (g), intermediary services in the meaning of the DSA also constitute political advertising services where they are provided without consideration for the preparation, placement, promotion, publication, delivery or dissemination for specific messages. Within this limited scope vis-à-vis intermediary services, it introduces complementary obligations to the ones provided in the DSA, including to VLOPs and VLOSEs defined by reference to the DSA.

Article 3(8) defines VLOPs by cross reference to the DSA, as "an online platform designated as a very large online platform pursuant to Article 33(4) of Regulation (EU) 2022/2065." Article 3(9) defines a VLOSEs also by cross reference to the DSA as "an online search engine designated as a very large online search engine pursuant to Article 33(4) of Regulation (EU) 2022/2065."

Where the provision of political advertising involves targeting or ad-delivery techniques that rely on the processing of personal data, in line the GDPR and its data protection legal basis, the Regulation on political ads applies to "controllers" as defined in Article 3(14): "a 'controller' as defined in Article 4, point 7, of Regulation (EU) 2016/679 or, where applicable, as defined in Article 3, point 8, of Regulation (EU) 2018/1725."

*Material scope*

The material scope of the Regulation has to be understood for the purpose of the application of the specific requirements of its chapter 2 (internal market) relevant in particular to the provision of services, offline and online, and 3 (data protection) relevant to targeting and ad delivery of political advertising involving the processing of personal data.

The concept of "political advertising,", (see Article 3(2)) covers "the preparation, placement, promotion, publication, delivery or dissemination, by any means, of a message, normally provided for remuneration or through in-house activities or as part of a political advertising campaign," where the message is either "by, for or on behalf of a political actor, unless of a purely private or purely commercial nature", or "liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level." As stated in Article 1(2), the Regulation does not apply to political opinions and editorial content that are subject to editorial responsibility unless "specific payment or other remuneration is provided for, or in connection with, their preparation, placement, promotion, publication, delivery or dissemination by third parties", as such content does not constitute political advertising. Article 1(3) further provides that "political opinions expressed in a personal capacity shall not be considered political advertising".

In addition, the Regulation provides for several explicit exclusions from the definition of political advertising. Article 3(2)(b), points (i)–(iii), expressly exclude:

> (i) messages from official sources of Member States or of the Union strictly limited to the organisation and modalities of participation in elections or referendums,
>
> (ii) public communications by or on behalf of public authorities not designed to influence political outcomes, and
>
> (iii) presentation of candidates in publicly allocated spaces or media provided by law, free of charge, and on equal terms.

The Regulation provides for specific rules focusing on transparency and accountability (see below). In the three months preceding an election or referendum, its Article 5(2) provides that political advertising services pertaining to that election or referendum "shall only be provided to a sponsor, or service provider acting on behalf of a sponsor, who declares itself to be: (a) a citizen of the Union; or (b) a third-country national permanently residing in the Union and having a right to vote in that election or referendum in accordance with the national law of the Member State of residence; or (c) a legal person established in the Union which is not ultimately owned or controlled by a third-country national, with the exception of third-country nationals referred to in point (b), or by a legal person established in a third country."

*Enforcement*

The supervision framework of the TTPA laid down in Article 22 involves data protection authorities, in charge of the oversight and enforcement of the data protection-related provisions. For obligations related to targeting and ad-delivery techniques under Articles 18 and 19, the competent supervisory authorities are those designated under the General Data Protection Regulation (GDPR) and Regulation (EU) 2018/1725 for EU institutions22(1)). For other aspects, competent authorities are designated by Member States.

Article 21(1) requires providers of political advertising services established outside the Union but active within it to designate a legal representative in one of the Member States where services are offered. The legal representative is responsible for compliance with the Regulation and may be held liable for infringements (Article 21(2)). To facilitate compliance as well as the enforcement, the Regulation establishes specific obligations for both national competent authorities and the Commission. In particular, the national competent authorities must maintain public registers of designated legal representatives (Article 21(4)), and the Commission must maintain a Union-wide portal linked to them (Article 21(5)).

As regards the supervision of obligations applicable to intermediary services falling within the scope of the Regulation, Article 22(3) of the TTPA requires Member States to designate competent authorities to supervise compliance of providers of intermediary services with Articles 7-17 and 21 TTPA. These may include the authorities designated under the DSA, such as the Digital Services Coordinators (DSC). The DSC is in any case responsible for ensuring coordination at national level in relation to intermediary services under the TTPA. The TTPA refers to the relevant DSA provisions on the designation of DSCs (Article 49), their investigative and enforcement powers (Article 51, mutatis mutandis), and cross-border cooperation and mutual assistance (Articles 58(1-4) and 60(1)).

For the supervision of all other aspects of the TTPA not referred to in Article 22(1) and (3), including Articles 5, 6, and 20, Member States must designate one or more independent competent authorities (Article 22(4)), which may also be different from those designated under Article 22(1) and (3), including DSCs, but also be the same ones as the ones referred to in the AVSMD Directive.

According to Article 22(7), Member States shall ensure that there is effective and structured cooperation and coordination at national level among all relevant authorities referred to in paragraphs 1 to 4.

Additionally, the governance structure of the Regulation relies on a new dedicated Network of national contact points for cooperation at EU level among Member States and with the Commission on all aspects of the TTPA. The network serves as a platform for regular exchange of information, best practices and structural cooperation. It shall facilitate the preparation of guidelines to support sponsors and providers of political ads services to comply with the requirements of the Regulation on political ads.

In this context, Member States are required to designate one competent national authority as a national contact point (Article 22(9)).

DSCs may be designated by their Member States as national contact points taking into account national competences and the coverage of services being provided offline. In any case and as mentioned above, the DSCs shall be responsible for ensuring coordination at national level in respect of providers of intermediary services.

Cooperation with other structures is explicitly foreseen in the Regulation. The Network of national contact points will also work in close cooperation with the European Cooperation Network on Elections, the Media board and other relevant networks or bodies (Article 22(8) TTPA). The reference to other relevant networks or bodies makes clear that this list is not limitative and can cover other networks including those established under the DSA.

As a main rule, the enforcement of the TTPA lies with those authorities which have been designated by their Member States as competent authorities under that Regulation (Article 22(1), (3) and (4), except where it concerns compliance with Articles 18 and 19 by the EU institutions and compliance by VLOPs and VLOSEs with their specific obligations laid down in Article 13.

*Interactions with the DSA*

According to Article 2(3), point (i) of the TTPA, the latter is without prejudice to the rules laid down in the DSA. Recital 51 further confirms that as regards the provisions of intermediary services falling within the scope of application of both texts, the obligations under the TTPA are intended to add further granularity to the DSA framework, in particular as regards VLOPs, while remaining without prejudice to the obligations in the DSA. This concerns for instance information related to the funding of political advertisements.

Regarding **personal scope**, activities potentially covered by both the DSA and the TTPA are limited to intermediary services involved in the dissemination of political advertising.

Under the TTPA, specific obligations apply offline and online to a defined set of actors involved in political advertising activities, including sponsors, providers of political advertising services and political advertising publishers which are a subset of providers of political advertising services (Article 3).

While the TTPA excludes from the definition of "political advertising services" intermediary services provided without consideration for the specific message (Article 3(5)), online intermediary service providers may be covered by specific transparency and accountability obligations, when they actively publish, deliver or disseminate political advertising with consideration for the specific message.

Where an online intermediary service provider (as defined in Article 3(g) DSA) is involved in the dissemination, delivery or publication of political advertising, it may have to comply with the obligations laid down in both instruments.

The TTPA makes explicit reference to VLOPs and VLOSEs which are defined by reference to Articles 33(4) DSA in Article 3(8)-(9).

On **territorial scope**, in terms of services being provided within the Union by providers established outside the Union, the requirements are consistent. Whereas the DSA, according to Article 2(1) DSA, applies to online intermediary services offered to recipients in the Union, irrespective of where the provider is established, Article 2(1) of the TTPA sets out that the Regulation applies where political advertisements are disseminated in the

Union, are brought into the public domain in one or several Member States or are directed to Union citizens, irrespective of the place of establishment of the provider.

A third-country provider of an intermediary service which qualifies as a political advertising service and disseminates political advertisements in the Union may fall under the territorial reach of both instruments and have to comply to both in a complementary manner.

Regarding the **material scope**, the TTPA introduces obligations related to the dissemination of political ads that go beyond the scope of the DSA and covers other, including offline, services. Regarding the rules specifically applicable to the provisions of intermediary services, the rules under the Regulation on political ads complement, the horizontal obligations in the DSA.

On labelling and transparency requirements and notices, Articles 11 and 12 of the TTPA complement the DSA's obligation under Article 26(1) prescribing more detailed disclosures tailored to political advertising, including information on financial value, origin of remuneration or entity ultimately controlling of the sponsor.

Similarly, on targeting and ad-delivery, building on the GDPR, Article 18 of the TTPA aligns with the DSA's general data-protection related prohibitions under Articles 26(3) and 28(2) while introducing data protection-specific requirements linked to the targeting or ad delivery of political advertising such as specific consent prerequisite, requirements for data collection and exemptions for internal party communications.

Beyond these examples, the TTPA establishes obligations that are connected to those provided for in the DSA: Article 9 introduces a standalone record-keeping obligation; Article 13(2) requires VLOPs and VLOSEs to make political advertising data available both in the DSA repository (Article 39 DSA) and accessible through the European repository under the TTPA; Article 14 creates campaign-level reporting obligations; Article 17 establishes an additional access right, among others, for vetted researchers within the meaning of Article 40(8) DSA vis-à-vis providers of political advertising services to be provided with the information that they are required to have in their possession pursuant to Articles 9, 11 and 12 of the TTPA, including, where applicable, information under Article 19(1), point (c) on the main parameters of targeting or ad-delivery techniques where applicable; and Article 19 establishes additional transparency requirements concerning targeting and ad-delivery. Article 21 requires designation of a legal representative in the EU for providers established outside the Union, which may be the same one as the DSA representative while being subject to partially additional requirements, such as mandatory registration in the context of the provision of political ads services within the Union.

In sum, when it comes to obligations applicable to intermediary services, the TTPA largely complements the DSA's framework, introducing specific obligations for the political advertising context when the provision of intermediary services is at stake. This results in a model of coherence and complementarity: where intermediary services fall within the scope of the TTPA, DSA obligations continue to apply without prejudice, complemented by sector-specific requirements protecting core democratic processes such as electoral integrity as well as legislative and regulatory processes.

The **enforcement** framework of the TTPA is based on authorities to be designated by Member States, while also taking the DSA into consideration when it comes to intermediary services, and the GDPR when it comes to data protection related provisions.

For providers of intermediary services, Article 22(3) of the TTPA establishes that Member States shall designate competent authorities to supervise compliance with its Articles 7 to 17 and 21 and makes specific provisions of the DSA applicable *mutatis mutandis*. The Digital Services Coordinator (DSC) designated under Article 49 DSA is, even if it is not designated as competent authority, responsible for coordination at national level under the TTPA in respect of providers of intermediary services as well. Of note, unlike the DSA, where the European Commission exercises direct supervisory and enforcement powers over VLOPs and VLOSEs, the TTPA vests in principle all enforcement competence in Member State authorities, without any enforcement role at European level. However, the Commission should assess compliance of VLOPs/VLOSEs with their obligations concerning the European repository for online political advertisements (Recital 91).

Article 23 of the TTPA creates a cross-border enforcement framework substantively analogous to Articles 56-60 DSA, while its Articles 22(8)-(9) establish a separate network of national contact points distinct from the European Board for Digital Services under the DSA. At the same time, the TTPA explicitly provides in its article 22(8) that this network shall work in close cooperation with relevant networks and bodies. Finally, Article 25 of the TTPA creates an autonomous sanctions regime that broadly mirrors Article 52 DSA in structure while providing for specific responsibility for sponsors and requires consideration of freedom of the press and freedom of expression in other media and the rules or codes governing the journalist profession.

Concerning the applicable supervision mechanism whilst considering activities falling both under the TTPA and the DSA, the general principle is that both supervision regimes are in principle complementary. However, there are certain provisions under which the TTPA refers to DSA enforcement provisions by making them applicable within the enforcement framework of the TTPA. Additionally, there are cases in which obligations under the DSA should further align with the logic of the TTPA (see Article 13(2) and Recital 46).

Given the complementarity of the requirements under the TTPA and the DSA on substance related to intermediary services and on the governance, it is important that there is in practice a close cooperation at different levels as provided for in the TTPA. At national level, there is a need for close cooperation between the DSCs and other designated competent authorities in particular when the provision of intermediary services is at stake (see Article 22(7) of the TTPA).

Furthermore, there is a need of close cooperation between the designated competent authorities under the TTPA, including DSCs where relevant, and the Commission to ensure a consistent application of the TTPA concerning obligation related to the European repository for online political advertising as provided for in Article 22(8) of the TTPA. Additionally, the Network of national contact points is required in line with Article 22(8) of the Regulation to work, where relevant, with other networks such as the European Board for digital services (beyond the European Cooperation Network on Elections and the media board). Strengthening the cooperation as foreseen in the Regulation on political ads in its Article 22(8) shall facilitate the swift and secured exchange of information on issues connected to the supervision and enforcement.

*Special remarks on potential overlaps*

Certain specific provisions of the DSA and the TTPA potentially overlap, which merits further analysis in the following section.

- **Notice-and-action mechanism**: Both regulations require mechanisms for third parties to notify providers of potentially non-compliant (Article 15 of the TTPA) or illegal content (Article 16 DSA). Article 15 obliges political advertising publishers to establish notification channels for political advertisements suspected of breaching the TTPA's transparency or targeting rules. Article 16 DSA, by contrast, requires all hosting service providers to implement notice and action mechanisms covering any "illegal content" within the meaning of Article 3(h) DSA.

  Both regulations apply in parallel for providers of intermediary services that simultaneously qualify as political advertising publishers under the TTPA and as hosting service providers under the DSA. In such cases, both Article 15 and Article 16 require accessible notification mechanisms, confirmation of receipt, and diligent follow-up, with Article 15 of the TTPA establishing shorter deadlines for notifications submitted in the last month preceding elections.

  The applicable norms are coherent in respect of online platforms acting as both publishers and hosting providers. In such cases, platforms must organize their activities to ensure that their notification mechanisms satisfy the requirements of both instruments, although the substantive triggers differ.

  Recital 69 of the TTPA makes clear that political advertising publishers should be able to rely on existing mechanisms, with a particular reference to notice and action mechanism established under the DSA. This means that one notice and action mechanism under the DSA should satisfy the requirements of both Regulations (with possible targeted adaptations), without the need to establish a separate instrument.

Both instruments interact also providers of intermediary services do not qualify as political advertising publisher under the TTPA. In cases where providers of intermediary services do not qualify as political advertising publisher under the TTPA, they may still be notified pursuant to Article 16 of the DSA of alleged illegal political advertisements under the TTPA. Consequently, relevant providers would be required to process the notices, and decide upon them in a timely, diligent, non-arbitrary and objective manner, i.e. the provider will have to decide whether it agrees with the assessment of the person or entity notifying potentially illegal content. If in such a case the provider obtains actual knowledge or awareness of an illegal political advertisement, it should act expeditiously to remove or to disable access to that advertisement if it wishes to benefit from the liability exemption pursuant to Article 6 of the DSA. To give rise to actual knowledge or awareness pursuant to Article 6 DSA, the illegality of the content should be identifiable by a diligent online platform without a detailed legal examination (e.g., where the online platform is provided with a decision of a competent national authority finding the political advertisement, or identical content disseminated via other channels, as illegal).[144]

- **Statement of reasons**: Article 15(9) of the TTPA and Article 17 DSA both includes obligations applicable to service providers of intermediary services to inform relevant parties when measures are taken that affect the availability or visibility of certain information - in this case, political advertisements. While Article 15(9) requires political advertising publishers to inform sponsors or providers of political advertising services of any such measures taken in response to a notification under the TTPA, Article 17 DSA imposes an obligation on providers of hosting services to issue a detailed statement of reasons to affected recipients whenever content is restricted due to illegality or a breach of terms and conditions. Both provisions are applicable to an online platform when it acts as both a political advertising publisher under the TTPA and a hosting service under the DSA, particularly where a political advertisement is removed or restricted following a notification.

  In practice, this means that both provisions apply when non-compliance with the TTPA requirements also qualifies as "illegal content" within the meaning of Article 3(h) DSA. According to the TTPA, a mislabeled or incomplete political advertisement does not automatically lead to discontinuation of the political advertisement. Instead, under the TTPA, a stepwise approach applies: the sponsor or political advertising service must be given the opportunity to correct or complete the missing information.

  A removal or restriction of the advertisement would trigger both Article 15(9) of the TTPA, requiring notification to the sponsor or service provider, and Article 17 DSA, requiring a statement of reasons to the recipient of the service. While statements of reasons sent pursuant to Article 17 DSA will be publicly available under the Transparency Database pursuant to Article 24 DSA, the notification sent pursuant to Article 15 of the Regulation will not be reflected therein as the scope of the Transparency Database is limited to statement of reasons sent under the DSA.

  In light of the above, the applicable norm is parallel application, where relevant. In principle, both Article 15(9) of the TTPA and Article 17 DSA may apply simultaneously where the political advertisement in question is both non-compliant under the TTPA and qualifies as "illegal content" within the meaning of the DSA. In such cases, when fulfilling the more extensive statement of reasons' obligation under the DSA towards the recipient of the service, intermediaries must comply with the specific notification obligation under the TTPA vis-à-vis the sponsor or service provider being the recipient of the service.

- **Right to lodge a complaint:** Article 24 of the TTPA and Article 53 of the DSA both establish complaint mechanisms that allow individuals or entities to notify competent authorities of alleged infringements and to receive follow-up information. The TTPA provides for a general right to lodge notifications of possible infringements related to political advertising, with specific urgency requirements in the period preceding elections or referendums and also includes provisions on forwarding complaints to authorities in other Member States. The DSA similarly establishes a complaint mechanism for recipients of intermediary

[144] See also Communication from the Commission – Guidance to support the implementation of Regulation (EU) 2024/900 on the transparency and targeting of political advertising, C(2025)6829 of 8.10.2025, page 40-41.

services and their mandated representatives, with a structured process for submission to the Digital Services Coordinator and subsequent cross-border referrals as appropriate. While the scope of application of the two Regulations differs, the procedural functions of complaint lodging, authority notification, and transmission obligations may apply in parallel. In cases where a political advertisement is disseminated via an intermediary service, both mechanisms could apply concurrently.

The two provisions are not mutually exclusive and can apply in parallel, subject to the nature of the service and the actor involved. Complaints related to political advertising content disseminated through intermediary platforms that constitute a publishing service of political advertising may trigger both the TTPA and the DSA complaint regimes. In such cases, there is no integrated or shared mechanism with the DSA complaint system to resolve jurisdictional or procedural duplication. As DSCs will be responsible for ensuring coordination at national level in respect of providers of intermediary services under the TTPA and, where applicable, DSCs may be designated to supervise compliance of providers of intermediary services with the obligations laid down in Articles 7 to 17 and 21 of the TTPA, the involvement of the DSCs may ensure that uncertainties and duplication of enforcement layers are avoided.

- **Repositories for online advertising:** Article 13 of the TTPA provides for the establishment of a European Repository for online political advertisements ('the European repository') by the Commission. Political advertising publishers providing online political advertising services must make each political advertisement they publish, deliver or disseminate, and the information required under Article 12(1) of the Regulation available in the European repository. The obligations relating to the European repository will only become relevant as of the date of its deployment. In order to avoid any possible overlap with the parallel obligation under Article 39 DSA for very large online entities to put in place a publicly available advertisement repository, Article 13(2) of the TTPA "plugs in" the DSA by stating that those political advertising publishers that are very large online platforms and very large online search engines shall ensure that each political advertisement is made available in their DSA repository together with the information required under Article 12(1) of TTPA. In addition, it lays down that those political advertising publishers shall enable access to that information through the European repository from the moment of publication and for the entire period during which they present the political advertisement and for seven years after the political advertisement was last presented on their online interfaces. Furthermore, the enforcement of the specific obligations set forth in Article 39 DSA is a competence of the Commission, under the powers granted under the DSA. As pointed out in Recital 91 of the TTPA, to the extent that the Commission has exclusive competence to supervise and enforce the compliance of VLOPs and of VLOSEs within the meaning of the DSA with the obligations laid down in that Regulation, the Commission should assess compliance of those actors with their obligations concerning the European repository.

- **Legal representative:** Similar to Article 13 DSA, Article 21(1) of the TTPA requires providers of political advertising services established outside the Union but active within the Union to designate in writing a legal representative in one of the Member States where they offer services. The legal representative is responsible for compliance with the Regulation and may be held liable for infringements (Article 21(2) of the TTPA). In contrast to Article 13 DSA, Article 21 envisages additional requirements for the providers of political advertising services, i.e. mandatory registration, and entails also requirements for the national competent authorities and the Commission to further facilitate compliance. In this context, national competent authorities must maintain public registers of designated legal representatives (Article 21(4)), and the Commission must maintain a Union-wide portal linked to them (Article 21(5)). In sum, Article 13 DSA and Article 21 of the TTPA can apply in parallel.

  There is no incoherence between the rules on legal representative while some specificities can apply to the context of political advertising. Recital 89 of the TTPA clarifies that the legal representative appointed under Article 21 TTPA could be the representative designated on the basis of Article 27 of Regulation (EU) 2016/679 or the legal representative designated on the basis of Article 13 DSA.

- **Systemic risks:** Under Articles 34 and 35 DSA, providers of VLOPs and VLOSEs shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service

and its related systems, including algorithmic systems, or from the use made of their services and put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified.

The TTPA does not contain a specific requirements related to systemic risks. However, it refers in Recital 46 to the DSA and specifies Articles 34 and 35. Accordingly, Recital 46 states that political advertising publishers that are also VLOPs and VLOSEs within the meaning of the DSA should diligently identify, analyse and assess any systemic risks that their political advertising services pose in the context of their risk assessments according to Article 34 of that Regulation and put in place reasonable, proportionate and effective mitigation measures in accordance with Article 35 of that Regulation to address those risks.

*Special remarks on overlaps*

In sum, the TTPA and the DSA apply concurrently, in a limited, coherent and complementary manner, only to intermediary services involved in the dissemination of political advertising.

While its scope extends to offline and other activities, regarding the provision of intermediary services covered by the DSA, the TTPA can be seen as complementing DSA obligations by introducing sector-specific rules tailored to political advertising justified by the impact of those activities on core democratic processes, including detailed labelling and transparency requirements (Articles 11-12), restrictions and enhanced transparency on targeting and ad-delivery (Articles 18-19), and a European repository for online political advertisement (Article 13).

For this limited scope, both instruments can apply, imposing similar procedural duties, such as notification mechanisms (Article 15 TTPA / Article 16 DSA), statements of reasons (Article 15(9) TTPA / Article 17 DSA), complaint handling (Article 24 TTPA / Article 53 DSA) and ad repository (Article 13 TTPA / Article 39 DSA). These cases are not contradictory.

On supervision and enforcement, when the provisions of intermediary services connected to political ads is at stake, the DSA governs the horizontal supervision of intermediary services, while the TTPA governs the oversight of political advertising. Where the same conduct engages both sets of obligations, each framework follows its own supervisory track. In this context, the regulation on political ads explicitly addressed the need for cooperation between both at national and Union level, including through dedicated platforms (e.g. Network of national contact points which has to work in close cooperation with other networks such as the European Board for Digital Services). This cooperation should serve as the basis for sharing best practices and ensuring coherence in applying and enforcing the rules.

Overall, the relationship between the two instruments is best characterised as complementary with partial parallel application in some instances, for a limited scope of relevant services, i.e. intermediary service involved in the dissemination of political advertising. The TTPA introduces specific obligations for political advertising without prejudice to the DSA. In order to avoid possible operational uncertainty for providers or duplication in procedural duties, close cooperation between the relevant competent authorities as explicitly provided in the TTPA, will be important.

## Regulation (EU) 2024/1028([145]) – [Short Term Rental Regulation]

*General information*

The Short-Term Rental Regulation (STR Regulation) was adopted on 11 April 2024, and it will be applicable from 20 May 2026. The European Commission will carry out an evaluation of the Regulation by 20 May 2031 (Article 18 STR Regulation).

As per Article 1 STR Regulation, the "Regulation lays down rules for data collection by competent authorities and providers of online short-term rental platforms and data sharing from online short-term rental platforms to competent authorities relating to the provision of short-term accommodation rental services offered by hosts through online short-term rental platforms". The STR Regulation thus aims to set new standards for data collection and sharing on short-term rentals within the EU in order to enhance transparency, provide reliable information for public authorities, improve housing market regulation, and protect consumers from fraudulent offers.

The Regulation does not oblige Member States to set up a registration system for short-term rentals, but if they do, the Regulation and its harmonised rules apply. Registration procedures are based on self-declarations by hosts of short-term rental units. Registration numbers will be publicly accessible via a registry to be put in place by Member States.

*Personal scope*

As per Article 2(1) STR Regulation, the Regulation applies to (1) online short-term rental platforms providers (defined in Article 3(5) STR Regulation as an 'online platform' referring to Article 3(i) DSA, that allows guests to conclude distance contracts with hosts for the provision of short-term accommodation rental services), and to (2) hosts providing short-term accommodation rental services. The Regulation does not apply to hotels and similar accommodations, including hostels, resort hotels, suite or apartment hotels and motels, as well as accommodation in camping grounds, recreational vehicle parks and trailer parks (Article 3(1) STR).

As per Article 2(1) STR Regulation, the Regulation applies to online short-term rental platforms providers offering their services in the EU, irrespective of their place of establishment.

*Material scope*

The Regulation lays down rules for data collection by competent authorities and providers of online short-term rental platforms, as well as data sharing from online short-term rental platforms to competent authorities. More specifically as regards short-term rental platforms, the Regulation sets out compliance by design obligations (Article 7), an obligation of such platforms to conduct a best-effort assessment of the self-declaration submitted by hosts regarding the application of a national registration procedure (Article 8), and finally reporting obligations for platforms (Article 9).

*Enforcement*

Article 15 STR Regulation lays down the rules for enforcement. The Article specifies that for the purposes of the enforcement of the compliance by design obligations on short-term rental platforms pursuant to Article 7(1), and the best effort checks under Article 8 STR Regulation, the enforcement rules under DSA Chapter IV apply. Additionally, Recital 29 reiterates that the authority to enforce the compliance by design obligation set out in the STR Regulation lies with the designated Digital Services Coordinator of the country where the platform is established, other competent authorities, or the European Commission, according to the division of

[145] Regulation (EU) 2024/1028 of the European Parliament and of the Council of 11 April 2024 on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724.

responsibilities established in DSA Chapter IV. It further clarifies that the Commission's power to take direct enforcement actions is framed to Very Large Online Platforms (VLOPs).

On the other hand, Recital 30 and Articles 15(2) and (3) specify that the authorities designated by the Member State of the relevant single digital entry point (i.e. usually where the relevant accommodation is located) are competent to enforce Articles 6 (verification of host's declaration and supporting documents), 7(2) (transmission of information on random compliance checks to competent authorities), 7(3) (information regarding the applicability of registration procedures) and 9 (transmission of activity data and registration numbers), rather than the Member State where the service provider is established. This approach centralises enforcement responsibilities with the Member State managing the digital interface, thereby streamlining oversight and compliance monitoring under the STR Regulation.

*Interactions with the DSA*

The STR Regulation was adopted after the DSA, and contains several references in its Recitals (8, 16, 17, 29) and Articles 2(3)(b), Article 3(5) and Article 15(1), being generally without prejudice to the DSA.

On **personal scope**, the STR Regulation only applies to online short-term rental platforms providers as per Article 2(1) STR Regulation, which are a subset of online platforms under the DSA. The respective definition in Article 3(5) STR therefore also directly references Article 3(i) DSA, identifying those providers as allowing guests to conclude distance contracts with hosts for the provision of short-term accommodation rental services. The particular difference in personal scope of these two instruments is twofold; first, the relevant provisions of the DSA applying to online marketplaces (Articles 30-32 DSA) cover only B2C relationships (allowing traders to conclude distance contracts with consumers), while the STR' short-term rental platforms can also cover C2C relationships (private hosts to guests). Second, the DSA exempts small- and micro-sized companies from those obligations, while a small short-term rental platform is subject to the STR.

Recital 8 STR Regulation also specifies that webpages or other electronic means which connect hosts with guests without any further role in the conclusion of direct transactions should be excluded from the scope of the Regulation. Online platforms intermediating the provision of short-term accommodation rental services without remuneration, for example, online platforms intermediating the exchange of dwellings, are not covered by these rules unless, due to the specific way they are designed, they involve remuneration, including any form of economic compensation.

With regards the **territorial scope**, both the DSA and the STR Regulation apply to providers that offer services in the EU, irrespective of their place of establishment (See Article 2(1) DSA and Article 2(1) STR Regulation).

As per **material scope**, the DSA and the STR Regulation interplay, as they both include obligations for online platforms in relation to information obligations (Article 5 STR Regulation, Article 30 DSA), compliance by design (Article 7 STR Regulation, Article 31 DSA), monitoring obligations (Article 8 STR Regulation, Article 30(2) DSA), data reporting obligations (Chapter III STR Regulation, Chapter II DSA), as well as implementation and enforcement (Chapter IV STR Regulation, Chapter IV DSA). However, there is no overlap in material scope in any of these provisions (they are rather of a complementary nature), as the STR is adding specific obligations, "on top" of the DSA obligations for a particular sub-set of platforms.

The sections below provide further analysis on each of these topics:

- **Obligation for information provision**: Article 5 STR Regulation requires hosts to provide detailed data to ensure transparency, which adds to the obligations under Article 30 DSA on the traceability of traders. However, in case of Article 5 STR Regulation it is the host (trader) that must provide this information to the competent authorities, whereas Article 30 DSA requires online platform to collect this information from the trader. Hence, there is an interplay, but no overlap and these obligations are complementary in as far as professional hosts, qualifying as traders under the DSA, are concerned.

- **Compliance by design:** Article 31 DSA obliges all providers of online platforms allowing consumers to conclude distance contracts with traders to organise and design their online interface in a way to allow traders to comply with their information obligations under Union law, in particular their name, address, telephone number and email address. In addition, the providers must make best efforts to assess whether traders have indeed provided the required information Meanwhile, Article 7 STR Regulation contains additional requirements for short-term rental platforms interfaces which must be designed and organised in a way to oblige hosts to self-declare whether the unit offered for short-term accommodation rental services is located in an area where a registration procedure has been established, and allow users to identify the unit through a registration number which needs to be displayed as part of their listing. Both legislations therefore describe how the online interface should be designed and organised, and which information needs to be provided.

  Whereas the information requirements under Article 31 DSA are however of a general nature and refer further to information requirements under applicable Union law, Article 7 STR Regulation specifically addresses the self-declaration of the host. Moreover, while under Article 31(2) DSA the online interface must only *enable* the trader to provide the information, Article 7 STR Regulation has a stricter scope by providing that the online interface must *require* the host to provide information – in this case a self-declaration. In both cases the provider must make best efforts to assess whether the information has been provided and is complete (Article 31(3) DSA and Article 8 STR Regulation). Hence, insofar as a host also qualifies as a trader under the DSA, the two frameworks are complementary: the STR Regulation adds sector-specific compliance requirements that build upon the obligations in the DSA.

  Both articles also oblige the platform providers to conduct random checks of the content of the information provided with reasonable effort. Article 7(2) STR Regulation however further obliges the provider to inform the competent authority if the results of such checks indicate incorrect information. Similarly to Article 8 DSA, Article 8 STR Regulation prohibits any general monitoring obligation.

- **Reporting obligations:** While both frameworks impose reporting obligations, they differ in scope, purpose, and content. Chapter III STR Regulation imposes specific reporting obligations on online short-term rental platforms and hosts, focusing on data collection, sharing with authorities, and transparency regarding rental activities. The DSA, however, requires providers of intermediary services to publish annual transparency reports detailing content moderation activities, including orders received from authorities, complaints handled, and the use of automated tools.

  When considering reporting obligations, insofar as the personal scope overlaps, both DSA and STR Regulation are applicable at the same time. The STR Regulation focuses on activity data and registration number transmission to the single digital entry point of the Member State where the unit is located, and the establishment, functionalities and coordination of these single digital entry points. Meanwhile, Chapter III DSA centres around transparency in content moderation and platform governance, such as recommender system and advertising transparency. As such, these distinct objectives mean that while both pieces of legislation impose certain reporting duties, they address different facets of platform operation, thus applying in parallel rather than overlapping.

Finally, both Regulations include provisions on enforcement. While the STR Regulation refers to the DSA when it comes to the enforcement of Article 7(1) and Article 8, Article 15(2) STR Regulation provides for an enforcement mechanism specific for the sector in certain cases and stipulates that the authorities designated by the Member State of the relevant single digital entry point are competent to enforce:

- Article 7(2): Platforms' obligation of providing information to the competent authorities on the result of random compliance checks (incorrect declarations of hosts, the misuse of a registration number, or invalid registration numbers);
- Article 7(3): Platforms' obligation of providing information to hosts of the applicability of registration procedures;

- Article 9: Platforms' obligation of transmitting complete and accurate activity data per unit, together with the corresponding registration number as provided by the host, the specific address of the unit and the URL of the listing.

*Special remarks on interplay*

As we have observed, both Regulations have several touching points. The personal scope of the STR and the DSA partially interplay, when dealing with online short-term rental platforms providers, but in a more narrowed way and without contradiction. When it comes to the material scope, despite both Regulations imposing reporting duties, they cover different aspects of the platform operation, thus interplaying but not overlapping, ending up in complementarity.

DSA transparency and information requirements apply horizontally to online platforms' activity, whilst STR focuses on sector specific-reporting obligations duties, working together with synergy.

It is relevant to note how the DSA already fully applies to several situations and cases for the interest of the STR, especially considering the delayed application of some of its provisions.

Thus, Article 10 DSA could be applied to issue orders to provide information (recipients or registered hosts, listings, e.g.) by online short-term rental platform providers, whenever national law provides the necessary legal basis for it. Furthermore Articles 30 and 31 under Section IV DSA can be also applied but limited to traders and professional hosts (B2C). Online short-term rental platform providers are required to design their interface in a way that information necessary for the clear and unambiguous identification of the service is provided (Article 31(2) DSA). The same applies for the random checks for identified illegal products, based on Article 31(3) DSA, although its applicability again depends on the characteristics of such databases and the national legal framework.

## Regulation (EU) 910/2014 ([146]) – [eIDAS Regulation]

*General Information*

The eIDAS Regulation was adopted in July 2014 and has been in application since 1 July 2016, with some exceptions (Article 52(2)). The Regulation has been amended twice since its adoption, most prominently through Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. This amending Regulation extensively improved Regulation (EU) 910/2014 by enhancing the existing provisions on trust services and establishing the European Digital Identity Framework, including the EU Digital Identity (EUDI) Wallet.[147] The revised legal framework is commonly known as eIDAS2. In line with Article 49(1), the Commission shall review the application of the Regulation by 21 May 2026.

The eIDAS Regulation aims to ensure the proper functioning of the internal market and achieve an adequate level of security of electronic identification (eID) means and trust services used across the EU. This is with the aim of enabling and facilitating the right of natural and legal persons to participate in the digital society safely and to access online public and private services throughout the EU – Article 1. To achieve this, the Regulation:

- Establishes the conditions under which Member States should recognise the eID of natural and legal persons under the scheme of another Member State, including via European Digital Identity Wallets (EUDI Wallets) – Article 1(a).
- Establishes rules for trust services – Article 1(b).

[146] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[147] Regulation (EU) No 910/2014 was also subject to amendments by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

- Establishes a legal framework for a wide range of electronic trust mechanisms (e.g. electronic signatures, electronic seals, electronic archiving, etc.) – Article 1(c).

*Personal scope*

The eIDAS Regulation primarily places obligations on a range of different types of entities:

- Trust service providers established in the EU – defined in Article 3(19) as 'a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider', with trust services defined in Article 3(16) as 'an electronic service normally provided for remuneration which consists of' a wide range of electronic trust mechanisms (e.g. the issuance and validation of certificates for electronic signatures, certificates for electronic seals). Typically, these services are provided by private companies.
- Relying parties – defined in Article 3(6) as 'a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service'. Examples include banks, financial institutions, eGovernment portals, etc.
- EUDI Wallet Providers – As per Article 5a(2), these can be Member State authorities, private contractors working under national mandates, or public-private consortia working independently of a Member State but recognised by that Member State.

*Territorial scope*

The eIDAS Regulation primarily applies to eID schemes notified by a Member State, to EUDI Wallets provided by a Member State and to trust service providers established in the EU. However, Article 14 (on international aspects) governs trust services provided by trust service providers established in a third country or by an international organisation – such services need to be recognised by means of implementing acts or an agreement concluded between the EU and the third country or international organisation.

*Material scope*

The eIDAS Regulation governs eID schemes, EUDI Wallets and the provision of trust services within the EU, in particular for electronic transactions (Article 1).

Chapter II governs digital identity, establishing rules for the implementation, governance and use of:

- **EUDI Wallets** (Section 1, Article 5a-5f) – these provisions mandate that each Member State shall provide at least one EUDI Wallet (Article 5a(1)) and details the ways in which such wallets can be provided, as well as other requirements related to, amongst others, user functionalities and control, security breach notifications, validation mechanisms, technical support and data protection (Article 5a). The remainder of this section stipulates provisions related to the registration requirements for relying parties (Article 5b); certification (Article 5c and 5d); security breach handling (Article 5e); and cross-border acceptance of EUDI Wallets (Article 5f).

- **eID schemes** (Section 2, Article 6-12b) – these rules provide for mandatory cross-border recognition of eID schemes (Article 6); notification to the Commission (Article 9) and related eligibility for notification (Article 7); assurance levels and criteria for eID schemes (Article 8); and rules on issues such as security breaches (Article 10), liability (Article 11), cross-border identity matching (Article 11a), interoperability (Article 12), certification (Article 12a) and access to hardware and software features (Article 12b).

Chapter III governs trust services, outlining general provisions in section 1, regulating issues such as liability and burden of proof for trust service providers (Article 13) and provision of trust services by providers established in third countries or by international organisations (Article 14). Specific provisions on the requirements for qualified trust services (Section 3) and non-qualified trust services (Section 2) are then

provided, before specific rules on the wide range of electronic trust mechanisms covered by the Regulation are stipulated. These cover electronic signatures (Section 4), seals (Section 5), time stamps (Section 6), registered delivery services (Section 7), website authentication (Section 8), electronic attestation of attributes (Section 9), electronic archiving services (Section 10), and electronic ledgers (Section 11).

*Enforcement*

The governance framework for the eIDAS Regulation is established under Chapter IVa. Specifically, it contains separate supervision provisions for the EUDI Wallet Framework (Article 46a) and trust services (Article 46b) through the designation of supervisory bodies; as well as single points of contact (Article 46c); and an overarching Cooperation Group (Article 46e).

The supervisory bodies designated by each Member State have a range of powers, including: to audit or request a conformity assessment body to perform a conformity assessment of qualified trust service providers – Article 20; liaison with Data Protection Authorities (DPAs) under GDPR on personal data protection breaches – Article 20(2); grant/withdraw qualified status; and carry out on-site inspections and off-site supervision related specifically to the European Digital Identity Wallet – Article 46a(4)(d).

In addition, Member States are required to maintain and publish trusted lists, in particular for qualified trust service providers (Article 22), while penalties as regards trust service providers are established in Article 16.

*Interactions with the DSA*

The original text of the eIDAS Regulation was adopted prior to the DSA; but, the amendments to the eIDAS Regulation by Regulation (EU) 2024/1183 establishing the European Digital Identity Framework introduced a reference to the DSA within Article 5f(3) of eIDAS. This Article concerns cross-border reliance on EUDI Wallets, and specifically requires VLOPs (as per Article 33 of the DSA) that require user authentication for access to online services to accept and facilitate the use of valid EUDI Wallets. As Recital 57 states, given the importance of these very large platforms' reach, as expressed in important number of recipients of the service and economic transactions (at least 45 million users in the EU), the obligation to accept European Digital Identity Wallets is necessary to increase the protection of users from fraud and to secure a high level of data protection. As discussed further below, this has specific implications for the implementation of age assurance and age verification measures for the online protection of minors under Article 28 DSA.

The DSA references the eIDAS Regulation in Article 30 concerning the traceability of traders. Specifically, Article 30(1)(b) DSA allows the use of eID (as defined by Article 3 of the eIDAS Regulation) by online platforms that allow consumers to conclude distance contracts with traders to fulfil their obligation to identify such traders for the purpose of allowing those traders to use their platform 'to promote messages on or to offer products or services to consumers located in the Union'.

Furthermore, the Guidelines on measures to ensure a high level of privacy, safety and security for minors online[148], developed and published by the European Commission pursuant to Article 28(4) of the DSA, state that EUDI Wallets (as provided for by eIDAS Regulation), once implemented, will provide 'safe, reliable, and private means of electronic identification' and will embed the opportunity to 'receive a token of age', which would represent a 'privacy-preserving, data-minimising, non-traceable and interoperable' solution. EUDI Wallets are therefore considered to be an appropriate and proportionate measure that can be implemented by providers of online platforms to meet their obligations under Article 28(1).

On **personal scope**, there are several points of interplay between the DSA and the eIDAS Regulation.

[148] Annex to the Communication to the Commission. Approval of the content on a draft Communication from the 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. Last accessed on 7 August 2025 at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.

Under Article 30(1)(b) of the DSA, providers of online platforms have the possibility of acting as relying parties under the eIDAS Regulation and accept eID for the purpose of identifying traders concluding distance contracts with consumers located in the EU on their platform.

Under Article 5f of the eIDAS Regulation, providers of very large online platforms (VLOPs) are required to accept and facilitate the use of EUDI Wallets in accordance with the eIDAS Regulation where they require user authentication for access to online services.

With regards to **territorial scope**, while the DSA applies to providers established outside the EU that are providing services to users within the EU, the eIDAS Regulation only permits recognition of non-EU services via specific agreements.

On **material scope**, the related provisions in the two laws are complementary, with: (i) an obligation for VLOPs to accept EUDI Wallets for user authentication purposes (Article 5f eIDAS); and (ii) a requirement for providers of online platforms that allow consumers to conclude distance contracts with traders to permit electronic identification (as per eIDAS) for trader identification (Article 30(1) DSA).

The use of EUDI Wallets for age verification purposes is also relevant in the context of Article 28 DSA; while this possibility is not explicitly stated in the DSA, the Commission's guidelines on the protection of minors pursuant to Article 28(4) DSA (paragraph 42-44) specify that the development of a harmonised, EU-wide approach to age verification, accompanied by a comprehensive age verification blueprint, will support compliance, with this provision applicable to online platforms accessible to minors.[149] However, EUDI Wallets are only planned to be provided by Member States by end of 2026.

Beyond these complementary (additional) provisions, the two laws do not contain any overlapping or conflicting substantive rules.

Finally, on **enforcement**, the enforcement mechanisms established in the two laws are similar in structure, but the content focus differs and overlaps only in very specific circumstances – i.e. as relates to: (i) the use of electronic identification established (as governed by eIDAS) for trader identification under Article 30 DSA; or (ii) the (future) use of EUDI Wallets for user authentication by VLOPs (Article 5f eIDAS).

*Special remarks on interplay*

The two laws do not contain any overlapping or conflicting rules, thus interplaying in a complementarity manner. The interacting provisions is not in application yet, given that EUDI Wallets will be provided by Member States only by end of 2026.

[149] 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.

## Directive (EU) 2024/1385 ([150]) – [Violence Against Women and Domestic Violence Directive]

*General Information*

Directive (EU) 2024/1385 on combating violence against women and domestic violence (VAWDV) was formally adopted on 14 May 2024. Member States are required to transpose the Directive into national law by 14 June 2027, ensuring a harmonised minimum level of protection and legal certainty across the EU.

The primary aim of the VAWDV Directive is to prevent and combat violence against women and domestic violence by setting minimum common standards for criminalising certain forms of violence, supporting victims, and improving access to justice and protection. The Directive also strengthens cross-border cooperation and encourages Member States to adopt effective, coordinated responses that uphold the fundamental rights and dignity of victims, in line with EU values.

*Personal scope*

The VAWDV Directive applies to a range of public and private actors with responsibilities for preventing and responding to violence, particularly in the areas of criminal justice, victim protection, and online content governance. Specifically, the Directive imposes obligations on the following categories of actors: Member States and their competent authorities; judicial, prosecutorial, and law enforcement authorities; victim support services, healthcare providers, and social services; employers and educational institutions. The Directive does not impose obligations on providers of online intermediary services covered by the DSA. However, it mandates Member States to take the necessary measures to ensure that online publicly accessible material is promptly removed or that access thereto is disabled, such as removal orders (Article 23).

The Directive requires Member States to establish jurisdiction over the offences set out in Articles 3-9 (see section I.1.3 on material scope below) when the crime occurs on their territory or when the offender is a national (Article 12(1)(a)-(b)). Jurisdiction is also extended to offences committed abroad where the victim or offender has nationality or habitual residence ties to the Member State, with notification to the Commission (Article 12(2)(a)-(b)). Where offences are committed via information and communication technologies (ICT), Member States must assert jurisdiction whenever the content is accessed from their territory, regardless of the provider's location (Article 12(3)). This acknowledgement aligns the Directive with the DSA's recognition of the systemic risks posed by platform-based content and services as regards actual or foreseeable negative effects in relation to gender-based violence, the protection of public health, and minors and serious negative consequences to a person's physical or mental well-being (Article 34(1)(d) DSA). Thus, the Directive ensures that its protective and preventive measures address not only violence occurring in physical spaces within the Union but also emerging forms of harm facilitated through digital environments and cross-border interactions.

*Material scope*

The material scope of the VAWDV Directive spans five main areas: Chapter 2 harmonises Member States' criminal laws with respect to specific forms of violence, requiring them to establish effective penalties for the following intentional conduct: Female genital mutilation (Article 3), forced marriage (Article 4), non-consensual sharing of intimate or manipulated material (Article 5), cyber stalking and cyber harassment (Articles 6–7), cyber incitement to violence or hatred (Article 8), inciting, aiding and abetting and attempt of the abovementioned criminal offences (Article 9), with penalties, aggravating factors, and jurisdictional provisions further clarified in Articles 10–13.

[150] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence.

Chapter 3 and 4 lay out procedural rights and safeguards for victims including: The right to report through safe and accessible channels (Article 14), obligations on competent authorities to investigate effectively and without delay and adopt protection measures (Articles 15–19), individual risk and support assessments (Articles 16–17), protection of victims' private life (Article 20), guidelines for law enforcement and prosecutorial authorities (Article 21), victims' access to compensation (Article 24), specialist support services (Articles 25–33), including for children, victims of female genital mutilation, sexual violence, and harassment at work. Article 23 introduces content related obligations, requiring Member States to ensure the removal or disabling of access to illegal online publicly accessible material related to criminalised VAWDV offences. These provisions apply in complementarity with the DSA and specifically target material addressed under Articles 5, 7, and 8 of the Directive. Competent authorities may issue binding legal orders to remove or disable access to these materials, subject to the requirements set out in Article 9(2) of the DSA.

Chapter 5 mandates awareness-raising and public education (Article 34), promotion of the centrality of consent in sexual relationships (Article 35), training and capacity-building for professionals in law enforcement, judiciary, healthcare, education, and media (Article 36), development of intervention programmes to prevent first-time offences and recidivism (Article 37).

Finally, the Directive also promotes cooperation, monitoring, and data-sharing through: National bodies, including equality bodies (Article 22), Multi-stakeholder engagement with civil society, service providers, and social partners and institutional support for victims with intersectional vulnerabilities (Article 33). It is worth noting that Article 42 VAWDV Directive mandates Member States to encourage self-regulatory cooperation between relevant intermediary service providers, such as the establishment of codes of conduct. This is complementary to the system of codes of conduct at Union level under Article 45 DSA.

*Enforcement*

The VAWDV Directive relies on a network of designated national bodies, cooperation protocols, and data transparency requirements to ensure effective compliance. Key components include: National Coordinating Bodies (Article 38), National Action Plans (Article 39), multi-agency coordination (Article 40), Civil Society and NGO Cooperation (Article 41), Digital Platform Involvement (Article 42), EU-Level Cooperation (Article 43), Data Collection and Oversight (Article 44), Judicial Remedies and Redress (Article 23(4)).

*Interactions with the DSA*

Article 46(1)(f) VAWD establishes that the Directive does not affect the application of the DSA, therefore recognising the complementary nature of the two legal instruments in addressing gender-based violence.

The VAWDV explicitly refers to the DSA in several provisions to acknowledge and align with the regulatory framework governing intermediary services and online platforms in particular. Notably:

- The Directive's provisions on removal or disabling of illegal online material (Recital 52) and encouragement of Member States to promote voluntary self-regulatory measures and cooperation between relevant intermediary service providers on detecting and removing illegal material related to cyber violence (Recital 86) operate in complement to the DSA.
- Article 2, letters (d) and (e), "adopt" the definitions of "hosting service providers" and "intermediary service providers" from Article 3(g) of the DSA Regulation, integrating the terminology and scope of digital service providers within the VAWDV framework.
- Article 23(1), which mandates Member States to ensure the prompt removal or disabling of access to online publicly accessible material related to offences covered by the VAWDV, in accordance with the conditions set out in Article 9(2) of the DSA.
- Article 46(1)(f), which denotes that the Directive does not affect the application of the DSA.

The DSA contains references to the material scope of the VAWDV, namely Recital 83, Recital 87, Article 34(1)(d), Article 35(1)(c), where gender-based violence and/or cyber violence is addressed as part of systemic

risks, content moderation duties, protection of vulnerable groups, and codes of conduct to prevent abusive activities online.

On **personal scope**, the Directive refers to definitions from the DSA on hosting service providers and online intermediary service providers as some of the Directive's provisions mention intermediary and hosting service providers (notably Article 23 on measures to remove online materials and Article 42 on cooperation between intermediary service providers), but it does not impose standalone obligations on them.

The personal scopes of the DSA and VAWDV interplay, in particular where conduct criminalised under the VAWD is qualified as illegal content under national law.

Regarding **material scope**, the VAWDV Directive defines and criminalises various acts of gender-based and domestic violence, including online-specific conduct such as cyber stalking, cyber harassment, non-consensual sharing of intimate material, and incitement to violence or hatred on gender grounds. It establishes substantive criminal offences, victim protection measures, and state obligations to investigate and sanction such acts through national criminal justice systems. As a consequence, these offences are to be considered "illegal content" in the context of the DSA under Article 3(h) DSA, triggering mechanisms such as orders to act against illegal content and to provide information (Articles 9 and 10), notice and action (Article 16) or systemic risk assessment and mitigation obligations (Articles 34 and 35) for very large online platforms and very large online search engines.

Therefore, the VAWDV "plugs in" to the scope of the DSA: by defining the illegality of certain online behaviours, and triggers DSA's procedural responses by intermediary service providers. Furthermore, Article 23 of the VAWDV obliges Member States to empower national authorities to issue binding legal orders to remove or to disable access to publicly accessible material linked to the Directive's offences. This is a necessary complement to Article 9 DSA, which is not an empowering provision, but applies in the case of orders issued on the basis of Article 23 VAWDV's transposition.

As regards **enforcement**, the VAWDV's enforcement is rooted in national criminal justice systems. Member States are required to investigate, prosecute, and sanction criminal offences such as non-consensual dissemination of intimate material (Article 5), cyber stalking (Article 6), and related cybercrimes. Competent national authorities are responsible for issuing protection measures and, where applicable, removal orders for online content linked to such offences (e.g., under Article 23). The enforcement focus here is on individual perpetrators and the protection of victims, not on platforms as regulated entities. There is therefore no overlap or conflict in terms of enforcement of both instruments. National orders issued in the context of Article 23 will be enforced following the rules under VAWDV and its transposition, while Article 9 DSA (which imposes extra obligations on the receiving intermediary) will be enforced in the context of the DSA enforcement structure.

*Special remarks on interplay*

In summary, the interplay between the VAWDV and the DSA is characterised by complementarity. The Directive does not create direct obligations for intermediaries, but by criminalising specific forms of online gender-based violence, it defines categories of "illegal content" that activate the procedural duties of intermediary services under the DSA. Article 23 VAWDV strengthens this connection by empowering national authorities to issue removal orders, which in turn fall under the framework of Article 9 DSA. Enforcement remains distinct: the VAWDV relies on national criminal justice systems to address perpetrators and protect victims, while the DSA governs the obligations of intermediary services once notified of illegal content. This dual structure ensures that the Directive supplies the substantive illegality, while the DSA provides the procedural infrastructure for content moderation, without creating conflicts or duplication.

## Regulation (EU) 2024/1781 ([151]) - [Ecodesign for Sustainable Products Regulation]

*General Information*

The Ecodesign for Sustainable Products Regulation (ESPR) was adopted on 13th June 2024 and entered into force in July 2024. It is required to be evaluated by 19 July 2030.

Based on Article 114 TFEU, the ESPR sets out the legal framework for the setting of ecodesign requirements for a wide array of products placed on the EU market, aiming to improve the circular economy and enhance environmental sustainability across the Union. It mandates performance and information requirements for products, via a digital product passport to ensure traceability and provide consumers and other actors with crucial data throughout a product's life cycle. The ESPR also introduces measures to prevent the destruction of unsold consumer products and to specifically prohibit the destruction of textiles and footwear, alongside provisions for market surveillance and conformity assessment by notified bodies to ensure compliance. The European Commission is empowered to adopt delegated acts to specify these ecodesign requirements for various product groups, ensuring alignment with existing environmental and energy objectives.

*Personal scope*

The ESPR applies to any physical goods that are placed on the market or put into service, including components and intermediate products, with the exception of food, feed, medicinal products, veterinary medicinal products, living plants, animals and micro-organisms, products of human origin, products of plants and animals relating directly to their future reproduction and vehicles (in respect of those product aspects for which requirements are set under sector-specific Union legislative acts applicable to those vehicles).

The ESPR is a framework legislation that lays the foundation for the subsequent adoption of concrete rules, either on a product-by-product basis or horizontally, based on groups of products with similar characteristics.

The process started with a prioritisation exercise, following this, the Commission adopted the first ESPR and "Energy Labelling Working Plan" in April 2025, setting out which products will be prioritised over the coming years.

Article 2 (46) of the ESPR defines "economic operators" who are subject to obligations. These are the manufacturer, the authorised representative, the importer, the distributor, the dealer, and the fulfilment service provider.

The ESPR applies to providers of online marketplaces, which are defined in Article 2(54) as an "intermediary service(s) using an online interface which allows customers to conclude distance contracts with economic operators for the sale of products covered by delegated acts".

*Territorial scope*

The ESPR applies to all products placed on in the EU market, regardless of where they are manufactured. The Regulation aims to ensure that economic operators comply with ecodesign (performance or information) requirements adopted in delegated acts based on the ESPR when selling to EU customers. Its territorial scope is aligned with other EU product legislation, making compliance mandatory for any product circulating within the EU.

*Material scope*

[151] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC, OJ L, 2024/1781.

The ESPR sets out a framework for setting out specific sustainability criteria throughout the life cycle of products, such as durability, repairability, recyclability, energy efficiency, recycled content or restrictions on substances of concern that negatively affect the circularity of products. The ESPR also provides for the creation of a digital product passport to improve transparency and traceability. The ESPR aims to reduce the environmental impact of products and promote a circular economy by setting eco-design rules for a wide range of product categories.

While the ESPR does not regulate online platforms as economic operators, it assigns them a supporting role in enforcing compliance for products sold online. Pursuant to Article 35 ESPR, providers of online marketplaces must cooperate with market surveillance authorities to facilitate any action taken to eliminate or mitigate the non-compliance of a product that is or was offered for sale online through their services. For that purpose, the ESPR highlights the compliance by design obligations for providers of online platforms under Article 31 DSA, regular and structured exchanges with market surveillance authorities on actions taken against non-compliant products, including the removal of product offers and granting access to their interfaces to help market surveillance authorities identifying non-compliant products sold online (Recital 71). Article 35(2) ESPR establishes a legal basis for market surveillance authorities to order a provider of an online marketplace to act against specific items of content referring to a non-compliant product. Such orders must be issued in accordance with the requirements set out in Article 9 DSA. Article 35(3) ESPR furthermore obliges providers of online marketplaces to establish a single contact point for the purposes of direct communication with Member States' market surveillance authorities, which can be the same point of contact as established under Article 11 DSA.

*Enforcement*

For its enforcement, the ESPR relies on Regulation (EU) 2019/1020 (Market Surveillance Regulation - MSR). National market surveillance authorities are responsible for monitoring compliance, conducting inspections and taking corrective actions such as withdrawing or recalling non-compliant products. Customs authorities also play a role in checking products entering the EU market. The ESPR additionally supports enforcement through the use of digital product passports, which provide electronically accessible product compliance data. Online platforms are required to cooperate with authorities, including removing non-compliant listings when ordered. This framework ensures coordinated enforcement across the EU internal market.

*Interactions with the DSA*

The ESPR makes several references to the DSA in Article 35 as well as Recitals 70 to 72. The DSA does not make references to the ESPR.

On **personal scope**, Article 35 ESPR sets out obligations for providers of online marketplaces. While the DSA does not explicitly mention online marketplaces, it regulates online platforms and sets out specific obligations for online platforms allowing consumers to conclude distance contracts with traders, such as online marketplaces.

With regards to **territorial scope**, the ESPR applies to all products placed on or made available in the EU market, regardless of where they are manufactured. Meanwhile, the DSA regulates services that are offered to recipients in the EU, regardless of the place of establishment of the service provider.

Referring to the **material scope**, the ESPR stipulates several obligations for providers of online marketplaces, which complement the corresponding obligations in the DSA. While Article 35 sets out that Articles 11 and 30 DSA shall apply for the purposes of ESPR as well, Recital 71 also refers to the compliance by design obligations under Article 31 DSA. Accordingly, for the purpose of compliance with Article 31(3) DSA, providers of online marketplaces should utilise information available in the public user interface of the information and communication system referred to in Article 34 MSR. Providers of online marketplaces are also required to cooperate with market surveillance authorities such as by having regular exchanges on actions taken against non-compliant products, including the removal of product offers. Such a cooperation obligation does not follow from the DSA and can therefore apply in parallel. Providers of online marketplaces are mandated to establish a single contact point for direct communication with Member States' market surveillance authorities regarding

compliance with the ESPR. This contact point may be the same as those required by Article 22(1) GPSR or Article 11(1) DSA.

According to Article 35(2) ESPR, Member States must grant their market surveillance authorities the power to order a provider of an online marketplace to act against specific content referring to a non-compliant product, including its removal. Market surveillance authorities may issue such orders in accordance with Article 9 DSA.

The **enforcement** framework of the ESPR relies on the Market Surveillance Regulation and does not foresee cooperation mechanisms with the enforcement authorities of the DSA.

*Special remarks on interplay*

As describe above, there are no overlaps or contradictions between the DSA and the ESPR. Rather, the ESPR complements the DSA. Additionally, Articles 11 and 30 DSA apply for the purposes of the ESPR.

# Regulation (EU) 2024/1689([152]) – [Artificial Intelligence Act]

*General Information*

The Artificial Intelligence Act (AI Act) was adopted on 13 June 2024, entered into force on 1 August 2024, and envisages several deferred entry into application, depending on the concrete subject: From February 2025 (Chapters I and II), August 2025 (Chapters III, Section 4; Chapter V, Chapter VII, and Articles 78, 99 and 100, August 2026 (remainer Articles except for Article 6(1)), and August 2027 (Article 6(1)). Beyond this, Article 112 places a wide range of evaluation and review obligations on the Commission across several timelines[153].

As per Article 1 of the AI Act: "The Regulation aims to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation".

*Personal scope*

As set out in Articles 2(1), and 3(3) to 3(7), the AI Act applies to a defined set of actors in the AI value chain, including: (a) providers of AI systems and general-purpose AI (GPAI) models; (b) deployers of AI systems; (c) authorised representatives; (d) importers, or (e) distributors.

*Territorial scope*

According to Article 2, the AI Act applies when AI systems or GPAI models are placed on the Union market, or when AI systems are put into service or used in the Union, when providers are established or located in the Union or in a third country, and the output produced by the AI system is used in the Union, and when deployers are established or located in the Union. The AI Act also defines the rights of affected person that are located in the Union. Providers established in third countries that are making a high-risk AI system available on the Union market (Article 22 AI Act) or placing a GPAI model on the Union market (Article 54 AI Act) are required to appoint an authorised representative that is established in the Union.

*Material scope*

The AI Act establishes rules governing the technical requirements for and corresponding obligations of operators related to the placing on the market, the putting into service and the use of AI systems and the placing on the market of GPAI models in the EU, following a risk-based approach, while ensuring consistency with other applicable EU legislation. In particular, it covers the following areas:

- **The prohibition of certain AI practices:** Article 5 prohibits the following AI practices: the placing on the market, putting into service of use of AI systems which deploys subliminal or purposefully manipulative or deceptive techniques in significantly harmful ways; the placing on the market, putting into service of use of AI systems which exploit vulnerabilities of people due to their age, disability or specific

[152] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

[153] By 2 August 2028, the Commission shall report on the need for amendments to the list of high-risk AI systems (Annex III), amendments to the list of AI systems requiring additional transparency measures in Article 50, amendments enhancing the effectiveness of the supervision and governance system (Article 112(2)), the functioning of the AI Office (Article 112(5)), the progress on the development of standardisation deliverables (Article 112(6)) and the impact and effectiveness of voluntary codes of conduct (Article 112(7)); by August 2029, the Commission shall submit a report on the evaluation and review of the Regulation (Article 112(3)); and by 2 August 2031, the Commission shall carry out an assessment of the enforcement of the AI Act (Article 112(13)).

socioeconomic status in significantly harmful ways; the placing on the market, putting into service of use of AI systems which evaluate or classify natural persons or groups based on social behaviour or personal or personality characteristics in a way that can lead to their detrimental or unfavourable treatment; the placing on the market, putting into service of use of AI systems which assess or predict individual criminal offence risk; the placing on the market, putting into service of use of AI systems which create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV; the placing on the market, putting into service of use of emotion recognition systems in the workplace and education institutions, unless for safety and medical reasons, the placing on the market, putting into service of use of biometric categorisation systems which categorise according to certain sensitive categories, and the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement (unless strict exceptions apply and prior authorisation and other safeguards are in place).

- **Mandatory requirements for high-risk AI systems and obligations for operators of such systems:** Chapter III covers high-risk AI systems in detail:

- **Transparency obligations for providers and deployers of certain AI systems:** Detailed in Article 50, the AI Act places transparency obligations on: (i) providers of AI systems intended to interact directly with natural persons; (ii) providers of AI systems, including GPAI systems, generating synthetic content; (iii) deployers of emotion recognition or biometric categorisation systems; (iv) deployers of AI systems generating content.

- **Rules on GPAI models:** Chapter V sets out specific requirements for GPAI models (Article 53), including additional obligations for those that classify as posing systemic risks (Article 55).

  Some of these obligations include the drawing and keeping up-to-date technical documentation of the model, making available information and documentation to providers of AI systems intending to integrate the model into their AI systems, have a policy to comply with EU copyright and related rights legislation, and publish a detailed summary about the content used for training of the GPAI model. In addition, in the case of GPAI models with systemic risk, obligations further expand to perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, assessing and mitigating possible systemic risks at EU level, keeping track and reporting of serious incidents and ensuring an adequate level of cybersecurity and the physical infrastructure of the model.

*Enforcement*

The AI Act establishes a two-tiered governance system, at national and European level.

At national level, as per Article 70 AI Act, each Member State shall establish or designate as national competent authorities at least one "notifying authority" and at least one "market surveillance authority" (MSA), the latter also being appointed as single point of contact for the purposes of this Regulation (Art. 70(2)).

MSAs supervise and enforce compliance with the rules for AI systems, including prohibitions and rules for high-risk AI systems, according to Regulation (EU) 2019/1020 (Market Surveillance Regulation) (Article 74(1)). Member States shall determine the rules on penalties and other enforcement measures applicable to violations of the AI Act (Article 99(1)).

At EU level, the Commission oversees the AI Act's enforcement and implementation across Member States and has specific supervisory, investigatory and monitoring powers over providers of GPAI models (Articles 88-93). It has the power to conduct evaluations of GPAI models, request information and measures, and impose sanctions. According to Article 88(1), these powers are entrusted to the Commission's European Artificial Intelligence Office ('AI Office').

Article 75 contemplates several mutual assistance scenarios between the AI Office and MSAs when it comes to "general-purpose AI systems", where the competences of both levels interact. Moreover, Article 75(1) sets out

a special rule that where an AI system is built on a general-purpose AI model and both are offered by the same provider, the AI Office is responsible for the oversight and control of that AI system.

*Interactions with the DSA*

The AI Act contains several references to the DSA:

a. Recital 11 and Article 2(5) stipulate that the AI Act shall not affect the application specifically of the provisions on the liability of providers of intermediary services as set out in Chapter II of the DSA.

b. Recitals 118 to 120 of the AI Act clarify how the provisions of the AI Act complement the obligations for providers of intermediary services that embed AI systems or models into their services regulated by the DSA. Recital 118 states that, to the extent such systems or models are embedded into designated VLOPs/VLOSEs, thus being subject to the DSA's risk-management framework (as per Article 34-35 DSA) the corresponding obligations under the AI Act shall be presumed to be fulfilled, unless significant systemic risks not covered by the DSA are identified in such models.

c. Recital 119 clarifies that AI systems (as per the AI Act) may be provided as intermediary services or parts thereof (as per the DSA), while Recital 120 draws links between the provisions of the AI Act on the 'detection and disclosure that the outputs of those AI systems are artificially generated or manipulated' (i.e. Article 50 AI Act) and the risk-management provisions of the DSA (in particular its Articles 34 and 35).

d. Recital 136 highlights the complementarity between the AI Act's transparency rules for generative AI systems and AI-generated content and several provisions of the DSA, including the risk-management provisions (Articles 34 and 35) and on the general notice and action mechanisms (Article 16(6) DSA). As regards the notice and action mechanism, recital 136 states that the requirement to label certain AI-generated content under the AI Act should neither affect the assessment of that content's illegality nor impact the processing of illegal content notices hosting services providers.

The DSA makes no reference to the AI Act. Interplay with the scope & enforcement mechanism of the DSA

On **personal scope** and being a product safety regulation, the AI Act regulates AI systems and models, placing obligations on different types of operators, as listed above and which includes providers of high-risk AI systems, providers of GPAI models and deployers of high-risk AI systems, providers and deployers of prohibited AI systems and providers and deployers of certain systems subject to transparency obligations.

AI systems might be considered as online platforms or search engines by themselves or may be embedded into those services. More precisely, Recital 119 states that AI systems may be provided as intermediary services, or parts thereof, within the meaning of the DSA, such as search engines. This underlines the complementary of the AI Act as a product safety legislation to the DSA, whereby the AI Act ensures the safety of AI systems and certain AI models that are embedded into or constitute online platforms or search engines covered by the DSA.

Therefore, a provider and/or deployer of AI systems might be also subject to the DSA and be qualified as an intermediary services provider, including the designation of such intermediary service as a VLOP/VLOSEs.

When it comes to **territorial scope**, as per Article 2 AI Act, the Regulation applies to providers placing on the market, putting into service and use of AI systems and models in the Union, irrespective of whether they are established or located within the Union or in a third country. The DSA applies also to intermediary services offered to recipients of the service that are based in the Union (Article 2(1) DSA). Therefore, both territorial scopes interplay in a complementary manner.

Referring to **material scope**, the AI Act and the DSA pursue different but related objectives. As a product safety legislation, the AI Act aims to ensure that AI systems and models are safe, transparent, and compliant prior to their placing on the market or putting into service, and throughout their deployment and use. The DSA,

by contrast, aims to enhance safety and trust in the online environment, avoiding any societal risk which might appear from the use and interaction between online intermediary services providers and the recipients of those services, especially protecting users' fundamental rights including protection of minors online, information integrity and consumer protection. According to Article 2(4)(f) DSA, the DSA is without prejudice to Union law on product safety specifying and complementing its rules. The two frameworks interact when AI systems and models are embedded in online intermediary services or constitute online intermediary services. In these cases, the same practices may in principle fall under both sets of obligations. In this regard and within the meaning and taxonomy of this Report, several overlaps might be identified, as further developed below.

On **enforcement**, the AI Act is enforced at the national and EU level, as explained above. Under the DSA, compliance of online platforms and search engines not designated as very large is enforced at the Member State level by the Digital Service Coordinators, while the Commission has exclusive competence to enforce and monitor compliance of VLOPs and VLOSEs with the obligations the DSA imposes upon them to address systemic risks. When the same actor and the same practice is scrutinised under both the AI Act and the DSA, because it concerns an AI system or GPAI model embedded into an online platform or search engine, or the AI system can be considered a platform or search engine by itself, there is a risk of duplicative or inconsistent enforcement in case the AI Act and the DSA obligations are the same.

Regarding the enforcement of the two legal frameworks, issues may arise where the Commission may be responsible for supervision of the risk management obligations for VLOPSs and VLOPSEs embedding AI systems, while those AI systems may be subject to MSA's supervision for what concerns their compliance with the AI Act's rules for AI systems. A platform accessible to minors and embedding AI systems will be subject to obligations to protect minors under the DSA under supervision of DSCs, but that AI system is also subject to supervision by MSAs as regards AI systems exploiting vulnerabilities of minors, which is prohibited by the AI Act when likely to cause significant harm. Therefore, coordination between competent authorities is essential to ensure consistent application of EU law and avoid fragmentation across the Union.

*Special remarks on overlaps*

As mentioned above, there can be instances in which the same activity is subject to rules following from the DSA and the AI Act. How these rules interplay is established in several Recitals, nonetheless, these provisions still leave margin for interpretation.

Specific interactions between DSA and the AI Act are identified, which might apparently lead to some inconsistencies or contradictions.

- **Prohibited practices**

Article 5 AI Act prohibits certain practices, such as the placing on the market, putting into service or use of AI systems that deploy manipulative or deceptive techniques and that exploit of vulnerabilities of natural persons or specific group, including minors, in a way that causes or is likely to cause significant harm. These prohibitions apply to a subset of AI practices that are also covered by obligations under the DSA, for example the requirement that online platforms providers shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions (Article 25 DSA); and shall take appropriate and proportionate measures to ensure a high level protection of minors in online environments and not to present advertisements based on profiling of minors' personal data (Article 28 DSA); and VLOPs and VLOSEs are required to identify, assess, and mitigate systemic risks, including those arising from algorithmic or recommender systems (Articles 34-35 DSA).

The rules of the AI Act and the DSA both aim to prevent manipulative or harmful practices, but at different levels of intervention and through different set of requirements and means of enforcement. The AI Act's prohibitions only apply to a subset of practices when their conditions are fulfilled and in particular in case of deceptive, manipulative or exploitative AI system causing significant harms. They apply outright as practices that should be avoided by the online platforms and other intermediary service providers as these AI systems should not be put on the EU market or into service from the very outset. Compliance with the DSA obligations

for transparency of recommender systems, the behavioural VLOPS/VLOSEs obligations for systemic risk assessment and mitigation and the proportionate measures required by online platforms for minor protection can thus help to mitigate the risk of manipulative and deceptive AI systems deployed via the intermediary services, but they might not be enough in all cases. If the practice is proven to constitute a prohibition under the AI Act which is more specific and targets specific types of significantly harmful manipulative, deceptive and exploitative AI system, the AI Act explicit prohibitions complement the DSA provisions and strengthen the protection. The AI Act prohibitions also apply in all cases regardless of whether the algorithmic system is relevant to the functionality of the service for VLOPs/VLOSEs, in cases the platform or the search engine is not qualified as a 'very large' and even in cases when the AI system is provided through other means than an intermediary service which ensure equal level of protection for all persons affected and a level playing field for all types of intermediary service providers and more generally all providers and deployers of AI systems, regardless of whether they qualify or not as an intermediary service provider. The AI Act's prohibitions provide a stronger mandate to the enforcement authority to intervene, impose sanctions and request mitigations. Additionally, they are also designed to offer third party protection through liability claims. Nevertheless, where AI systems are used by online platforms, online platforms may face some parallel obligations under the DSA, AI Act and other applicable EU legislation (e.g. data protection, product safety, consumer protection etc.), which becomes particularly relevant in the enforcement.

When examining the prohibitions under Article 5 AI Act, due to its nature, they complement the DSA's obligations for online platforms and search engines.

The previous situation reflects how the protective net of both legislations addresses some practices as harmful and needed for special protection. Whilst the prohibited practices under the AI Act apply also in the earlier phases of the product supervision chain (placing on the market), the DSA becomes relevant at the stage of the use and in relation to the consequences that may arise from such use. This distinction is particularly significant for enforcement, as it may lead to overlaps between different levels of authority (national and EU), as the final section will further address.

- **High-risk AI systems**

As mentioned, the AI Act identifies high-risk AI systems as those either embedded as safety components into products or constituting such products regulated under Union law set out in Annex I AI Act and subject to third party conformity assessment or those explicitly listed in Annex III, due to their potential to significantly impact the health, safety, or fundamental rights of individuals. Examples include biometric categorisation and emotion recognition, systems for the recruitment of natural persons, systems affecting access to and enjoyment of essential private services and essential public services and benefits. These systems are subject to strict risk management, data quality and governance, human oversight, transparency, documentation, accuracy, robustness and cybersecurity requirements under the AIA. Both providers, who are placing those high-risk AI systems on the market or putting them into service, as well as deployers, using these high-risk AI systems under their authority, have specific obligations under the AI Act that are very distinct in nature and scope from the obligations in the DSA. In particular, providers need to ensure conf

rmity assessment of the AI system, have in place a quality management system, including post-market monitoring and serious incident reporting and register high-risk AI systems listed in Annex III in a public database.

Online platforms may use high-risk AI systems as part of their services. That would be the case, for instance, where a VLOP intermediating jobs' demand and offer sides uses an AI system to target and recommend particular job offers or job seekers. While the AI Act sets requirements for the design, risk management, and transparency of the system itself, which the providers of the system has to ensure compliance with prior to its placement on the market/ putting into service and throughout the system lifecycle, certain obligations extend to deployers. Relevant obligations for deployers are the use of the high-risk AI system according to its instructions, human oversight and, monitoring and in certain cases for Annex III systems, information obligations towards affected persons. Under the DSA, such VLOP should assess and mitigate relevant risks negatively affecting the fundamental right to non-discrimination. Since deployers of high-risk AI system do not have obligations of similar nature, the overlap appears relatively limited.

In any case, the AI Act's requirements for risk management and the specific and detailed requirements for human oversight, documentation, accuracy, robustness and safety and transparency of the systems are more specific and distinct in scope and nature compared to the generic obligations for risk assessment and mitigation applicable only to VLOPs/VLOSEs.

Under the AI Act, AI systems that classify as high-risk must be developed and designed to meet the requirements set out in Chapter III Section 2, in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. Providers of high-risk AI systems must ensure that their high-risk AI system is compliant with these requirements,[154] and must themselves comply with a number of obligations set out in Chapter III Section 3, notably the obligation to ensure that the high-risk AI system undergoes a conformity assessment prior to its being placed on the market or put into service, ergo prior to its being embedded into the services of an online platform within the meaning of the DSA. Once embedded into the services of an online platform, the provider of that platform is considered a deployer of a high-risk AI system and subject to the obligations set out in Article 26. In addition, the DSA's transparency and due diligence obligations apply and, where that online platform is a VLOP, the risk management obligations according to Article 34 and 35 that remain more generic compared to the specific risk management obligations in Article 9 AI Act that include a detailed risk assessment and methodology and testing process.

According to Article 9(10) AI Act, VLOPs and VLOSEs may integrate this more specific and detailed risk management framework specifically for the high-risk AI system into their general risk assessment for the intermediary services under Articles 34 and 35 DSA. Such integration remains however only an option. Both obligations and legal frameworks remain applicable and need to be supervised in parallel. For the risk management framework under Article 9 AI Act, European harmonised standards will detail how to operationalise the requirement and provide a presumption of conformity.

- **General transparency obligations on AI systems**

Both the AI Act and the DSA establish transparency obligations but they have different content and apply to different systems.

Under the AI Act, transparency obligations (Article 50) apply to AI systems that interact with natural persons, generate or manipulate content, or process biometric or emotion data. Providers of AI system directly interacting with persons (e.g. chatbots) must develop it in such a way that the user is informed when interacting with an AI system unless this is obvious. Providers of generative AI systems must ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated (e.g. through watermarks). Article 50 AI Act also contains disclosure obligations for deployers. Notably, deployers of AI systems must disclose "deep fakes") and for certain type of AI generated text publications on matters of public interest. Deployers must also inform people when they are using emotion recognition and biometric categorisation systems.

As mentioned, the DSA also imposes transparency obligations on online platforms, although these are different in nature. For example, Article 27 DSA specifically addresses transparency of recommender systems, including explanation of the main ranking parameters. Moreover, Article 35(1)(k) DSA, for instance, puts forward as a possible risk mitigation measure for VLOPs/VLOSEs to ensure that AI-generated or manipulated images, audio, or video that may be mistaken for authentic or truthful content are properly distinguished and recognised when disseminated through the VLOP/VLOSE's services, and provide functionality enabling users to indicate such information.

When examining the set of transparency requirements under Article 50 AI Act, the AI Act rules complement the DSA's transparency obligations for online platforms and search engines.

If providers of VLOP/VLOSE choose to implement such risk mitigation measure under Article 35(1)(k) DSA, it can be expected that the AI Act's obligation to include machine-readable marks in AI-generated content will facilitate the detection of unlabelled AI-generated content and ensure the effective implementation of the DSA's

[154] Point (a) of Art 16 AI Act.

rules, as set out in recital 120 AI Act. These obligations are thus fully complementary and aim to reinforce online platforms' capacities to fight against misinformation and detect AI-generated content and ensure its transparency further in the dissemination value chain.

- **GPAI models without systemic risks**

GPAI models that do not pose systemic risks are subject to specific obligations under Article 53 AI Act. Providers must maintain up-to-date technical documentation, make information available to downstream AI system providers, comply with copyright legislation, and publish a summary of the data used for training. In this context, it is important to clarify that GPAI models are often components of AI systems and the integration into an intermediary service likely takes place as an AI system.

When it comes to the DSA, the transparency, risk management, and content moderation requirements under Articles 25 to 28, 34 and 35, 38 and 39 DSA can also apply to a GPAI model that is integrated into an intermediary service. GPAI models may be embedded into or constitute online platforms and VLOPs/VLOSEs, thereby bringing them under the scope of the DSA insofar as the previous due diligence and risk management obligations are concerned if they constitute 'related systems' (Article 34(1) DSA).

The obligations under Article 53 AI Act and of the above-mentioned DSA provisions differ in substance. The obligations under Article 53 AI Act primarily aim at value chain transparency, whereas the cited DSA provisions address transparency, risk management and content moderation at the level of deployment of the GPAI model where such GPAI model is a component of an AI system that is embedded in or constitutes an online platform.

The AI Act's rules for GPAI models without systemic risk and the applicable rules of the DSA are distinct from each other. Although Article 53 AI Act can be applied without friction on a substance level, this does not pre-empt those online intermediary services providers from having to fulfil the above-mentioned DSA provisions.

Therefore, limited practical impact and implication are expected.

- **GPAI models with systemic risks**

The AI Act subjects GPAI models that pose systemic risks to stricter obligations. As mentioned above, in addition to the requirements of Article 53, Article 55 AI Act requires providers to perform model evaluations using standardised, state-of-the-art protocols, including adversarial testing to identify and mitigate systemic risks; assess and mitigate potential Union-level systemic risks arising from development, deployment, or use; report serious incidents and corrective measures to the AI Office and relevant national authorities without undue delay; and ensure an adequate level of cybersecurity for the model and its infrastructure. Article 51 specifies that a GPAI model is classified as a GPAI model with systemic risk if it has high-impact capabilities, and/or is designated as such by the Commission in line with the criteria outlined in Annex XIII AI Act.

The AI Act defines a 'systemic risk' as 'a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain' (Article 3(65) AI Act). The GPAI Code of Practice's risk identification process requires providers to compile a list of risks that could stem from their models and be systemic, in particular risks to fundamental rights and society, public health and public security such as of major accidents; risks to critical sectors or infrastructure, public mental health, freedom of expression and information, non-discrimination, privacy and the protection of personal data, the environment, non-human welfare, economic security, and democratic processes; and risks from concentration of power and illegal, violent, hateful, radicalising, or false content, including risks from child sexual abuse material (CSAM) and non-consensual intimate images (NCII)[155]. The GPAI Code of Practice moreover includes detailed measures that specify how providers can technically and organisationally implement risk mitigation measures.

The DSA's risk management requirements for VLOPs/VLOSEs (Articles 34 and 35) require these providers to identify, assess, and mitigate systemic risks related to the dissemination of illegal content, manipulation, and

[155] See Appendix 1.1 of the Safety and Security Chapter of the GPAI Code of Practice.

other societal harms, which can include integrated GPAI models with systemic risk if they are 'related systems' in the sense of Article 34(1) DSA. These risks have a societal impact, including the dissemination of illegal content and negative effects on fundamental rights, civic discourse and electoral processes, public security, gender-based violence, the protection of public health and minors and a person's physical and mental well-being (Article 34(1)).

Where a GPAI model is embedded into a VLOP/VLOSE and constitutes a 'related system' within the meaning of Article 34(1) DSA, an assessment and mitigation of systemic risks has to be performed both within the AI Act's framework under Article 55(1)(b) and Articles 34 and 35 DSA. However, these risk management obligations are distinct in several ways. The AI Act frames systemic risks primarily around model capabilities, while the DSA attributes systemic risks to the platform or search engine level, arising from its reach. The AI Act also applies earlier in the lifecycle, including at the development stage where integration into a VLOP/VLOSE may not yet be foreseen. The same GPAI model that is embedded into a VLOP/VLOSE may be also offered via application programming interfaces (API) or directly to downstream developers, in which case only the AI Act's risk management framework applies to the supply of the model outside the VLOP/VLOSE.

The interplay between the two risk management frameworks is particularly relevant where GPAI models with systemic risk under the AI Act are embedded in or fully constituting a VLOP or VLOSE. Recital 118 AI Act states, when referring to the interaction between the systemic risk assessments of GPAI models with systemic risk and VLOPs/VLOSEs, compliance with the AI Act's systemic risk assessment and mitigation (Article 55(1), point (b), AI Act) should be presumed to be fulfilled when performing risk assessment under Article 34 DSA, unless other significant systemic risks appeared.

Recital 118 AI Act highlights the clear intention of the EU legislature to avoid a duplication in risk management, to the extent such duplication exists. However, its practical implementation is challenging for multiple reasons, notably the fact that the AI Act applies earlier in the lifecycle, and it addresses potentially different systemic risks. The recital therefore does not provide a sufficiently operational solution to achieve its aim, namely the smooth interplay between both risk management frameworks.

- **Enforcement**

All the intersections mentioned above interact with the above described two-tiered enforcement regime under both legislations (MSAs, notifying authorities and the European Commission (AI Office) for the AIA; Digital Services Coordinators and the European Commission for the DSA).

For example, if an AI system is qualified as high-risk under the AI Act because it incorporates an automated online AI recruitment system for candidate filtering, screening and ranking, the provider and the deployer would be subject to the supervision of the correspondent MSA (national level, country-of-destination logic). However, if the same AI system qualified as high-risk is embedded into an online platform, it would also be subject to the relevant diligence obligations under the DSA, particularly the ones on recommender systems' transparency (Art 27), with the DSC where the platform is established as sole competent authority (country-of-origin logic). In addition, if the online platform is designated as VLOP, the European Commission will be the competent authority, thereby confronting an AI Act national enforcement authority with a DSA European level authority.

Moreover, as regards GPAI models with systemic risk, if a VLOP or VLOSE is using that model in its content moderation systems and/or generation of content, the European Commission would need to monitor under the DSA whether the content moderation systems based on the referred model is the basis of a "related system" and therefore covered under VLOP's designation. In parallel, the AI Office would supervise compliance with the obligations applicable to providers of GPAI models with systemic risk, creating potential intersections with regards to the time when the two supervisors may act, and with regards to certain risks.

## Regulation (EU) 2024/2865 ([156]) – [Classification, labelling and packaging of substances Regulation]

*General Information*

The amendments to the provisions of the Classification, labelling and packaging of substances Regulation (CLP) will become fully applicable on 1 January 2027. Some provisions of the Regulation will have to be evaluated by 11 December 2029.

Based on Article 114 TFEU, the CLP will govern the classification, labelling, and packaging of substances and mixtures. The amending regulation will seek to address, in particular, the fact that the supply chain of the regulated products is no longer entirely located in the Union. It will thus aim to enhance safety and environmental protection by introducing rules for online sales, refill stations, and digital labelling. It will also clarify assessment methods for complex substances and mixtures, will streamline the harmonisation of hazard classifications and improve the transparency of information available to authorities and the public. The Regulation lays down transitional periods to allow suppliers to adapt to these new requirements.

*Personal scope*

The amended Regulation will apply to multiple categories of economic operators. Economic operators are not defined by the Regulation, but this is a common term used in EU product law. CLP refers to economic operators as "suppliers". The definition of supplier includes any manufacturer, importer, downstream user or distributor that places chemical substances or mixtures on the market. The CLP does not entail obligations for online platforms.

*Territorial scope*

The CLP regulates the classification, labelling and packaging of substances and mixtures made available on the Union market.

*Material scope*

The CLP requires that chemical substances and mixtures placed on the EU market are properly classified according to their hazards and clearly labelled with standardised warnings, symbols, and safety information. It seeks to ensure that users, including consumers and workers, are informed about potential chemical risks through harmonised pictograms, hazard and precautionary statements. The regulation will also set rules for the packaging of hazardous chemicals to ensure safety and prevent misuse.

*Enforcement*

The Regulation will rely on the Market Surveillance Regulation. Article 46 CLP lays down general enforcement measures.

*Interactions with the DSA*

The Regulation 2024/2865, amending CLP makes reference to the DSA. In recital 1 the amending regulation states that the requirement for there to be a supplier established in the Union, together with the requirements in Regulations (EU) 2019/1020, (EU) 2022/2065 and (EU) 2023/988 of the European Parliament and of the Council, would improve compliance with and enforcement of Regulation (EC) No 1272/2008 and thereby ensure a high level of protection of human health and the environment.

[156] Regulation (EU) 2024/2865 of the European Parliament and of the Council of 23 October 2024 amending Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures, OJ L, 2024/2865.

Recital 37 states the following: “to keep pace with technological developments and new means of sale, it is necessary to require that the label elements be indicated in the event of distance sales, including via online marketplaces. The compliance by design obligations laid down for providers of online marketplaces in Article 31 of Regulation (EU) 2022/2065 of the European Parliament and of the Council will therefore apply to the display of these label elements. The enforcement of such obligations is subject to the rules laid down in Chapter IV of Regulation (EU) 2022/2065”.

The DSA does not make references to the CLP.

On **personal scope**, the DSA regulates intermediary services, while the **territorial scope** shows that the CLP will regulate the classification, labelling and packaging of substances and mixtures made available on the Union market. On the other hand, the DSA applies if the service is offered to recipients that have their place of establishment or are located in the European Union.

Referring to the **material scope**, there is interplay between the DSA and the CLP regarding compliance by design and labelling requirements, as the DSA complements the CLP by adding obligations to online marketplaces but does not contradict it or alter its functioning. And on **enforcement**, the DSA will complement the enforcement of the CLP provisions by enforcing the requirement for online marketplaces to allow traders to provide CLP’s labelling elements in the event of distance sales.

*Special remarks on interplay*

The direct link between the CLP and the DSA concerns the issue of compliance by design. Article 31 DSA requires the providers of online platforms to integrate compliance with the DSA’s requirements directly into the design and functioning of their systems, interfaces, and algorithms. The CLP will require that labelling elements be indicated in the context of distance sales, including on online marketplaces. Chapter IV of the DSA facilitates the implementation of this requirement and reinforces the obligations for online marketplaces in this regard.

Thus, the DSA complements the CLP. This Regulation shows how to successfully link a product-specific instrument with the general protection of consumers by online intermediaries.

# Directive (EU) 2024/2853 ([157]) – [Product Liability Directive]

*General Information*

The Product Liability Directive (PLD) was adopted on 23 October 2024 and must be transposed by Member States until 9 December 2026. It repeals the existing Product Liability Directive (Directive 85/374/EEC) with effect from that day. The PLD harmonises the liability of economic operators for damage suffered by natural persons and caused by defective products as well as on compensation for such damages. It replaces Directive 85/374/EEC to address modern technological advancements, particularly artificial intelligence (AI) and new business models like the circular economy.

*Personal scope*

The Directive primarily establishes common rules for the liability of economic operators for damage suffered by natural persons by products which have been placed on the internal market. The scope of the PLD therefore covers any natural person who suffers damage from a defective product and any manufacturer of the defective product. In the absence of an EU-based manufacturer, their importers, authorised representatives and fulfilment service providers (when no importer or authorised representative is in the Union) can be held liable. Distributors can also be liable if upon request of an injured person they fail to promptly identify a responsible economic operator established in the Union.

Furthermore, if an online platform that allows users to conclude distance contracts acts as a mere intermediary, it would be outside the scope of this Directive. However, if it presents a product in a way that would lead an average consumer to believe that the product is provided either by the online platform itself or on its behalf, the provisions relating to distributors apply analogously – in line with Article 6(3) DSA.

*Territorial scope*

The Directive applies to products placed on the internal market (put into service after 26 December 2026).

*Material scope*

The Directive establishes a no-fault based liability to a wide range of actors and product types. It maintains the core principle of strict liability for defective products but clarifies the definition of "product" to include software and digital elements. It also introduces clearer rules on the liability of online platforms, fulfilment service providers, and operators involved in AI or complex supply chains compared to its previous version. Manufacturers remain the primarily liable party, but the Directive ensures that victims can claim compensation against an economic operator involved in the supply chain of the defective product, where the manufacturer is not established in the EU

*Enforcement*

The Directive envisages an enforcement regime of civil liability before national courts.

*Interactions with the DSA*

The DSA is mentioned in the preamble of the Directive (Recital 38) and is referred to for the definition of online platform under Article 4(16) PLD. Article 8(4) PLD refers to the liability exemption for hosting services set out in Article 6(3) DSA.

[157] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, OJ L, 2024/2853.

There are no references to the PLD (or its repealed versions) in the DSA. However, Article 2(4)(f) generally sets out that the DSA is without prejudice to Union law on product safety which regulates other aspects of the provision of intermediary services or specifies and complements the DSA.

On **personal scope**, the relevant provision in Article 8(4) PLD applies to online platforms that allow consumers to conclude distance contracts with traders and that are not economic operators. This term aligns with the same term used in Section 4, Chapter III, of the DSA and Article 4 PLD defines "online platform" by reference to Article 3(i) DSA.

With regards to **material scope**, when online platforms act as manufacturers, importers, or distributors, they are fully liable for damages caused by a defective product or component like any economic operator. However, if they only act as intermediaries, they benefit from a conditional liability exemption under the DSA. According to Article 6(3) DSA, this exemption does not apply in respect of liability under consumer protection law when a platform presents a specific item or enables a transaction in a way that leads the average consumer to believe the platform itself is the seller. Article 8(4) PLD sets out that in such cases, the online platform can be held liable as a distributor under the Directive, if it cannot identify a responsible EU-based economic operator upon request. Recital 38 of the PLD clarifies this alignment with the DSA's consumer protection liability rules. Nevertheless, the PLD's liability regime is independent from the DSA and does not duplicate it.

*Special remarks on interplay*

The DSA and PLD apply in complementary manner.

# Regulation (EU) 2024/3110 ([158]) – [Construction Products Regulation]

*General Information*

The revised CPR was adopted on 27th November 2024 and its key provisions will apply as from 8 January 2026. The CPR harmonises the conditions for the placing and making available on the market of construction products, setting out requirements for their functionality, safety, and environmental sustainability throughout their lifecycle. The regulation focuses on ensuring free movement of construction products within the internal market, defining responsibilities for economic operators, and establishing procedures for assessment, verification, and market surveillance of construction products. The Commission will carry out an evaluation of the CPR no later than 9 January 2033.

Based on Article 114 TFEU, the primary objective of the CPR is to contribute to the proper functioning of the internal market by ensuring the free movement of safe and sustainable construction products in the Union. It also aims to contribute to the objectives of a green and digital transition, by preventing and reducing the impact that construction products have on the environment and on the health and safety of persons.

*Personal scope*

The CPR covers several categories: economic operators (Article 20 CPR) including manufacturers (Articles 21 and 22 CPR), importers (Article 24 CPR), distributors (Article 25 CPR), authorised representatives (Article 23 CPR) and fulfilment services providers (Article 27 CPR). It also specifically addresses one category of online intermediaries, namely online marketplaces (Article 28 CPR). Article 3(47) CPR defines online marketplace as "a provider of an intermediary service using an online interface which enables customers to conclude distance contracts with economic operators for the sale of products".

*Territorial scope*

The CPR applies to construction products placed on the internal market.

*Material scope*

The main provision concerning the DSA within the CPR is Article 28 CPR, which imposes a series of obligations on online marketplaces. In essence, online marketplaces are obliged to design and organise their online interfaces in such a way as to enable economic operators to fulfil their obligations under the CPR.

Online marketplaces must establish a single contact point for direct communication with Member States' competent national authorities regarding compliance. Online marketplaces are also required to respond appropriately to notices concerning accidents and other incidents involving products and to cooperate to ensure effective market surveillance measures, refraining from creating obstacles to such measures.

They must also inform competent national authorities of any action taken regarding non-compliance or suspected non-compliance of products covered by the Regulation and establish a regular and structured exchange of information on removed content at the request of authorities. Member States' market surveillance authorities are empowered to order online marketplaces to remove specific illegal content relating to non-compliant products, to disable access to it, or to display explicit warnings to end users. Online marketplaces must implement the necessary measures to receive and process such orders. Pursuant to Article 28(4) CPR, these requirements also extend to manufacturers, importers, or distributors who offer products online without the involvement of an online marketplace.

[158] Regulation (EU) 2024/3110 of the European Parliament and of the Council of 27 November 2024 laying down harmonised rules for the marketing of construction products and repealing Regulation (EU) No 305/2011, OJ L 2024/3110.

*Enforcement*

The CPR employs several mechanisms to ensure its effective enforcement by market surveillance authorities (MSAs). Member States are required to designate one or more market surveillance authorities that dispose of the particular knowledge to assess construction products technically and legally.

When an MSA has reason to believe that a product or its manufacturer is non-compliant with the requirements and obligations under the CPR, it requires the economic operator to take appropriate corrective actions, or to withdraw or recall the products. If the non-compliance extends beyond national borders, the MSA must inform the European Commission and other Member States. MSAs also possess the authority to address products that, despite being compliant, still pose a risk to health, safety, or the environment, compelling economic operators to mitigate these risks or remove the products from the market. Member States can also impose penalties against economic operators for non-compliance.

The enforcement of the CPR also relies on other mechanisms, such as the Member States' single liaison points, the Union Safeguard Procedure, complaint portals and information exchange systems.

*Interactions with the DSA*

The CPR refers to the DSA in the text of Article 28. The DSA does not quote the CPR.

The CPR defines the rights and obligations for economic operators dealing with construction products or their components and sets out obligations for other actors providing services linked to the manufacturing and commercialisation of products covered by the Regulation. In addition, it also sets out certain due diligence obligations for providers of online platforms which are online marketplaces. While this definition does not exist per se under the DSA, the definition used by the CPR entails that Chapter III Section 4 of the DSA is applicable to these online marketplaces to ensure the safety and functionality of construction products. To that extent, Article 28 CPR repeatedly refers to the DSA but it does not explicitly specify if it must be considered its *lex specialis*. Under Article 12 CPR, on the relationship with Union law, the Regulation establishes that its provisions prevail in cases of conflict with Regulation (EU) 2024/1781 (Ecodesign for Sustainable Products) and Regulation (EU) No 1025/2012 (European standardisation). That provision is however silent on the DSA.

On **personal scope**, the CPR refers to both "intermediary services for the placing on the market of products" (Article 29(3) CPR) and "online marketplaces" (Article 28 CPR) while providing a definition only for the latter in Article 3 (47) CPR, but not for "intermediary services" within the meaning of Article 29(3). The CPR is thus concerned with a subset of the addressees of the DSA. While the definitions of the respective personal scope of the two instruments do not rely on the same concepts, it is nevertheless clear that online marketplaces covered by the CPR are included in the scope of the DSA. Therefore, the personal scopes of the DSA and the CPR coincide partially.

With regards to the **territorial scope**, per its Article 2(1), the DSA applies to "intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment." Both the DSA and the CPR may therefore also apply irrespective of where the provider is located.

Referring to the **material scope**, both instruments regulate providers of online marketplaces and impose similar obligations. But the specific reference to the DSA in Article 28 CPR shows that both instruments are complementary: the CPR does not replace the DSA when construction products are concerned, but rather clarifies and, to some extent, specifies the application of several provisions of the DSA. In this regard:

- Article 28(1)(a) CPR determines first that the interface of an online marketplace must be designed in such a way that allows economic operators to fulfil their obligations in the context of the CPR. Manufacturers (for instance) must make visible the CE marking or the information relating to the digital product passport of their goods. This obligation repeats, specifically related to construction products, the compliance by

design obligations stemming from Article 31(1) DSA. Article 28(1)(a) CPR does not impose a different obligation, as it specifies that it is "for the purpose of complying with Article 31 DSA".

- Article 28(1)(b) CPR requires online platforms to set up a contact point for communication with the authorities similar to Article 11(1) DSA. The text does not specify whether the same contact point can serve for the purposes of both regulations, though both provisions may apply in parallel.

- Article 28(1)(c) CPR requires online marketplaces to give an appropriate answer to notices related to the notification of accidents and other incidents involving products received in accordance with Article 16 DSA. The notice and action mechanism under the DSA is limited to the notification of illegal content, that includes any information that, in itself or in relation to an activity that is in breach of Union or national law. Therefore, the obligation applies to such accidents and incidents which constitute evidence that the products concerned relate to an illegal activity.

- Article 28(1)(d) CPR requires online marketplaces to cooperate with national authorities for the purpose of market surveillance. These aspects are not envisaged in the DSA and are thus complementary. Moreover, online marketplaces must also inform the competent national authorities of any action taken with regard to the non-compliance or suspected non-compliance of products covered by the CPR (Article 28(1)(e) CPR); and must establish a regular and structured exchange of information regarding content that has been removed by online marketplaces at the request of competent national authorities (Article 28(1)(f) CPR).

- Article 28(2) CPR empowers national authorities to order online marketplaces to remove illegal content relating to a non-compliant product from their interface. Online marketplaces must comply with these orders (Article 28(3) CPR). These orders to act against illegal content must also comply with Article 9 DSA, which determines their formal and substantive conditions of validity.

On **enforcement**, the CPR, with its focus on market surveillance mechanisms, complements the DSA in matters of enforcement of requirements. In general, it imposes duties that the DSA does not specify.

*Special remarks on interplay*

Consequently, the CPR here complements, by "plugging-in" to the content of the DSA.

In addition to the provisions targeting online marketplaces, Article 29(3) CPR states that providers of "intermediary services for the placing on the market of products" must fulfil the obligations regarding the display of certain product-related information, especially related to the visibility of the CE marking and the digital product passport when a product is offered for distance sales.

The CPR, with its focus on market surveillance mechanisms, complements the DSA in matters of enforcement of requirements. In general, it imposes duties that the DSA does not specify.

## Regulation (EU) 2025/40 ([159]) – [Packaging and Packaging Waste Regulation]

*General Information*

The Packaging and Packaging Waste Regulation (PPWR) was adopted on 19 December 2024 and will become applicable on 12 August 2026. It will have to be evaluated by 12 August 2034.

Based on Article 114 TFEU, the PPWR aims to minimise packaging waste and promote a circular economy by establishing comprehensive rules across the entire packaging lifecycle. It will introduce measures such as mandatory recycled content targets for plastic packaging and restrictions on certain single-use formats, alongside requirements for re-use and refill systems. The regulation also mandates harmonised labelling for easier sorting and outlines extended producer responsibility obligations, ensuring manufacturers contribute to waste management. Furthermore, it details monitoring, reporting, and enforcement mechanisms to ensure compliance and effective environmental protection.

*Personal scope*

The requirements of the PPWR apply to a wide variety of "economic operators" which according to Article 3(1)(12) include the manufacturer, supplier, importer, distributor, authorised representative and final distributor of packaging and packaged products, as well as the fulfilment service provider. The PPWR also applies to online platforms directly referencing the definition of "online platforms" in Article 3 (i) DSA.

*Territorial scope*

The PPWR applies to all packaging placed on the EU market, and packaging waste, regardless of where it is manufactured, including packaging used in products sold through distance or online sales to EU consumers (See Recital 10 PPWR).

*Material scope*

The PPWR requires that all packaging placed on the EU market be sustainable, recyclable, and minimised in volume and weight. It sets design requirements for recyclability, bans certain types of unnecessary packaging, and introduces targets for reusable packaging and recycled content. The Regulation also mandates clear labelling to improve consumer sorting and a digital product passport for packaging. Producers must take responsibility for the full life cycle of their packaging through extended producer responsibility (EPR) schemes, while online sellers and importers are also subject to these obligations when targeting EU consumers.

With regards to online platforms that allow consumers to conclude distance contracts with manufacturers, importers and distributors of packaging and packaged products ("producers"), Article 45(4) PPWR sets out an obligation for the provider to obtain information from producers about their compliance with the 'extended producer responsibility' (EPR) obligations set out in the PPWR, including information on the registration in the register of producers stipulated by Article 44 PPWR and its registration number, as well as a self-certification confirming compliance with the EPR, to the extent that it can be interpreted as applying only to producers who sell directly through those platforms. Furthermore, Recital 135 clarifies that where a producer sells its products via an online marketplace, the PPWR furthermore opens up the possibility that the EPR obligations are met directly by the provider of the online platform on behalf of the producer based on a written mandate. While the term "online marketplace" is not defined in the PPWR, it follows from the first sentence of Article 45(4) PPWR, that this refers to online platforms which fall within the scope of Section 4 of Chapter III of the DSA.

[159] Regulation (EU) 2025/40 of the European Parliament and of the Council of 19 December 2024 on packaging and packaging waste, amending Regulation (EU) 2019/1020 and Directive (EU) 2019/904, and repealing Directive 94/62/EC, OJ L, 2025/40.

*Enforcement*

The supervision and enforcement of the PPWR is the responsibility of the market surveillance authorities in the Member States. Whereas the PPWR sets out enforcement powers in Article 58, it relies on the Market Surveillance Regulation (MSR) with regards to sustainability requirements that are set pursuant to this Regulation (Recital 168). However, the enforcement of the obligations that apply to online marketplaces rely on the enforcement mechanism set out in the DSA (recital 132 PPWR).

*Interactions with the DSA*

There are various references to the DSA in the preamble and Article 45 PPWR. These references cover traceability of traders' obligations (Article 45, Recital 132), the register of producers (Recital 134), the definition of online platform as per the DSA (Article 3) and extended producer responsibility (Article 45). There are no references to the PPWR in the DSA.

On **personal scope**, the PPWR applies to online platforms that fall within the scope of Section 4 of Chapter III of the DSA, that allow consumers to conclude distance contracts with producers offering packaging or packaged products to consumers in the Union.

Regarding the **territorial scope**, the PPWR applies to all packaging and packaged products placed on the EU market, regardless of where they are manufactured and where the producer, fulfilment service provider or online platform is established. The DSA regulates services that are offered to recipients in the EU, regardless of the place of establishment of the service provider.

With regards to **material scope**, the PPWR relies on the DSA to define the concept of an online platform in Article 3(70) PPWR. It complements the DSA by further specifying the traceability of traders' obligations under Article 30(2) and (3) DSA for providers of online platforms that allow consumers to conclude distance contracts with producers offering packaging and packaged products to consumers in the Union in Article 45(4). According to Recital 132, any producer that offers packaging by means of distance contracts directly to consumers located in a Member State should be considered to fall within the definition of a trader under the DSA. Prior to the use of their services, providers of online platforms therefore must obtain from producers the information set out in Article 30(1) DSA, which the PPWR specifies to include also information on the registration in the register of producers under Article 44 PPWR and a self-certification confirming compliance with EPR obligations.

On **enforcement**, as per Recital 132, the rules on traceability of traders selling packaging and packaged products online are subject to the enforcement rules set out in the DSA.

*Special remarks on interplay*

The PPWR covers online marketplaces for the same purposes as the DSA. However, it can be considered that it complements the DSA by further specifying the obligation of the provider of an online platform to obtain public register and self-certification information from a trader under Article 30 DSA. The PPWR also uses the DSA's terminology to define online platforms. There are no overlaps or conflicting provisions in the two instruments. However, it is important to note that Article 45 PPWR can only apply where the producer sells directly through the online platform – if a distributor mediated such sale, the online marketplace would only be obliged to receive the information –and make best efforts to check it- from the distributor, but not from the producer, who would not be in that case a "business customer" of the platform, but of the distributor.

# Council Directive (EU) 2025/516 of 11 March 2025([160]) – [ViDA Directive], Council Regulation (EU) 2025/517([161]) – [ViDA Regulation] and Council Implementing Regulation (EU) 2025/518 of 11 March 2025 amending Implementing Regulation (EU) No 282/2011 as regards information requirements for certain VAT schemes([162]) – [ViDA Implementating Regulation]

*General Information*

The VAT in the Digital Age (ViDA) package has been adopted on 11 March 2025 and will be rolled out progressively until January 2035 as per Article 6 of the ViDA Directive. Article 5(19) defines that the Commission has to present an interim evaluation report on the functioning of the electronic invoicing, as well as on the functioning of the intra-Community and domestic digital reporting requirements by 31 March 2033. Additionally, by 1 July 2033 the Commission also must evaluate the application of the VAT rules on facilitation services, including the impact on the functioning of the internal market and the effectiveness of VAT collection as per Art. 3(1) of ViDA Directive.

The ViDA package aims to modernise and simplify the EU's Value Added Tax systems by creating a more efficient and digital system for VAT obligations, while reducing administrative burdens, and helping to combat VAT fraud through fast, automatic and digital exchange of information between companies and tax authorities and between tax authorities on cross-border B2B transactions.

*Personal scope*

Regarding the personal scope, the ViDA package does not change the personal scope of the 2006 VAT Directive[163] which applies to taxable persons (natural or legal), as well as to non-taxable legal persons in certain cases as defined by Articles 2-4.

*Territorial scope*

The ViDA package does not introduce a substantial change in the territorial scope of the 2006 VAT Directive. According to Art. 2, the legislation applies within the EU with the exceptions listed in Article 6[164] Additionally, Section (Articles 369(l)-369(x)) of the 2006 VAT Directive also provides for a special scheme for distance sales of goods imported from third territories or third countries. Recital 37 of ViDA Directive mentions that the 2006 VAT Directive is amended to clarify that all the non-resident taxable person's business-to-consumer supplies of services within the EU fall under the non-Union one-stop shop ('OSS') scheme ('the non-Union OSS'), and not only supplies of services to Union established customers.

*Material scope*

---

[160] Council Directive (EU) 2025/516 of 11 March 2025 amending Directive 2006/112/EC as regards VAT rules for the digital age.

[161] Council Regulation (EU) 2025/517 of 11 March 2025 amending Regulation (EU) No 904/2010 as regards the VAT administrative cooperation arrangements needed for the digital age.

[162] Council Implementing Regulation (EU) 2025/518 of 11 March 2025 amending Implementing Regulation (EU) No 282/2011 as regards information requirements for certain VAT schemes.

[163] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

[164] These are: Mount Athos, the Canary Islands, the French overseas departments, the Åland Islands, the Channel Islands, the Island of Heligoland, the territory of Büsingen, Ceuta, Melilla, Livigno, Campione d'Italia and the Italian waters of Lake Lugano.

The 2006 VAT Directive established the common system of value added tax (Art. 1) with a breakdown which supplies of goods and services (Art. 2) fall under the regime and which are exempted (in Articles 3 and 4). The ViDA package has introduced changes to addresses the challenges of increased online trade and level the playing field between platforms and traditional providers in the short-term accommodation rental and passenger transport sectors. Article 5 of the ViDA Directive introduces mandatory e-invoicing and Digital Reporting Requirements. Moreover, Member States with a domestic digital real-time transaction reporting obligation must also align their systems with the EU standards (Art. 5(20)).

*Enforcement*

The enforcement mechanism of the 2006 EU VAT Directive is characterised by a framework that predominantly entrusts Member States with the responsibility and discretion to implement and enforce the Directive's provisions within their national legal systems. While the Directive contains numerous provisions stipulating that Member States "may" or "shall take measures" to ensure compliance (such as ensuring the submission of VAT returns, preventing evasion, and imposing administrative obligations), there is no explicit, standalone article that unequivocally establishes a general enforcement competence vested in Member States. Rather, enforcement is implicitly grounded in the Directive's design as a legal instrument addressed to Member States, which are required to transpose its provisions and take the necessary administrative and legal steps to secure its effective application. The ViDA package has not amended this.

*Interactions with the DSA*

The 2006 VAT Directive was adopted before the DSA and therefore does not contain any references to it. Neither the text of the ViDA Regulation, nor the text of the ViDA Implementing Regulation mentions the DSA. The ViDA Directive makes one reference to the DSA in the preamble, namely: *Recital 34 - This Directive is without prejudice to the rules laid down in other Union legal acts, in particular Regulation (EU) 2022/2065 of the European Parliament and of the Council, which regulates other aspects of the provision of services by online platforms, such as obligations applicable to providers of online platforms allowing consumers to conclude distance contracts with traders.*

The ViDA package has been adopted after the DSA, therefore the DSA does not make any reference to this legislative package. The DSA also does not mention the 2006 VAT Directive per se but there is one reference to the VAT Information Exchange System in the preamble, in relation to the obligation of Article 30 DSA (Traceability of traders): *Recital 73 - To ensure an efficient and adequate application of that obligation, without imposing any disproportionate burdens, providers of online platforms allowing consumers to conclude distance contracts with traders should make best efforts to assess the reliability of the information provided by the traders concerned, in particular by using freely available official online databases and online interfaces, such as national trade registers and the VAT Information Exchange System, or request the traders concerned to provide trustworthy supporting documents, such as copies of identity documents, certified payment accounts' statements, company certificates and trade register certificates.*

The interplay with **personal scope** depends on the nature of the business the provider is conducting and the role it performs, either acting as economic operator (goods and/or services being subject to VAT) or just as a mere intermediary (where DSA fully applies). Article 56(k) of the 2006 VAT Directive refers to electronically supplied services, such as those referred to in Annex II of the Directive (e.g.: web hosting).

Moreover, the ViDA package has been created to adapt to the digital economy (ViDA Directive recital 1), including addressing the challenges of the platform economy (recital 2). While recitals 25 to 31 do not explicitly mention the DSA, they describe challenges posed by the platform economy to VAT rules, notably changes in competition between online platforms and traditional businesses, and the introduction of the '**deemed supplier**' category to assign VAT collection responsibilities to platforms in sectors such as short-term accommodation rentals and passenger transport by road, while allowing Member States discretion to mitigate administrative burdens and ensuring consistency in the treatment of place of supply and facilitation services.

It is relevant to mention how the "*deemed supplier*" concept was considered reconcilable with the liability exemption established in Directive 2000/31/EC ("the Electronic Commerce Directive"), as tax measures are excluded from the scope of the latter. Furthermore, the consideration of e-commerce online platforms as deemed suppliers is done for the sole purpose of tax collection, and does not contradict nor undermine the exemption of liability for content hosted at the request of the recipients of their service pursuant to Article 6 of DSA, for instance in the context of the sale of illegal or non-compliant products. At the same time, it does not contradict nor impose general monitoring obligations for online intermediary services providers, as stated under Art. 8 DSA.

The DSA and the VAT Directive have the same **territorial scope**: The DSA applies to providers that offer services in the EU, irrespective of their place of establishment (See Article 2(1) DSA). Article 2 of the 2006 VAT Directive specifies that the legislation is applicable to the supply of goods and services within the territory of the EU. The ViDA package does not change this.

There may be indirect interactions in the **material scope** where online platforms (regulated by the DSA) intermediates allowing the sale or distribution of goods and/or supply of services subject to VAT (regulated under ViDA package). In such cases, the platforms would have to comply with both the DSA obligations (e.g., transparency, traceability) and ViDA requirements (e.g., e-invoicing, digital reporting requirements), in the latest for the sole purpose of tax collection. However, these are distinct obligations which do not overlap. This is also confirmed in recital 34 of the ViDA Directive, which notes that the Directive is without prejudice to the rules laid down by the DSA, which regulates other aspects of the provision of services by online platforms.

*Special remarks on interplay*

As the material scope does not overlap, there should be no issue of parallel enforcement.

As described above, even though the personal scope might overlap (e.g.: online intermediary services providers, such as online platforms, that allow online distance sale of goods and/or provision of services), the material scope does not, due to the distinct obligations under DSA and the ViDA package. However, there is complementarity between them as online platforms need to comply with both DSA obligations (e.g., transparency, traceability of traders) and ViDA requirements (e.g., e-invoicing, digital reporting requirements) when acting as mere intermediary services providers and for tax collection only. Similarly, when it comes to enforcement, as the material scope does not conflict, no overlaps are observed.

## Directive (EU) 2025/1982 ([165]) - [Waste Framework Directive]

*General information*

The Waste Framework Directive (WFD) has been recently amended by the Directive (EU) 2025/1892, and Member States will need to transpose into their national laws by 17 June 2027, after the publication in the Official Journal.

Based on Article 192(1) TFEU, the WFD "lays down measures to protect the environment and human health by preventing or reducing the generation of waste, the adverse impacts of the generation and management of waste and by reducing overall impacts of resource use and improving the efficiency of such use, which are crucial for the transition to a circular economy and for guaranteeing the Union's long-term competitiveness." The targeted revision proposed by the Commission in 2023 essentially seeks to reduce food and textile waste. It does so by introducing mechanisms of extended producer responsibility for textiles and setting legally binding food waste reduction targets for Member States.

*Personal scope*

The WFD applies to multiple categories of economic operators. The revision introduces a new definition for 'producer of textile, textile-related and footwear products' that is absent in the current version of the Directive. This definition makes clear that it includes any such producer in its scope "irrespective of the selling technique used". Recital 44 indicates that these producers should be considered as traders for the purposes of Article 30 of the DSA. The revision also introduces a definition of "online platform" which refers to Article 3 DSA.

*Territorial scope*

With regard to the making available of goods on the internal market, the Directive will apply to producers established in the territory of the Member States. In the case of textile, textile-relative and footwear products sold by means of distance communication to end-users on the internal market by producers established in third countries, the Directive will also apply (Article 3(4b)(d)). With regard to the regime of 'Extended Producer Responsibility' (EPR), Member States may require producers established in third countries to designate an authorised representative on their territory for the purpose of fulfilling the EPR obligations (Article 22a(3)).

Material scope

The targeted revision seeks a systemic solution with a lifecycle approach to increase the circularity and valorisation of food waste and the re-use of bio-based textiles, thereby reducing the environmental footprint of these sectors. The central provision of the revision is the mechanism of EPR, which seeks to make producers responsible for the waste their textile, textile-related, and footwear products create.[166] This aims to create an economy for collection, sorting, re-use, preparing for re-use, and recycling (especially fibre-to-fibre recycling), and to incentivise producers to design products according to circularity principles. Producers will finance waste management costs, including for unsold consumer products.

*Enforcement*

In light of its Article 36, Member States shall be responsible on enforcing the WFD provisions. However, the rules on enforcement laid down in Chapter IV of the DSA apply to providers of online platforms allowing consumers to conclude distance contracts with traders, in relation to the established traceability rules.

---

[165] Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ 2008 L 312, p. 3), as amended by the revision here analysed.

[166] We should note that the revised WFD is the lex generalis of the Packaging and Packaging Waste Regulation, which provides for a specific regime of EPR for packaging and the packaging of packaged products. Article 45(4) PPWR will apply cumulatively to the requirements of the revised WFD analysed here.

*Interactions with the DSA*

The Directive makes multiple references to the DSA both in the preamble (Recitals 44 to 47) and in the amended Article 3(4b)(4e) (definitions) and Article 22a(13) (extended producer responsibility scheme for textiles). The DSA does not refer to the WFD.

The WFD interplays with the **personal scope** of the DSA in that it also applies to online platforms as defined in the DSA (Article 3). On **territorial scope**, Article 22a (EPR for textiles) will apply when consumers are located in the Union. Referring to **material scope**, the WFD complements the DSA. Article 30 DSA obliges providers of online platforms that allow consumers to conclude distance contracts with traders to obtain certain identification information and a self-certification from those traders prior to the use of their services. The specifies that, for the purposes of its EPR scheme:

Producers offering textile, textile-related, and footwear products to consumers in the Union are considered "traders" within the meaning of the DSA
The registration in the national textile producer register (established by Art. 22b of the Directive) would be considered appropriate information for the DSA's Article 30(1)(d).
The self-certification would relate with DSA's Article 30(1)(e) and must cover the producer's commitment to comply with the EPR requirements for textile, textile-related, and footwear products as laid down in the revision.

On **enforcement**, Chapter IV of Regulation (EU) 2022/2065 apply to online platforms in relation to these requirements, supporting compliance with the WFD.

*Special remarks on interplay*

Article 22a of the WFD works in a complementary manner with the DSA, as specifies Article 30 of the DSA with regards to the EPR.

# Toy Safety Regulation ([167])

*General Information*

Following the evaluation of Directive 2009/48/EC on the safety of toys identifying a number of weaknesses in its practical application, the European Commission proposed, in July 2023, a Toy Safety Regulation aiming to improve the protection of children from potential risks in toys. A political agreement was reached by the Council and Parliament in April 2025, however the text has not yet been published yet. It will become applicable the first day of the month following 54 months after the date of entry into force of the Regulation.

Based on Article 114 TFEU, the Regulation will lay down essential requirements to ensure the free circulation and, taking due account of the precautionary principle, the safety of toys. More precisely, the regulation will introduce enhanced chemical bans and a digital product passport.

*Personal scope*

The Regulation will impose obligations on a multitude of economic operators in the toy supply chain: manufacturers, importers, distributers and authorised representatives. It will also extend to online marketplaces, which the Regulation defines by reference to the General Product Safety Regulation as "a provider of an intermediary service using an online interface which allows consumers to conclude distance contracts with traders for the sale of products."

*Territorial scope*

The Regulation will apply to all toy products made available on the internal market of the Union.

*Material scope*

The Regulation sets out essential safety requirements to ensure that toys placed on the EU market do not present health or safety risks to users, particularly children. It will address mechanical, physical, chemical, electrical, flammability, hygiene and radioactivity hazards, requiring that toys are designed and manufactured to meet high safety standards throughout their foreseeable use. Compliance will be assessed through conformity procedures, supported by clear warnings, traceability obligations, and the provision of accurate information to consumers and authorities.

With regard to online platforms, the Regulation makes clear that an unsafe toy product constitutes illegal content under the DSA.

*Enforcement*

The Regulation relies on the Market Surveillance Regulation.

*Interactions with the DSA*

The Regulation makes references to the Digital Services Act in recital.48 (The Regulation must be consistent with the horizontal legal framework constituted by the DSA and the GPSR) and Article 14 (Obligations of online marketplaces). The DSA does not refer to the Toy Safety Regulation.

On **personal scope**, the Regulation enacts obligations for online platforms. As such, it has the same personal scope as the GPSR and thus addresses a subcategory of providers of intermediary hosting services. This is consistent with the Regulation being a product requirement legislation. When it comes to **territorial scope**, the Regulation applies once the product is made available on the European market.

---

[167] Proposal for a Regulation of the European Parliament and of the Council on the safety of toys and repealing Directive 2009/48/EC.

With regards to **material scope**, the main point of articulation between the Regulation and the DSA is Article 14.

Article 14(1) makes clear that information relating to an offer for non-compliant toys is deemed illegal content within the meaning of the DSA and is "subject to the measures established therein." The Regulation thus makes the provisions of the DSA on illegal content applicable to the online sale of toys.

Paragraph (2) of the same article clarifies that the obligations of traceability, of compliance by design and of consumer information apply to the online sales of toys. Paragraph (3) obliges the providers of online marketplaces to include a number of specific information on the offer for toys (CE marking, warnings and digital product passport). The Regulation does not oblige these providers to bear the obligations of economic operators. This provision should therefore be said to specify or complement the obligations contained in 31(2)(c) DSA as a sort of "plug in".

Paragraph (4) does not refer to the DSA and makes clear that a non-compliant toy is a dangerous product within the meaning of the GPSR. Finally, paragraph (5) finally empowers the Commission to issue guidelines on the good application of the first and second paragraphs of that provision.

The Regulation may also interact with the DSA in other respects. Articles 7 and 9 of the Regulation oblige manufacturers and importers to inform the providers of online marketplaces of non-compliance of products and of complaints and investigations. This, in turn, should trigger the applicability of the obligation to inform consumers set in Article 32 DSA.

The Toy Safety Regulation must, as a whole, be seen as complementary to the DSA as it specifies obligations for online marketplaces selling toys. Building on the horizontal legal framework provided by the DSA, Article 14 of Toy Safety Regulation requires online marketplaces to fulfil certain compliance by design requirements.

Information referring to an offer of toys placed on the market or made available on the market which are not compliant with the Regulation should be considered to be illegal content within the meaning of the DSA.

*Special remarks on interplay*

The DSA and Toy Safety Regulation apply to the same situations but could be seen as complementary.

# ANNEX 3: OVERARCHING ANALYSIS

| 1. General information | | | | | | 2. Interplay on personal scope (in terms of WHO is regulated/what types of services and sectors | | | | 3. Material scope (in terms of the type of requirements, obligations or rights it includes | | 4. Enforcement (in terms of who enforces what) | | 5. Assessment of overlaps and contradictions | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Legal instrument acronym | Title of EU legal instrument | Adopted before/after the DSA? | References to DSA Regulation (EU) 2022/2065? | References to Art. 12-15 e-commerce Directive? | References to the EU instrument in DSA? | Purpose / objective of EU legal instrument | Description of personal scope of EU legal instrument | Exemptions for Small and Medium-sized Enterprises (SMEs) | Interplay with personal scope DSA | Interplay with personal scope DSA | Description of material scope of EU legal instrument | Interplay with material scope DSA | Description of enforcement of EU instrument | Interplay with enforcement under DSA | Interplay or overlap with DSA? | Additional comments |
| ADR Directive | **Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC** | Before<br><br>2013 | No | No | Yes<br><br>Recitals 10 and 60, as well as Articles 2 (4)(f) and 21(3), expressly stating that the DSA rules on out-of-court dispute settlement are without prejudice to the ADR Directive | The ADR Directive aims to ensure that consumers have access to effective and efficient alternative dispute resolution mechanisms for resolving disputes with traders by harmonising rules on adopting ADR bodies across Member States. It seeks to promote consumer confidence in cross-border shopping by encouraging setting up on national level of a simple, fair, and low-cost way to resolve disputes without going to court. | The ADR Directive applies to disputes between consumers and traders arising from sales or service contracts. It covers both online and offline transactions, ensuring that consumers have access to ADR mechanisms regardless of the sales channel (Recital 16 and Article 2) | No<br><br>The ADR Directive does not provide a general exemption for SMEs. The obligations under the Directive apply to all traders, regardless of their size. | The ADR Directive and the DSA (Article 21) both apply in cases of dispute between consumers/users and traders/intermediaries online. However the ADR Directive has a broader personal scope in that it covers all types of services (incl. non digital and non intermediary), while the DSA is limited to regulating online digital intermediary services and dispute resolution with them through a specific out-of-court settlement body. The review of the ADR Directive (to be published by 2026) provides that where a dispute arises between a provider of an online platform and a recipient of that provider's service which relates to that provider's activities in moderating illegal or harmful content on its platform, Article 21 of DSA applies to that dispute subject to Article 2(4) of the DSA, given that Article 21 of the DSA lays down more detailed rules in relation to such disputes. (Recital 11) | The ADR Directive only applies to traders established in the EU. the DSA has a broader geographical personal scope as it applies to any digital service provider that operates within the EU or has customers/users from the EU, regardless of where the business is based. The review of the ADR Directive expands the geographical scope, hence third country traders may be able to engage in ADR disputes if willing to do so and if more conditions are met. | The ADR Directive material scope is to ensure that individuals have access to efficient ways to resolve disputes without resorting to court. The amendments proposed by the Commission aim to expand the material scope to include non-contractual and pre-contractual disputes. The review of the ADR Directive clarifies that the material scope shall include disputes related to a (pre-contractual and post-contractual stage of the contract, b) constructs for the provision of digital content and digital services, and c) contracts for which the consumer has not paid with money (but e.g. with data). | Similarly to the ADR, the DSA (article 21) also covers out of court dispute resolution. However, the DSA is narrower in scope. It regulates how users of online intermediary services can complain about decisions relating to visibility and suspension taken by the provider of the online platform, on the grounds that the information provided by the recipients constitutes illegal content or is incompatible with its terms and conditions. The ADR has a broader material scope covering contractual obligations stemming from sales contracts or service contracts (Article 2(1)). | Member States are mandated to promote collaboration between ADR entities and between ADR entities (Article 16) and national authorities that enforce EU consumer protection laws (Article 17). National competent authorities shall conduct necessary checks on the functioning and activities of the ADR entities to monitor compliance with the requirements of this Directive and report to the Commission every 4 years. | The Digital Services Coordinator of the Member State where the DSA out-of-court dispute settlement body is established is responsible for certifying that body.<br><br>Even though the European Commission does not play a role in regard to the out of court dispute settlement, is however designing a digital interactive tool to inform consumers and traders on redress mechanisms, which will include a list of these bodies on a dedicated website (Article 21 DSA) and will create a network for the ADR contact points which will assist | Interplay but no overlap<br><br>Complementary provisions | While the DSA and ADR do not have a similar scope, the DSA complements the ADR by establishing an expert body for the settlement of disputes related to online intermediary services providers and on the grounds that the information provided by the recipients constitutes illegal content or is incompatible with its terms and conditions (Article 21), moreover, the DSA (Article 21 (3b) and the ADR (Article 6 (1a)) both provide in a complimentary manner quality criteria for such dispute resolution bodies.<br><br>Depending on how ADR Directive was implemented in a given Member State, it could lead to the establishment of an ADR body specialising in the same area of disputes as the ones that are to be resolved under the DSA, as the ADR did not exclude an option for sector / issue specific ADR bodies (only encouraged Member States to authorise one general consumer ADR body at the very least).<br><br>DSA is without prejudice to the ADR. Similarly, article 3 of the ADR Directive also establishes that if any provision of such Directive conflicts with a provision laid down in another Union legal act and relating to out-of-court redress procedures initiated by a consumer against a trader, the provision of ADR shall prevail. |
| Unfair Contract Terms Directive (UCTD) | **Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts** | Before<br><br>1993 | No | No | Yes<br><br>Recital (10) specifically mentions that DSA should be without prejudice to Union law on consumer protection, in particular to Council Directive 93/13/EEC. Otherwise Art. 2(4)(f) mentions that DSA is without prejudice to the rules laid down by Union law on consumer protection and product safety. | Directive 93/13/EEC aims to protect consumers from unfair terms (Article 1(1)) in contracts concluded between sellers or suppliers and consumers. Its main objective is to approximate the laws of Member States concerning unfair contractual terms, thereby ensuring a common minimum level of consumer protection across the EU and contributing to the proper functioning of the internal market. It aims to prevent significant imbalances in parties' rights and obligations to the detriment of the consumer (Article 3(1)). Directive 93/13/EEC further aims to ensure that contract terms are transparent for the consumer (Article 4(2) and Article 5). | The UCTD applies to all contracts concluded between a consumer resident in a EU Member State and a seller or supplier. It applies irrespective of the legal form or location of the seller/supplier, including when the contract is governed by the law of a non-Member State if the contract has a close connection with a member State (Article 6(2)). (Art. 1. Contracts concluded between a seller or supplier (defined in Art. 2(c)) and a consumer (defined in Art. 2(b)) | No<br><br>UCDT does not provide a exemption for SMEs. All businesses, including SMEs, must comply with its provisions when contracting with consumers | As the DSA also applies when online intermediary service providers conclude non-individually negotiated contracts with consumers, there is an overlap of personal scope with the Directive. | Similarly to the UCPD, UCTD (Article 1) aims to apply to all contracts concluded with EU consumers (when these are targeted), regardless where the trader is located. Moreover, often jurisdiction clauses may be considered unfair terms, as consumers should be able to resolve disputes under EU law in the country of their residence. | Unfair terms in B2C contracts (Art. 1(1), definition in Art. 2(a), Art. 3) and non-transparent terms in B2C contracts (Articles 4(2) and 5). The Directive requires all traders and service providers drafting standard contract terms to refrain from imposing unfair or non-transparent terms on consumers. | If the online intermediary services include B2C contracts UCTD applies concerning unfair terms. In particular (Recitals 45, 46, 48-49 and Articles 14-15 DSA will apply, which impose obligations as to what to include in the terms and conditions by online intermediary service providers. Compliance with these DSA provisions can impact the evaluation of the fairness of terms and conditions of these providers and their transparency. | Generally, MS have to ensure compliance (Art. 6-7). MS have to lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to the Directive and take all measures necessary to ensure that they are implemented (Article 8b(1)).<br>The Modernisation Directive 2019/2161 harmonised penalty criteria (nature, scale, repeated conduct) and enabled sanctions up to 4 % of turnover or minimum €2 M when penalties are to be imposed in accordance with Article 21 of Regulation (EU) 2017/2394 | Reporting obligations of online intermediary service providers under DSA include information on compliance with terms and conditions, which can facilitate enforcement of UCTD. | Interplay but no overlap<br><br>Complementary provisions | The UCTD establishes more specific obligations regarding terms and conditions and transparency. Consumers could invoke the UCTD, or courts could apply it ex officio, alongside DSA procedures, demonstrating its relevance even when the primary claim targets DSA obligations, which confirms that the UCTD operates functionally alongside the DSA. |
| Digital Fairness Act (proposal under preparation)* * | **N/A - Proposal under preparation** | N/A (proposal under preparation) | N/A (proposal under preparation) | N/A (proposal under preparation) | N/A (proposal under preparation) | In the Mission Letter dated 17 September 2024, the President of the European Commission called on then Commissioner-designate for Democracy, Justice, Rule of Law and Consumer Protection, Michael McGrath, to develop a Digital Fairness Act ("DFA") to tackle unethical techniques and commercial practices related to dark patterns, marketing by social media influencers, the addictive design of digital products and online profiling, especially when consumer vulnerabilities are exploited for commercial purposes. | N/A (proposal under preparation) | N/A (proposal under preparation) | N/A (proposal under preparation) | N/A (proposal under preparation) | The Digital Fairness Act will aim at remedying the identified legal gaps in current EU consumer protection law. It is expected to focus on dark patterns, addictive design, unfair targeted advertising and difficult management of online subscriptions. Protection of minors online in their capacity of consumers will be a key priority. The DFA is expected to include simplification and burden reduction measures. | The Digital Fairness Act will strengthen consumer protection in a targeted manner. It will not duplicate nor reopen matters that were recently regulated and are already covered by existing legislation. It will strengthen the "safety-net" of consumer law which applies to all companies, irrespective of the technology or business model. | N/A (proposal under preparation) | N/A (proposal under preparation) | N/A (propose under preparation) | The DFA is currently in its preparatory phase (Impact assessment ongoing) |
| EMFA | **Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU** | After<br><br>2024 | Yes<br><br>DSA is mentioned throughout EMFA (Recitals 8, 50, 54, 55, 76, Art. 1(d), Art 2(9)(10), Art. 18), explicitly stating that it does not affect the rules laid down by the DSA and requiring very large online platforms (VLOPs) to respect DSA obligations, particularly regarding media freedom, transparency, and systemic risk mitigation, when moderating or restricting media content | Yes<br><br>Recitals 45, Art. 1(2)(a) and 15(1), which clarify that EMFA does not affect rules laid down by Directive 2000/31/EC | DSA was adopted before EMFA, but recitals 47 and 81 mention media freedom and pluralism. | It addresses the fragmented national regulatory approaches related to media freedom, pluralism, and editorial independence. It improves the functioning of the internal market for media services, and prevents the emergence of obstacles to the operation of media service providers across the EU. The Act also establishes a clear, legally binding framework for national regulatory authorities, that deals with providers that systematically engage in disinformation, including information manipulation and interference, and misuse the internal market in media, including by state-controlled media service providers financed by certain third countries. It also strengthens the role and cooperation between media regulators, including in matters affecting the EU's information space, and complements the actions taken to develop the EU's toolbox on Foreign Information Manipulation and Interference | Recital 9) sets the definition of media service provider should cover a wide spectrum of professional media actors falling within the scope of the definition of media service, including freelancers.<br>Recital 11 establishes that where providers exercise editorial control over a section or sections of their services, they could be qualified as both a video-sharing platform provider or a provider of a very large online platform and a media service provider. Article 2 considers providers of media services, public service media, press publication, audiovisual media service, online platforms, very large online platforms, video-sharing platforms, video-sharing platform services and state advertising. | No<br><br>EMFA does not exempt SMEs from its scope or obligations. | Article 2(8) establishes the definition of online platforms refers to Article 3(i) of DSA, and Article 2(10) sets-out definition of VLOPs refers to Article 33(4) of DSA. | Providers operating in the internal market are covered under Recitals 25 60, Art. 21(1); Art. 1(1) - Internal market for media services; Art. 2(1) - It refers back to Articles 56 and 57 TFEU on the provision of "services", therefore it covers services offered by entities based in the Union as well as to entities offering their services to recipients in the Union | It enshrines the right of recipients to access media services (Art. 3) and sets out the rights of media service providers (Art. 4), while introducing safeguards to ensure the independence of public service media providers (Art. 5). The instrument also imposes specific duties on media service providers (Art. 6), including compliance with professional standards and editorial responsibility. In the context of very large online platforms (VLOPs), the instrument addresses the moderation of media content (Art. 18) and establishes mechanisms for structured dialogue between VLOP providers, media service providers, and civil society organisations (Art. 19). It further empowers users by granting them the right to customise their media offering (Art. 20). To protect media pluralism and editorial independence, the instrument introduces provisions for the assessment of media market concentrations that may impact these values (Art. 22). Finally, it sets out transparency obligations (Arts. 24-25) as regards audience measurement and allocation of state advertising. | EMFA Art. 1(2)(d) explicitly states that the Regulation does not affect rules laid down by Regulation (EU) 2022/2065, thereby establishing that the EMFA is intended to coexist with the DSA, and not override or contradict it, and any overlap must be interpreted in a way that complies with the DSA's provisions.<br>The scope of EMFA's rules regarding online platforms is harmonised with the DSA, preventing regulatory divergence in terminology and coverage.<br>EMFA Art. 18 imposes additional obligations for VLOPs that supplement those in (partly) laid down in DSA.<br>EMFA Art. 19 calls for the Board to regularly organising a structured dialogue between VLOPs, media service providers and CSO representatives (not in DSA).<br>EMFA Art. 20 grants users the right to easily customise the configuration, including in default settings, to customise their media offering according to their interests or preferences. While DSA Art. 27 sets out requirements for the transparency of those online platforms that use recommender systems., EMFA has its regulatory focus on the device / interface layer, ensuring that users can configure how media services are accessed and displayed, while DSA ensures transparency and some user influence within the algorithmic systems of online platforms. DSA provides transparency and limited control within platforms, while EMFA requires broader user control over the entry points to media services. | Article 15 - Requests for enforcement of obligations of video-sharing platform providers refers back to Article 28b(1), (2) and (3) of Directive 2010/13/EU (Audiovisual Media Services Directive 2010) at national level. | EMFA does not stipulate separate enforcement measures or fines.<br>Additionally, Art. 1(2)(d) confirmed that the EMFA Regulation does not affect rules laid down by the DSA. | Interplay but no overlap<br><br>Complementary provisions | The EMFA complements the DSA by introducing sector-specific safeguards for media service providers and recipients rather than duplicating the DSA's general obligations for online platforms. Importantly, Article 1(2)(d) of the EMFA explicitly clarifies that the Regulation does not affect the rules established by Regulation (EU) 2022/2065 (the DSA), confirming that the EMFA is intended to coexist with the DSA without overriding or contradicting it. As such, any potential overlap between the two instruments must be interpreted in a manner that is consistent with the DSA's provisions. In practice, this ensures coherence between the two frameworks, with the EMFA reinforcing and specifying the DSA's broader digital governance principles as they apply to media services. |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trade Secrets | Directive (EU) 2016/943 (Trade Secrets Directive) | Before<br>2016 | No | No | Yes<br>Recital 97 as regards appropriate access for researchers to data from VLOPSEs | To harmonise the rules across the EU on the protection against the unlawful acquisition, use and disclosure of trade secrets - Art. 1(1) | All natural and legal persons in the EU that lawfully hold trade secrets and those who unlawfully acquire, use or disclose trade secrets - covering both right holders and infringers | The Trade Secrets Directive does not exempt SMEs from its scope or obligations. Instead, the Directive explicitly recognizes the particular importance of trade secrets for SMEs, noting that SMEs often rely on trade secrets even more than larger businesses (Recital 2). | Those subject to the DSA may be right holders or infringers under the Trade Secrets Directive. | Applies across all EU Member States and EEA / EFTA States | Covers the unlawful acquisition, use and disclosure of trade secrets, and provides civil law remedies for rightsholders (Art. 1 on scope; Art. 4 on unlawful acquisition, use and disclosure; Art. 6 on general obligations to provide availability of civil redress) | The DSA provides the procedural framework for removing or disabling access to illegal content on online intermediaries. According to this Regulation the unlawful acquisition, use and disclosure of trade secrets constitutes illegal content.<br>Furthermore, in providing access to researchers, VLOPSEs should consider the protection of their trade secrets in line with Directive (EU) 2016/943 (Recital 97 DSA). | Competent judicial authorities with powers to: impose provisional and precautionary measures against alleged infringers (Art. 10), require the applicant to provide evidence (Art. 11(1)), implement other conditions of application and safeguards (Art. 11), implement injunctions and other corrective measures (Art. 12); damages (Art. 14); and publication of judicial decisions (Art. 15). These authorities may also impose sanctions for non-compliance (Art. 16) | Distinct enforcement regimes, driven by private law (Trade Secrets) vs public law (DSA). However, there may be situations in which both laws are relevant and thus both enforcement regimes can act. For instance, considering the unlawful disclosure of trade secrets on an online platform could be challenged in the courts (under Trade Secrets Directive) and/or via a DSA notice-and-action. | Interplay but no overlap<br>Complementary provisions | While many entities subject to the DSA will also be right holders under the Trade Secrets Directive, the material scopes of the two laws are distinct. |
| NIS2 | Directive (EU) 2022/2555 (NIS2 Directive) | After<br>2022 | Yes<br>Recital 140 as regards whether VLOPs could be identified as essential entities under NIS2 | No | No | To achieve a high common level of cybersecurity for entities operating in critical sectors across the Union and thus improve the functioning of the internal market - Art. 1(1) | Essential and important public or private entities across sectors of high criticality (Annex I), including digital infrastructure (e.g. internet exchange point, DNS service, Cloud computing service, Trust service providers, as well as providers of public electronic communications networks and publicly available electronic communications services), and other critical sectors (Annex II), including digital providers (e.g. providers of online marketplaces, online search engines, social networking services). Art. 2 provides further criteria for entities to be considered within the scope<br>Member State authorities also have material obligations under NIS2 | The NIS2 Directive exempts small enterprises from its scope in principle (article 2), nevertheless also allowing for the inclusion of certain small and microenterprises that play a key role for society, the economy, or specific sectors. The Directive requires Member States to provide guidance and assistance to SMEs, including those outside its direct scope (Recitals 20, 52, 56; Article 7(2)(i)), and encourages policies and support tailored to their specific cybersecurity needs and challenges | Both NIS2 and the DSA would apply to essential and important entities in digital sectors. The sector "Digital Infrastructure" (Annex I NIS2) includes several types of providers of "mere conduit", "caching" and "hosting" services under the DSA (e.g. Providers of publicly available electronic communications services, Content delivery network providers and Cloud computing service providers). The sector "Digital providers" (Annex II NIS2) encompasses providers of online marketplaces, online search engines and social networking services platforms. | Applies to public or private entities that provide their services or to carry out their activities within the EU. Requires (as per Art. 26(3)) entities not established in the EU, but offering services in the EU, to designate a representative in the EU. | Governs cybersecurity risk-management measures and reporting obligations for entities in key sectors (Art. 1(2)(b) and Chapter IV)<br>Also, requires Member States to adopt national cybersecurity strategies, designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity and CSIRTs (Art. 1(2)(a) & Chapter II). | Both laws contain risk-management and reporting obligations. A certain overlap may exist between Article 21 NIS2 and Articles 34/35 DSA, for the prevalence of risks posed to the security of network and information systems used by VLOPs can be directly related to systemic risks in the sense of Article 34(1) DSA, in particular due to the negative effects on the exercise of fundamental rights (e.g. right to privacy) as well as civic discourse and public security. | Member States to designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks under NIS2, including cyber crisis management authorities, single points of contact and CSIRTs (Art. 1(2)(a)).<br>Supervisory tasks for competent authorities established in Chapter VII, including monitoring the implementation of the Directive at national level (Art. 8(2)); single point of contact to provide liaison function to ensure cross-border and cross-sectoral cooperation (Art. 8(4), also Art. 13); management of large-scale cybersecurity incidents and crises (Art. 9(1)); timely engagement with entities facing incidents (Art. 23); operational independence (Art. 31(4)), supervisory and enforcement measures, including inspections, security audits, requests for information, as well as issuing warnings about infringements, order entities to cease conduct, impose administrative fines (Art. 32 for essential and Art. 33 for important entities). They also have notification responsibilities under Art. 3(6).<br>Explicit references to ensure coherence with competent authorities established under eIDAS Regulation (e.g. Recital 94) and Directive (EU) 2018/1972 (e.g. Recital 95); and supervisory authorities under GDPR (e.g. Art. 31(3)).<br>EU level groups established, including: Cooperation Group established to facilitate cooperation and exchange of information between Member States (Art. 14), CSIRTs network (Art. 15); EU-CyCLONe (Art. 16). ENISA supports this work (e.g. providing the secretariat of EU-CyCLONe). | NIS2 foresees that the Commission should assess whether providers falling within its scope, that are designated as very large online platforms within the meaning of Article 33 DSA could be identified as essential entities under NIS 2. | Interplay but no overlap<br>Complementary provisions | NIS2 constitutes lex specialis for VLOPs in terms of the assessment and mitigation of cybersecurity risks. The results of the assessment of these due diligence obligations can however be relevant for the enforcement of the DSA as well. Even though there is a partial coincidence in personal scope, as certain entities subject to NIS2 (e.g. digital infrastructure providers, online platforms, search engines, etc.) will also be subject to the DSA, and while the nature of some material obligations and requirements are similar in terms of risk-management, both instruments may co-exist being NIS 2 lex specialis for VLOPs. |
| FLR | Forced Labour Products<br>(Regulation 2024/3015) | After<br>2024 | Yes<br>Recital 23, stating that "any information related to the sale of products contravening the prohibition of products made with forced labour established in this Regulation should be considered to be illegal content within the meaning of Article 3, point (h)" of the DSA | Recital 23 (footnote 12) | N/A | Prohibit the placing and making available of products made with forced labour on the EU market, strengthening supply chain due diligence and consumer protection, while amending Directive (EU) 2019/1937 to support effective enforcement and whistleblower protection. | All economic operators (Article 1(1) FLR), defined as any natural or legal person or association of persons placing or making available products on the Union market or exporting products (Article 2(9) FLR). | The Forced Labour Product Regulation does not exempt SMEs from its obligations or scope. Instead, the Regulation explicitly recognizes that SMEs may face greater challenges in compliance due to limited resources (Recitals 32, 33, 34, 35, 56) and therefore mandates a range of supportive measures. These include the development of tailored guidelines, risk indicators, and due diligence guidance that take SME size and resources into account (Articles 10, 11, Recitals 32, 34, 35). The Regulation also requires Member States to establish contact points and provide accessible support, training, and information channels specifically for SMEs (Article 10, Recital 33). During investigations and enforcement, authorities must consider the size and resources of SMEs, including when setting deadlines and compliance requirements (Articles 14, 18, 21). The Commission is further tasked with evaluating the Regulation's impact on SMEs, including compliance costs and competitiveness (Recital 67, Article 38). | Intermediaries such as online marketplaces are not in the personal scope of the Forced Labour Product Regulation unless they themselves are placing or making products available on the Union market or exporting products. | N/A | Prohibition of products made with forced labour (Article 3 FLR) which covers products made entirely or partially with forced labour, including at any stage of their supply chain; this applies to finished goods, components and raw materials (supported by Recitals 3, 6, 13, 15 FLR). Overall, the material scope of this Regulation is very broad - it applies to any product linked to forced labour, at any point in its supply chain, being placed on, made available in, or exported from the EU market - regardless of where the product or company is located (Article 1 FLR, Recitals 3, 5, 17 FLR). | Recital 23 clarifies that information about products made with forced labour is considered "illegal content" under the DSA, meaning that online marketplaces have obligations under the DSA (such as notice-and action procedures), but not under this Regulation itself | Under the FLR, both the Commission and Member State competent authorities will be in charge of investigating suspected violations of the forced labour ban, and of adopting related decisions. Economic operators violate the forced labour ban under Article 3 FLR if they place or make available on the Union market products made with forced labour, or if they export such products. Article 15 of the FLR specifies that the Commission will be competent to investigate suspected forced labour outside of the territory of the Union and to adopt related decisions, while Member States will be competent to investigate suspected forced labour within their respective territories and to adopt related decisions. Decisions ordering the withdrawal or disposal of products made with forced labour under Article 20 of the FLR are to be enforced by the Member States who will be able to apply penalties in case of non-compliance (Art.23 FLR). Under Article 26 FLR, customs authorities may suspend the release for free circulation or the export of products which may be subject to a violation decision, and should dispose of such products upon the confirmation by competent authorities that they indeed correspond to a decision (Article 30) | No direct interplay - the FLR and DSA operate separate enforcement systems. Even if a product made with forced labour is sold via an online platform, FLR obligations fall on the product's importer or distributor, not the intermediary; the platform's role (as intermediary) is covered under the DSA. | Interplay but no overlap<br>Complementary provisions | No overlap - Recital 23 FLR clarifies that information about the sale of forced labour products constitutes "illegal content" under the DSA, triggering notice-and-action obligations for online platforms; however, enforcement of the forced labour ban remains with economic operators under the FLR, not with intermediaries regulated by the DSA. |
| Detergents | Regulation (EC) No. 648/2004 on detergents | Before<br>2004 | No | No | No | Regulation establishes rules designed to achieve the free movement of detergents and surfactants for detergents in the internal market while, at the same time, ensuring a high degree of protection of the environment and human health. | Manufacturers (the natural or legal person responsible for placing a detergent or a surfactant for a detergent on the market; in particular, a producer, an importer, a packager working for his own account, or any person changing the characteristics of a detergent or of a surfactant for a detergent, or creating or changing the labelling thereof shall be deemed to be a manufacturer.) | No exemptions are foreseen for SMEs | The Regulation does not address online intermediaries, marketplaces, or platforms unless they themselves act as manufacturers, importers, or change the product/label (Article 2(10)). | N/A | The Regulation covers both detergents and surfactants used in detergents. Detergents are any substances or mixtures intended for washing and cleaning processes. Detergents may be in any form (liquid, powder, paste, bar, cake, moulded piece, shape, etc.) and marketed for or used in household, or institutional or industrial purposes. Surfactants are organic substances or mixture used in detergents as main ingredients supporting their cleaning function. | If a detergent is offered for sale online and does not comply with Detergent Regulation (e.g., improper labelling), the offer may be considered "illegal content" under the DSA. The product compliance obligations remain with the manufacturer under the Detergents Regulation. The DSA does not create product compliance obligations for intermediaries; it only creates procedural obligations regarding illegal content. | General obligation of enforcement addressed to MS | No direct interplay. The enforcement provisions in both legal texts work in parallel. | Interplay but no overlap<br>Complementary provisions | The Detergents Regulation and the DSA do not overlap in personal or material scope, but may interact in practice when non-compliant detergents are offered online, triggering DSA obligations for intermediaries and product compliance obligations for manufacturers. |
| FGGR | Regulation (EU) 2024/573 of the European Parliament and of the Council of 7 February 2024 on fluorinated greenhouse gases, amending Directive (EU) 2019/1937 and repealing Regulation (EU) No 517/2014 (Text with EEA relevance) | After<br>2024 | Yes<br>Article 29(3)(b) ("Without prejudice to Regulation (EU) 2022/2065 of the European Parliament and of the Council (29) ...") | No | No | Aims to protect the health and well-being of citizens from environment-related risks and impacts, while ensuring an inclusive, fair and just transition, leaving no one behind. (Recital 1) | The FGGR regulates natural and legal persons (Article 4(7)) involved in the production, use, recovery, recycling, reclamation, and destruction of fluorinated greenhouse gases. Specifically, it mentions producers and importers (Article 4(6)), operators and manufacturers of relevant equipment (Article 5(1), Article 6(1), a.o.). More generally, it also regulates those subject to the control and reporting obligations under the regulation, including producers, importers, distributors, and users of fluorinated greenhouse gases within the European Union (as per Article 1). | SMEs are not exempt from the Regulation, but the Regulation allows for proportionate reporting requirements to minimize unnecessary administrative burdens for them (Recital 36). | When it comes to the areas of interplay of personal scope between FGGR and the DSA, the DSA's personal scope is broader since it regulates providers of digital intermediary services which includes online marketplaces that are subjected to restrictions on FGG products as per the FGGR. | The FGGR regulates fluorinated greenhouse gases within the EU but includes mention of 'third country administrative authorities' for enforcement purposes. | | The product compliance obligations remain with the manufacturer under the Detergents Regulation | Chapter VII Enforcement (Articles 28-30):<br>enforcement powers provided to:<br>According to Article 28, the competent authorities of each Member State, including customs authorities, market surveillance authorities, environmental authorities and any other competent authority with inspection functions shall cooperate with their counterparts in other Member States, and with the Commission, as well as with administrative authorities of third countries, if necessary for the enforcement of the Regulation. When an infringement is detected by the abovementioned bodies, they shall notify the environmental authority or, if not relevant, any other authority responsible for the enforcement of penalties. | The DSA states that Member States shall designate one or more competent authorities for the enforcement of the DSA Regulation (Article 49(1)).<br>The competent enforcement authorities that are explicitly stated in the FGGR are customs authorities, market surveillance authorities and environmental authorities, although the text states that any other competent authority with inspection functions could also be included in enforcement. Theoretically, interplay in enforcement could arise if the Member State designates the same authorities that are responsible for the enforcement of the FGGR as the competent bodies to enforce the DSA | Interplay but no overlap<br>Complementary provisions | The FGGR imposes an additional obligation for Member States to conduct "checks of online platforms [that allow] distance contracts to be concluded with undertakings offering fluorinated greenhouse gases or products and equipment that contain such gases" (FGGR Article 29(3)(b)) in order to verify whether "the undertaking, the fluorinated greenhouse gases, the products or the equipment offered comply with the requirements laid down in [the FGGR]." (FGGR Article 29(3)(b)). This obligation is complementary to DSA provisions and does not introduce an overlap in law. |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OLR | **Regulation (EU) 2024/590 of the European Parliament and of the Council of 7 February 2024 on substances that deplete the ozone layer, and repealing Regulation (EC) No 1005/2009 (Text with EEA relevance)** | After 2024 | Yes<br>Article 26(3)(b): "checks of online platforms pursuant to this paragraph. Without prejudice to Regulation (EU) 2022/2065 of the European Parliament and of the Council..." | No | No | It address the depletion of the ozone layer by regulating substances that cause this depletion. It aims to contribute to the recovery of stratospheric ozone, limit global warming, and ensure compliance with the Montreal Protocol on Substances that Deplete the Ozone Layer and other relevant EU law and international commitments regarding environmental protection. | The OLR regulates any potential producers of ozone layer depleting substances (Article 3(7)), suppliers, providers, those who place such substances on the market, importers and exporters of these substances (Article 4), and explicitly prohibits those activities. | No exemptions are foreseen for SMEs | The DSA regulates providers of online intermediary services. This category includes marketplaces that are subjected to checks on ozone depleting substances as established in the OLR. | The OLR regulates ozone depleting substances within the EU but includes mention of 'third country administrative authorities' for enforcement purposes. | The ESPR is a framework legislation that lays the foundation for the subsequent adoption of concrete rules, either on a product-by-product basis or horizontally, based on groups of products with similar characteristics. | The DSA does not create product compliance obligations for intermediaries; it only creates procedural obligations regarding illegal content. | Chapter VII Enforcement (Articles 25-26). Article 25(1) states that the competent authorities of the Member States for enforcement of the OLR include customs authorities, market surveillance authorities, environmental authorities and any other competent authority with inspection functions. The Article stipulates that these authorities shall cooperate with their counterparts in other EU Member States or third country administrative authorities for purposes of enforcement of this Regulation, as well as with the European Commission. | OLR Article 26(3)(b) states that the competent authorities of Member States shall carry out checks of online platforms on the basis of substantiated concerns of risk to compliance with the OLR. Without prejudice to Regulation (EU) 2022/2065 of the European Parliament and of the Council (24), where an online platform, falling within the scope of Chapter III, Section 4, of that Regulation, allows distance contracts to be concluded with undertakings offering ozone-depleting substances or products and equipment that contain such substances, competent authorities of Member States shall verify whether the undertaking, the ozone-depleting substances, the products or the equipment offered comply with the requirements laid down in this Regulation. Competent authorities shall inform and cooperate with the Commission and with the relevant competent authorities referred to in Article 49 of Regulation (EU) 2022/2065 for the purpose of ensuring compliance with that Regulation. | Interplay but no overlap<br><br>Complementary provisions | Article 26(3)(b) of the OLR foresees checks of online platforms by the 'competent authorities' of Member States when it comes to substantiated risks of non-compliance with the Regulation. This introduces an additional obligation on Member States to carry out checks to online platforms that allow consumers to conclude distance contracts with undertakings offering ozone-depleting substances or products and equipment that contain such substances. The checks consist of verifying whether the undertaking, the ozone-depleting substances, the products or the equipment offered via an online platform comply with the requirements laid down in the OLR. |
| Rome I Regulation | **Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, p. 6–16.** | Before 2008 | No | Yes<br>Recital 40. | No | Rome I regulates conflict of laws in contractual obligations in most civil and commercial matters. It aims to provide legal certainty, predictability, and consistency in cross-border contracts by harmonising the conflict of laws rules that decide which national law governs contractual relationships within the EU. | Applies to all contractual parties. More specifically, it applies to physical and legal persons (any entity that the law recognises as having rights and responsibilities, such as companies, etc.) who can be bound by contract (Article 1(1)). Guides the work of public authorities, like courts or other relevant organs who have to determine applicable legislation to contractual obligations. | No exemptions are foreseen for SMEs | Rome I regulates the applicable legislation for all cross-border contractual disputes across EU Member States (except Denmark), in situations involving a conflict of laws to contractual obligations in civil and commercial matters, and covers all contractual parties. All providers of online intermediary services will most probably be involved in some type of contractual obligation or be contractual parties to their recipients. This means that there is an interplay with the DSA. | Applies to conflict of laws in all Member States of the European Union (Article 2, Article 1(4)), except Denmark (Recital 46). | | Recital 10 of the DSA states that the Regulation (DSA) shall be without prejudice to, among others, rules on the law applicable to contractual and non-contractual obligations. Rome I can potentially affect anything contractual, which can be materially connected to everything contractual the DSA regulates. Rome I offers the general guidelines on how to resolve cross-border conflicts of law arising from contractual obligations, which could definitely be applicable to the entities regulated by the DSA as per its personal scope.<br>The DSA itself does not contain any provision discussing which law shall be applicable to contracts concluded within the DSA's remit, therefore there is no duplication or overlap. Articles of the DSA that have an interplay with Rome I include Articles 29 through 32 addressing distance contracts concluded with traders. These Articles are compatible with Rome I and do not introduce any duplications or overlaps. | N/A (Rome I does not include provisions on enforcement) | N/A | Interplay but no overlap<br><br>Complementary provisions | No overlpas - the two Regulations can be applied harmoniously in parallel without conflicts |
| Rome II Regulation | **Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007, p. 40–49.** | Before 2012 | N/A | Yes<br>Recital 35 | No | Rome II regulates conflict of laws in non-contractual obligations in civil and commercial matters. It<br>It brings greater legal certainty as to the law applicable with respect to non-contractual obligations, in particular in cases of tort (common law jurisdiction) and delict (civil law jurisdiction). This regulation facilitates the smooth functioning of the internal market by reducing legal uncertainty and enhancing judicial cooperation in matters of non-contractual liability. | Applies to the public authorities, courts and other relevant organs who have to determine applicable legislation to non-contractual obligations.<br>Applies to physical and legal persons (any entity that the law recognises as having rights and responsibilities, such as companies, etc.) who can be bound by non-contractual obligations (Article 1(1)). | No exemptions are foreseen for SMEs | The Rome II Regulation's scope is much broader than the DSA seeing as it regulates the applicable legislation for all cross-border non-contractual disputes across EU Member States, in situations involving a conflict of laws to non-contractual obligations in civil and commercial matters. It would presumably also include the providers of online intermediary services, seeing as they could theoretically be bound by non-contractual obligations, for example unjust enrichment (Article 10), *Culpa in contrahendo* (Article 12), etc. | Applies to conflict of laws in all Member States of the European Union (Recital 2, Recital 6, Article 3), except Denmark (Article 1(4)).<br>Could apply to situations where the applicable law might be that of a non-EU country (Recital 2, Article 3). | The process started with a prioritisation exercise, following this, the Commission adopted the first ESPR and Energy Labelling Working Plan in April 2025, setting out which products will be prioritised over the coming years. | There is some interplay between the DSA and Rome II. Entities regulated by the DSA (such as online platforms) could be bound by non-contractual obligations as regulated by Rome II, but there is no duplication between the relevant provisions in Rome II and those in the DSA. Recital 10 of the DSA does mention Rome II by stating that the Regulation (DSA) shall be without prejudice to, among others, rules on the law applicable to contractual and non-contractual obligations. | N/A (Rome II does not include provisions on enforcement) | N/A | Interplay but no overlap<br><br>Complementary provisions | The DSA and Rome II are complementary. Rome II can be used to answer questions on applicable law arising from certain articles of the DSA, like Article 54 on damages claims. |
| CSAM(Under negotiation) ** | **CSAM Regulation (Proposal)** | N/A (under negotiation) | N/A - no official proposal | Yes<br>In the proposal - Recitals 7, 8, 10, 15, 16, 31, 40, 42, Art. 1, 2, and 4: all together stating that it is without prejudice to the ECD | No | To establish harmonised EU rules to prevent, detect, and combat child sexual abuse, protecting children's safety online and offline while safeguarding fundamental rights. | Hosting service providers (Article 2 (a) CSAM which also refers to DSA); Providers of interpersonal communication services (Article 2 (b) CSAM); App store providers (Article 2 (dl CSAM); Internet access services (Article 2 (e) CSAM); Providers of other relevant online services (Article 2 (f) CSAM)). Moreover, Recitals 9-15 justify the personal scope. | In the proposal, SMEs are not exempt from the CSAM Regulation's obligations, but the Regulation provides for cost exemptions and requires that penalties be proportionate to the size and resources of SMEs, thereby mitigating the regulatory burden on smaller providers (Article 3(3) and 35(5)(f)). | In the proposal, there is substantial but not complete overlap in personal scope between the CSAM Regulation and the DSA. The CSAM goes further, applying to personal messaging, ISPs and app stores, making its scope broader in some areas. Therefore, many providers will be subjected to both, but some (like WhatsApp or Vodafone) are subject only to CSAM and not to the DSA. Moreover, the DSA does not explicitly regulate app stores as a distinct category instead, they may fall under "online platforms" (Article 3 DSA) if they allow users to disseminate content to the public. App stores are explicitly included in the CSAM (Article 6 CSAM). | The proposal references DSA in Article 2(g): 'to offer services in the Union' means to offer services in the Union as defined in Article 2, point (d), of Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC] | CSAM aims to prevent, detect, report, remove and block child sexual abuse material and associated online activities. The CSAM focuses on two key types of online harms: child sexual abuse material (Article 2 (i-n) CSAM) and child sexual exploitation or grooming (Article 2 (o-s) CSAM). The CSAM introduces detailed rules across multiple areas: Risk assessment (Article 3 CSAM), Risk mitigation (Article 4 CSAM), Risk reporting (Article 5 CSAM), Issuance of detection orders (Article 7-8 CSAM), Reporting obligations (Article 12-13 CSAM), Removal orders (Article 14-15 CSAM), Blocking orders (Article 16-18 CSAM). Preservation of information (Article 22 CSAM), User notification and redress (Article 23-24 CSAM). | The CSAM Regulation and the DSA partially overlap in material scope, especially in shared responsibilities for hosting providers dealing with illegal content. However, the CSAM introduces additional, targeted obligations that go beyond or differ from the DSA - especially around detection, grooming, blocking, and preservation. The material scopes are complementary, but the CSAM clearly represents a sector-specific regime with standalone enforcement tools. Overlaps: Obligations to assess risk (Articles 3-4 CSAM - mandatory specific risk assessments) and General systemic risk for VLOPs (Articles 34-35 DSA) and Removal of illegal content (Articles 18-19 CSAM) and Orders to act against illegal content (Article 9 DSA). Partial overlaps: Transparency obligations (Articles 11-13 CSAM specific to CSAM incidents and detection reports) and General transparency on content moderation (Articles 15-24 DSA). On detection obligations (Articles 7-9 CSAM) there is a different approach to DSA - on CSAM there are specific detection orders possible from authorities. Blocking orders and preservation of evidence are CSAM-only, nothing equivalent in the DSA. | Articles 25-35 CSAM: Each Member State must designate a coordinating authority to oversee compliance by service providers, issue detection, removal, and blocking orders, handle user complains and appeals, coordinate with other Member States and the EU Centre (Articles 49-50 CSAM). Some powers, such as issuing detection orders, must be exercised by a judicial or independent administrative authority to ensure due process (Article 14(4) CSAM). The EU Centre on Child Sexual Abuse will act as a central node for CSAM detection and reporting, receive and validate reports from providers, provide hash databases, tools and guidance, coordinate and monitor cross-border enforcement. They Commission plans a supporting and coordinating role, including oversight of the EU Centre. It may also take infringement actions against Member States for failure to enforce. | Parallel but distinct enforcement tracks - the proposed CSAM Regulation and the DSA establish separate enforcement structures that may apply to the same providers, but in different legal contexts. Parallel enforcement may occur particularly where a hosting provider or app store is subject to both DSA and CSAM due to its size, reach or service type; the providers fails to mitigate systemic risks (Article 35 DSA) and also facilitates CSAM dissemination or grooming (Article 14 CSAM). A VLOP is under Commission supervision (DSA) and receives a detection or blocking order under CSAM. | N/A - no official proposal | The CSAM is still in negotiations and the text not published yet<br><br>However, from the proposal, there is clear overlap between the CSAM and DSA in terms of actors (hosting services, app stores, online platforms), some obligations (risk assessments, content removal), subject matter (illegal content - in this case, CSAM). However, the overlap is legally coherent: The CSAM is lex specialis for CSAM, introducing stricter, targeted obligations that go beyond the DSA. There is no contradiction between the two instruments. They are designed to operate in parallel, with distinct enforcement authorities and separate legal bases. |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Drugs precursors | **Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors (Text with EEA relevance)** | Before 2004 | No | No | No | To establish a harmonised legal framework within the European Union for controlling the manufacture, marketing, and distribution of substances that are used in the illicit manufacture of narcotic drugs and psychotropic substances. The Regulation aims to prevent the diversion of these precursor chemicals from legitimate trade into illegal drug production. Overall, the regulation is designed to balance the legitimate industrial and commercial use of these chemicals with the need to combat illegal drug production. | The DPR regulates "operators" as defined in Article 2(d) as "any natural or legal person engaged in the placing on the market of scheduled substances", where placing on the market denotes the supply (whether for return of payment or free of charge) of scheduled substances in the Union, or the "storage, manufacture, production, processing, trade, dis-tribution or brokering of these substances for the purpose of supply in the Union" (Article 2(c)). | No exemptions are foreseen for SMEs | The DPR personal scope includes both physical and online environments but does not directly regulate intermediary service providers as defined in the DSA. On the one hand, online intermediary platforms allowing traders to conclude distance contracts with customers are subject to the requirements laid down in the DSA. On the other hand, where the provider of a marketplace qualifies as an economic operator such as manufacturer, distributor or importer, the DSA would not apply, and instead the marketplace is subject to specific sectoral obligations according to Regulation (EC) 273/2004. | The Regulation applies within the territory of the EU, covering internal trade of scheduled substances that are frequently used in the illicit manufacture of narcotic drugs or psychotropic substances | The DPR's material scope focuses on regulating the conduct of operators who are involved in the placing on the market—defined broadly to include manufacture, import, export, distribution, and brokering—of scheduled substances listed in Annex I. These substances are divided into categories based on their risk of diversion, with Category 1 being subject to the most stringent controls. | The DSA sets out horizontal obligations for online platforms, such as requirements for trader traceability (Article 30), platform design to enable compliance with Union law (Article 31), and consumer information (Article 32), which apply across all product categories. In parallel, the DPR introduces sector-specific rules for the lawful marketing, distribution, and control of scheduled substances used in the illicit manufacture of narcotics, with Articles 3–5 and 7 imposing obligations on operators regarding classification, licensing, documentation, and labelling of precursor chemicals. These DPR obligations apply to all trade channels, including online, and thus intersect with the DSA's requirements for platforms facilitating such transactions. | According to Article 11(1), each Member State shall designate which are the competent authorities responsible for applying the Regulation and inform the Commission accordingly. As per Article 12, Member States will formulate the rules on applicable penalties for infringement (which must be effective, proportionate and dissuasive), giving the Member States great leeway in designating what their enforcement powers will be. Article 10(1) refines the scope of measures by stating that each Member State "shall adopt the measures necessary to enable its competent authorities to perform their control and monitoring duties, and in particular: (a) to obtain information on any orders for scheduled substances or operations involving scheduled substances; (b) to enter operators' business premises in order to obtain evidence of irregularities; (c) where necessary, to detain consignments that fail to comply with this Regulation." | There is an interplay only in certain areas that are regulated by the DSA and the Drugs Precursors Regulation. The Regulation requires Member States to lay down rules on penalties (Article 12 Drugs Precursors) but, unlike the DSA, does not define specific levels (Article 52 DSA). Furthermore, since the Member States are responsible for determining which are the competent authorities for enforcement in both the DSA and the Drugs Precursors Regulation, there is a theoretical scenario in which a Member State may designate the same authority as competent to enforce the two Regulations. | Interplay but no overlap<br><br>Complementary provisions |
| Energy labelling | **Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (Text with EEA relevance) and its delegated acts** | Before DSA | Yes (in delegated acts after 2022) | No | No | Improve energy efficiency as part of the Union's 2030 Climate and Energy Policy Framework. Enabling customers to make informed choices based on standardised informaiton on the energy consumption and energy efficiency of energy-related products. | Energy labelling puts obligations on suppliers and dealers of energy-related products covered by delegated acts. The supplier is the manufacturer established in the Union, the authorised representative of a manufacturer who is not established in the Union, or an importer, who places a product on the Union market. The dealer is a retailer or other natural or legal person who offers for sale, hire, or hire purchase, or displays products to customers or installers in the course of a commercial activity, whether or not in return for payment. | No exemptions are foreseen for SMEs | The Regulation directly addresses online intermediaries, marketplaces, or platforms only to the extent that they act as supplier or dealer. Dealers offering products online are subject to DSA's provisions on traders.<br><br>However, by setting labelling requirements for products sold online, the Regulation also creates compliance by design obligations for the concerned providers of online platforms, by virtue of Art. 31 of the DSA.<br>Six energy labelling delegated acts adopted in 2019 (prior to the DSA) set information and compliance by design obligations for hosting service providers that allow the direct selling of the concerned products through their internet website.<br>Newer energy labelling delegated acts, adopted after DSA, plug into Art. 31 of the DSA via a recital that clarifies how Art. 31 applies with respect to energy labelling. | The Regulation applies to energy-related products placed on the EU market, and targets suppliers and dealers of such products. The supplier is by definition established in the EU while the dealer can be esatbished inside or outside the EU (the latter more specifically in the case of online sales). | The Regulation is a framework that enables the Commission to set energy labelling requirements for specific energy-related products placed on the EU market through delegated acts. | If a product in scope is offered for sale online without complying to the applicable energy labelling requirements, the offer may be considered "illegal content" under the DSA. The compliance obligations remain with the supplier or the dealer, unless compliance by design is at stake. | General obligation of enforcement addressed to national market surveillance authorities. | There is an overlap with the six energy labelling delegated acts adopted in 2019 (prior to the DSA) which set information and compliance by design obligations for hosting service providers that allow the direct selling of the concerned products through their internet website. This overlaps with Art 31 of the DSA, and is to be enfored by national marke surveillance authorities.<br><br>For the other delegated acts, no specific interplay, the enforcement provisions in the respecte legal texts work in parallel. | Overlap for six delegated act adopted in 2019<br><br>Complementary interplay otherwise. |
| Tyre labelling | **Regulation (EU) 2020/740 of the European Parliament and of the Council of 25 May 2020 on the labelling of tyres with respect to fuel efficiency and other parameters, amending Regulation (EU) 2017/1369 and repealing Regulation (EC) No 1222/2009 (Text with EEA relevance)** | Before DSA | No | No | No | Improve fuel efficiency as part of the Union's 2030 Climate and tyre Policy Framework. Enabling customers to take cost effective and environmentally friendly decisions when purchasing tyres, based on standardised informaiton on the tyre rolling resistance, wet grip and noise. | Tyre labelling puts obligations on suppliers and distributors of tyres. The supplier is the manufacturer established in the Union, the authorised representative of a manufacturer who is not established in the Union, or an importer, who places a product on the Union market. The distributor is a natural or legal person in the supply chain, other than the supplier, who makes a product available on the market. | No exemptions are foreseen for SMEs | The Regulation directly addresses online intermediaries, marketplaces, or platforms to the extent that they act as supplier or distributor. Distributors offering products online are subject to DSA's provisions on traders.<br><br>In addition, the Regulation's Art. 8 sets information and compliance by design obligations for hosting service providers that allow the direct selling of tyres through their internet website (overlap with Art. 31 of DSA). | The Regulation applies to tyres placed on the EU market, and targets suppliers and distributors of such products. The supplier is by definition established in the EU. | The Regulation sets tyre labelling requirements for tyres placed on the EU market. | If a tyre in scope is offered for sale online without complying to the applicable tyre labelling requirements, the offer may be considered "illegal content" under the DSA. The compliance obligations remain with the supplier or the distributor, unless compliance by design is at stake. | Obligation of enforcement addressed to national market surveillance authorities. | The Regulation's compliance by design obligations overlap with Art 31 of DSA, and are to be enfored by national market surveillance authorities. | Overlap for compliance by design.<br><br>Complementary interplay otherwise. |

# ANNEX 4: SURVEY ANALYSIS

This Annex presents the findings from three targeted surveys conducted as part of the Commission services preparatory work for its evaluation of the interplay between the DSA and other EU rules applicable to online intermediaries. The surveys were addressed respectively to civil society organisations (CSOs), Digital Services Coordinators (DSCs) and other relevant authorities, and online intermediaries, including very large online platforms (VLOPs) or very large online search engines (VLOSEs).

The purpose of these surveys was to gather practical, "on-the-ground" insights from a diverse range of stakeholders regarding the application of the DSA in the broader context of the EU digital regulatory framework.

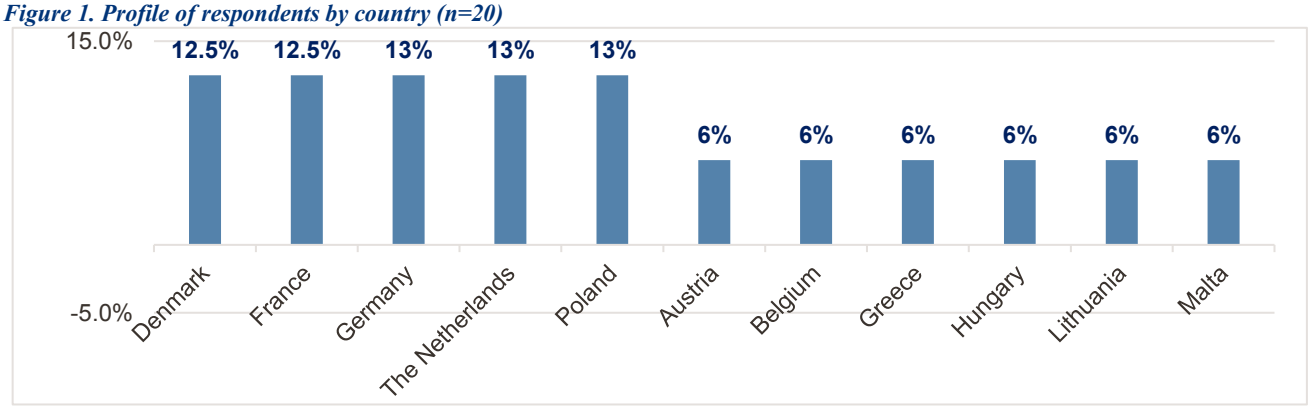
The three surveys were launched by the Commission services and received a total of 97 responses –20 from CSOs, 56 from DSCs and other authorities, and 21 from intermediaries. In addition, one additional VLOP provided some insight in writing (but did not complete the survey).

## 1.1 Civil society organisations

### *1.1.1. Profile of respondents*

Among the 20 CSOs which responded to the survey 7 (35%) indicated conducting activities at the EU wide level while 13 (65%) operate at the national level, collectively covering 11 Member States through their activities.

***Figure 1. Profile of respondents by country (n=20)***

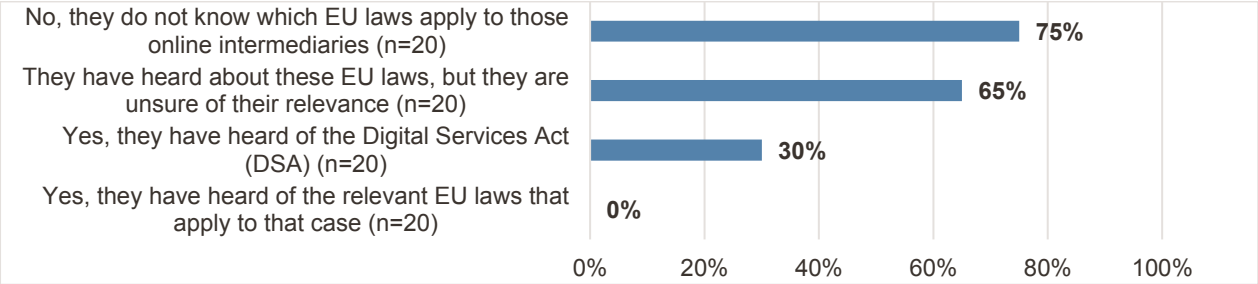



### *1.1.2. Awareness of Union law protecting users of online intermediary services*

CSOs were asked several questions to assess **whether the users they represent are aware of how Union law protects them when using online intermediary services** such as social media platforms, online marketplaces, or search engines.

The majority of respondents were of the opinion that users do not know which Union laws apply to online intermediaries (75%). Most (65%) considered that while users have heard about these laws, they are unsure of their relevance. When asked specifically about the DSA, only a few CSOs (30%) considered that users were aware of the instrument, and none believed that users were familiar with the specific Union laws relevant to their individual situations.

*Figure 2. In your view, would the users you represent know how Union law protects them as users of online intermediary services (like social media platforms, online marketplaces, or search engines)?*




*1.1.3. Knowledge of rules or authorities in specific situations*

CSOs were asked to describe, for several common online situations, who the users they represent would contact or what rules would apply.

**Receiving a dangerous or faulty product bought through an online marketplace (n=16):** Out of 16 responses received for this scenario, 9 (56%) indicated that users would know to contact a relevant authority or organisation, such as consumer protection agencies, consumer associations, or the platform itself. One response expressed uncertainty, while two responses noted that users would rely on informal channels such as parents or friends. Four organisations specifically emphasised that children, in particular, would be unlikely to seek help or would not be aware of the appropriate authority to contact.

**Being exposed to illegal or harmful content (e.g. hate speech, cyberviolence, disinformation) (n=20):** For this scenario, 15 out of 20 responded (75%) by identifying specific authorities or mechanisms that users might contact, including the police, national helplines, Digital Service Coordinators, or the platform's own reporting tools. The DSA was frequently mentioned as the relevant legal framework. However, a notable proportion of responses highlighted that users, especially children, often do not seek help or are unaware of the available mechanisms. In some cases, it was noted that users would turn to civil society organisations or friends rather than formal authorities.

**Being misled by a commercial offer (e.g. false advertising, unclear prices or terms) through an online platform (n=16):** When asked about misleading commercial offers, 9 out of 16 responses (56%) considered that users would know to contact consumer protection authorities, consumer associations, or the relevant platform. The remaining 7 responses indicated that users would not be aware of having been misled, or would not know which authority to contact. Children, in particular, were identified as being unlikely to recognise or report such issues. This points to a moderate level of awareness, but with significant gaps, especially among vulnerable groups.

**Having personal data misused or shared without their knowledge (n=18):** In the case of personal data misuse, 11 out of 18 responses (61%) considered that users would know to contact data protection authorities, such as national Data Protection Agencies or the platform in question. The General Data Protection Regulation was commonly referenced as the applicable legal framework. Nevertheless, seven organisations (39%) noted that users often do not seek help or rely on informal support networks. Some responses highlighted the complexity of the regulatory landscape, and the challenges users face in identifying the appropriate authority.

**Having their content taken down or their account restricted by an online platform (n=19):** For the scenario involving content removal or account restriction, 11 out of 19 responses (58%) considered that users would use the platform's complaint mechanism or contact an out-of-court dispute body, where available. The DSA was again frequently mentioned as the relevant framework. However, it was also observed that many users would not seek help, would wait for the account to be restored, or would not know the reason for the restriction.

*1.1.4. User experience and awareness regarding online platforms and Union law*

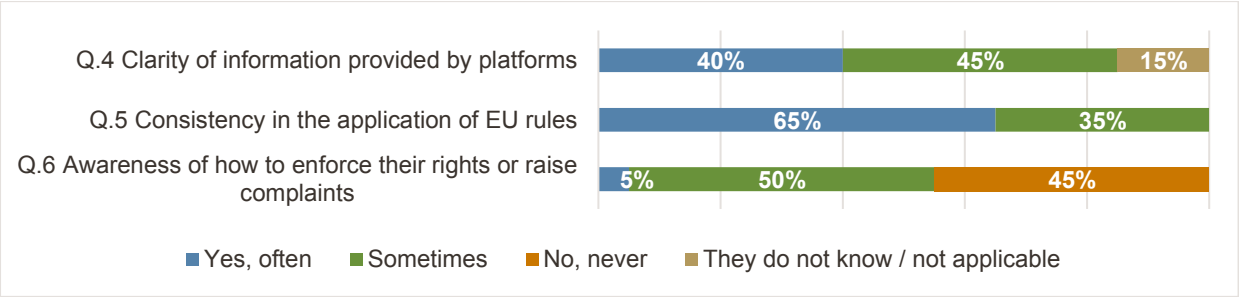
CSOs were asked three key questions[168] about the experiences and awareness of the users they represent regarding online platforms and the application of Union law:

First, regarding the **clarity of information provided by online platforms and search engines**, 40% of CSOs (8 respondents) reported that users "often" encounter unclear or contradictory information, while 45% (9 respondents) said this happens "sometimes." None of the CSOs selected "No, never," and the remaining 15% (3 respondents) either did not know or found that the question was not applicable to their experience.

Second, on the **consistency in applying EU rules**, 65% of CSOs (13 respondents) indicated that users have experienced inconsistent or unclear outcomes. No respondents stated that everything was consistent, and 35% (7 respondents) were unsure or considered the question not relevant to their experience.

Finally, concerning **users' awareness of how to enforce their rights or raise complaints**, only one organisation believed users are fully aware of the appropriate channels and authorities to contact. Half of the respondents (10 CSOs) felt users need additional support, while nearly as many (9 CSOs) reported a complete lack of awareness among users.

***Figure 3. CSO perspectives on user experience and awareness regarding online platforms and Union law (n=20)***

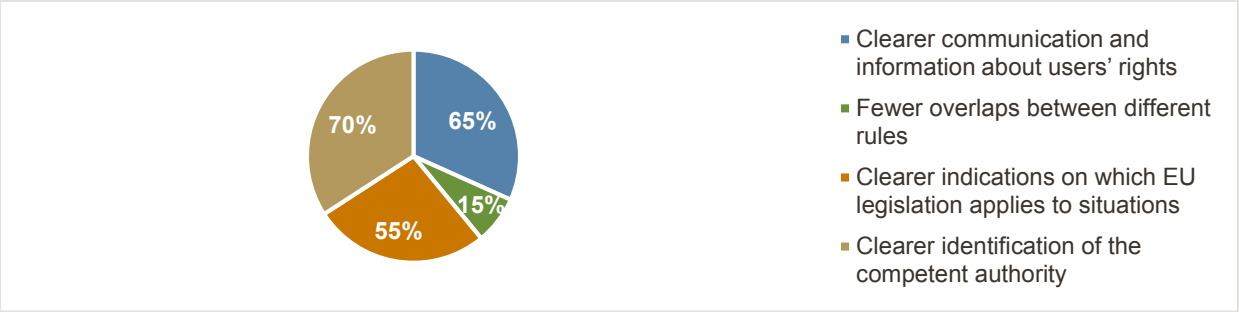



*1.1.5. Priorities for ensuring the correct applicability of EU rules on online services*

CSOs were provided options and asked to indicate which they considered **most important to ensure the correct applicability of EU rules on online services.** The most frequently selected priority was "clearer identification of the competent authority", which was chosen by 14 CSOs (70%). This was closely followed by "clearer communication and information about users' rights", selected by 13 CSOs (65%) and "Clearer indications on which EU legislation applies to concrete situations" (11 CSOs, 55%). In contrast, "fewer overlaps between different rules" was selected by only 3 CSOs (15%).

168 Q4. "Based on the experience gathered in your organization, have the users you represent indicated that online platforms and search engines gave unclear or contradictory information about their rights or the reasons behind a decision (e.g. content taken down, account blocked)?"
Q5. "Based on the experience gathered in your organization, have the users you represent experienced divergent or inconsistent results from the application of EU rules depending on the online platform, or the country, or the issue at stake?"
Q6. If the users you represent wanted to raise a complaint or enforce their rights online, would they in your view know which regulatory authority to contact or how to otherwise enforce their rights?

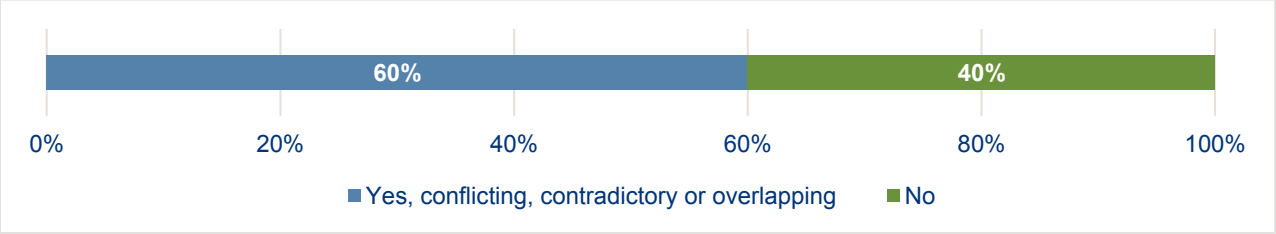
*Figure 4. In your view, what is most important to ensure the correct applicability of on online services? (n=20)*




### *1.1.6. Conflicting, contradictory, or overlapping provisions resulting from the DSA and other Union law instruments*

CSOs were asked whether they had identified any **conflicting, contradictory, or overlapping provisions resulting from the DSA and its interplay with other Union law instruments**. Ten CSOs reported that they had identified overlapping provisions between the DSA and other Union law instruments, and two reported conflicting or contradictory provisions (60% in total). The remaining eight CSOs (40%) stated that they had not identified any such issues.

*Figure 5. Have you identified any conflicting, contradicting or overlapping provisions resulting from the DSA and its interplay with other Union law instruments? (n=20)*




CSOs who selected "Yes, conflicting or contradictory" or "Yes, overlapping" were invited to provide further details regarding the nature of these issues. The qualitative responses reveal several recurring themes and specific areas where overlaps or ambiguities have been identified in the interplay between the DSA and other Union law instruments.

**The most frequently cited overlap was between the DSA and the General Data Protection Regulation (GDPR).** Seven out of twelve CSOs noted that provisions relating to the processing of personal data by online platforms, particularly those found in Articles 26(1), 26(3), 28(2), and 38 of the DSA, intersect with the GDPR. It was observed that while these articles of the DSA are intended to address specific concerns, such as the processing of personal data and the prohibition of dark patterns, they may nonetheless create uncertainty regarding which regulation should take precedence in particular cases. For example, questions were raised about which practices of online platforms fall within the scope of "addictive design" regulated by the DSA, such as whether features like endless scrolling or default notifications are included. Additionally, questions were raised about whether consumers and their advocates can rely on the DSA when Data Protection Authorities (DPAs) or consumer protection authorities reject their complaints based on the GDPR or consumer law—an issue frequently observed in Poland due to narrow legal interpretations and a conservative approach by these bodies. Finally, it was considered not clear whether the prohibition of targeted advertising under Article 28 of the DSA excludes targeting based on personal data that users knowingly and willingly provide (especially when the user is a minor), or if it only applies to targeting based on observed behavioural data, which typically involves profiling as defined by the GDPR.

**Ambiguity was reported in relation to Article 25 of the DSA, which addresses dark patterns**. Three CSOs highlighted a potential overlap with the Directive on Unfair Commercial Practices (UCPD). As one CSO explained: "*DSA introduced a prohibition of dark patterns which however does not apply to consumer to business commercial practices. In those cases, UCPD applies but lacks legal certainty due to the lack of more prescriptive provisions, and it is left to national courts to rule how the DSA and UCPD interplay*". To address this, some CSOs suggested that the forthcoming Digital Fairness Act could introduce similar provisions into the UCPD. As another CSO put it: "*It will be important to clarify the relationship between Article 25 of the DSA and relevant provisions of the forthcoming DFA*.".

**Overlaps were identified between the DSA and consumer protection law**. It was noted, in broader terms, that consumer law and data protection experts continue to debate the intended scope of certain DSA provisions, and that in practice, users and their advocates may face challenges when complaints are dismissed by data protection or consumer protection authorities on the grounds that the matter falls under a different legal regime.

One CSOs mentioned an overlap between the DSA and the Audiovisual Media Services Directive (AVMSD) in the context of disinformation on video-sharing platforms, without providing further details.

*1.1.7. Suggestions to facilitate the applicability and clarity of the EU regulatory Framework*

CSOs were invited to provide suggestions to facilitate the applicability of the EU regulatory framework for online intermediary services or to clarify its interplay with other Union law. The responses received highlight several recurring themes and practical recommendations.

**Clearer guidance and joint interpretation:** Four CSOs called for clearer, joint guidance from EU institutions and relevant authorities. Suggestions included the publication of joint guidelines or handbooks – such as between the European Commission and the EDPB – to clarify the interplay between the DSA and other legal instruments, particularly the GDPR and the UCPD (on dark patterns). The development of a "Handbook for Digital Service Providers" and a Digital Enforcement Strategy were specifically recommended to address complexity and ensure consistent application of the rules.

**Tools for regulatory mapping and navigation:** Two CSOs suggested the creation of regulatory mapping tools or databases to help non-expert users and businesses navigate the complex landscape of EU digital regulation. These tools would visualise the interaction between different laws and guide users to the correct authority or process.

**Improved communication and user information:** One CSO emphasised the importance of clearer communication for users. Recommendations included the creation of digital rights dashboards, public EU-wide digital hubs, and age-appropriate explanations for children and parents. Platforms, especially very large online platforms (VLOPs), were encouraged to provide users with transparent dashboards detailing data collection, algorithmic processes, content removal reasons, and complaint mechanisms.

**Enhanced coordination and cooperation among authorities:** One CSO highlighted the need for improved coordination and cooperation among regulatory authorities, both at the EU and national levels. It was proposed that coordination platforms be established to streamline enforcement, facilitate information sharing, and ensure that different authorities can cooperate effectively, particularly in cases involving overlapping investigations or cross-border issues.

**Special considerations for children and vulnerable users:** One CSO stressed the importance of making reporting tools and complaint mechanisms accessible and child-friendly. It was recommended that children and young people be heard in the enforcement process, and that representatives, such as parents and organisations, be able to bring cases on their behalf.

**Other specific suggestions:** One CSO highlighted the need for effective enforcement of sanctions, such as those targeting Russian media under the DSA; another emphasised the importance of providing adequate resources for Trusted Flaggers; while a third called for the development of standardised criteria to determine when services fall under multiple regulatory frameworks.

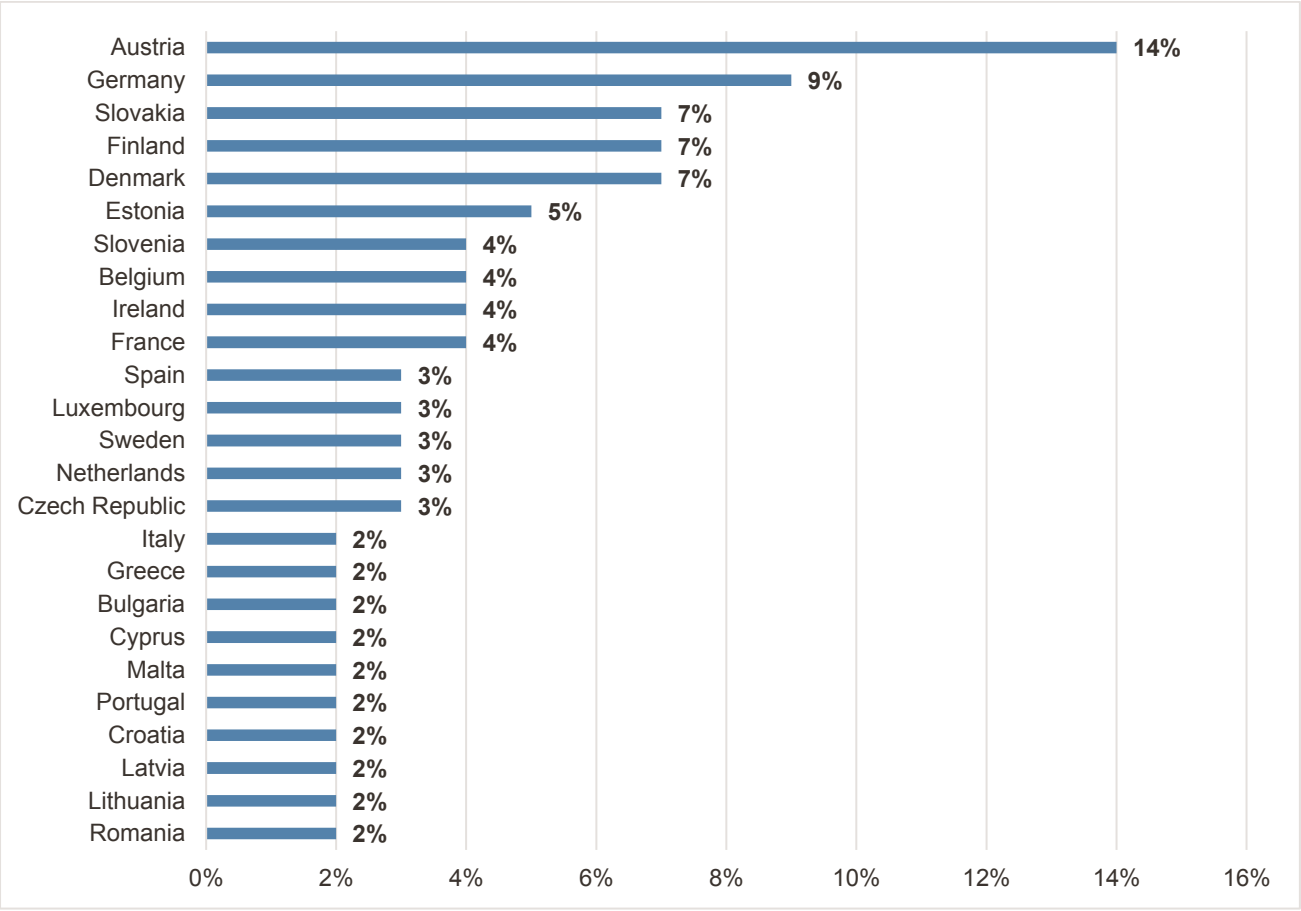
## 1.2. DSCs & other relevant authorities

### *1.2.1. Profile of respondents*

A total of 56 responses were received to the survey from authorities in 25 EU Member States. The majority of responses were from national-level authorities (89%), with a smaller number representing regional or city-level bodies (11%). Austria recorded the highest number of responses (eight authorities), Germany followed (five), Denmark (four), Finland (four), and Slovakia (four). Hungary and Poland are not represented.

The authorities represented in the survey covered a broad range of areas of competence, reflecting the horizontal scope of the DSA. These included digital services, data protection, consumer protection, audiovisual media regulation, electronic communications, competition law, market surveillance, product safety, postal regulation, agri-food law, and among others. Several authorities indicated competence in multiple areas.

***Figure 6. Distribution of responding authorities by Member State (n=56)***




### *1.2.2. Regulatory frameworks for supervisory and enforcement activity*

***Authorities were asked which sets of rules and regulatory frameworks are most relevant to their supervisory and enforcement activity. Respondents could select multiple options from a list.***

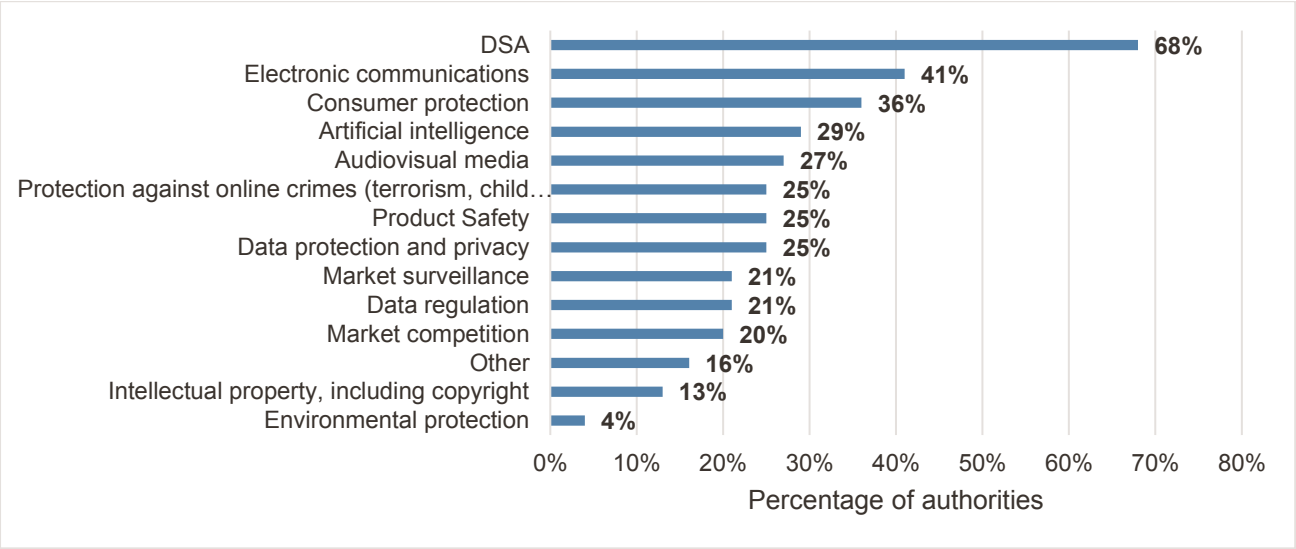
The DSA emerged as the most relevant framework for the concerned authorities, selected by 38 authorities (68% of respondents), followed by electronic communications (23 authorities, representing 41% of respondents), consumer protection (20 authorities, representing 36% of respondents), artificial intelligence and audiovisual media, each considered relevant by 16 authorities (29% of respondents).

Product safety, protection against online crimes, data protection and privacy, data regulation, and market surveillance were each considered relevant by 14 authorities (25% of respondents).

Environmental protection (4% of respondents) and intellectual property (13% of respondents) were the least relevant for the concerned authorities' activities.

Notably, 9 authorities (16%) selected the "Other" category and provided additional details about regulatory frameworks relevant to their supervisory and enforcement activities, such as postal services, energy regulation, and transport regulation.

***Figure 7. Relevance of regulatory frameworks to supervisory and enforcement activity (n=56)***




*1.2.3. Overlaps in EU regulatory areas*

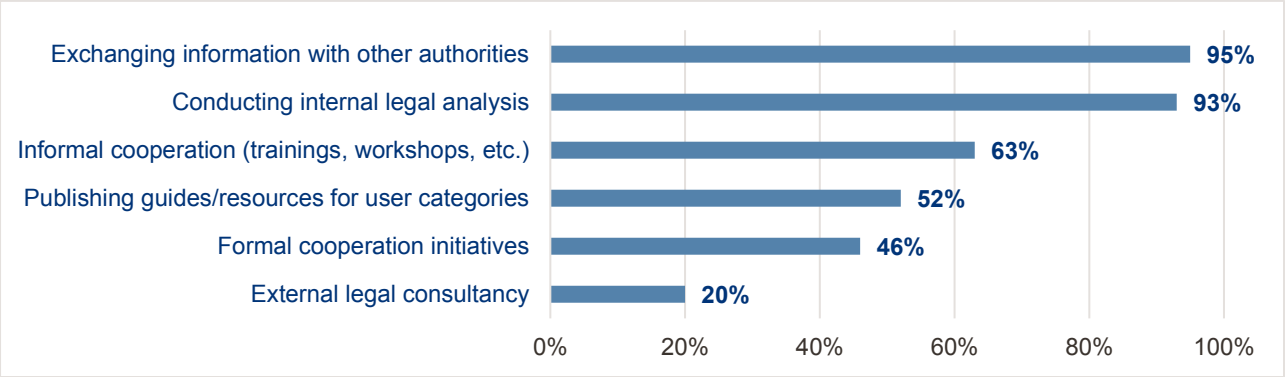
Authorities were presented with six predefined approaches and asked to select all that applied (i.e., approaches used) when addressing questions and situations at the intersection of multiple EU regulatory areas and legal instruments.

Nearly all authorities who responded to the survey reported exchanging information with other regulatory authorities (95%) and conducting internal legal analysis (93%) to address questions at the intersection of multiple EU regulatory areas.

Most authorities (63%) also reported using informal cooperation initiatives, such as trainings and workshops, while formal cooperation initiatives, such as official partnerships or memoranda of understanding, were reported by fewer authorities (46%). Most authorities (52%) also reported publishing guides and resources tailored to different user categories.

In contrast, external legal consultancy is relatively uncommon, with only 11 authorities (20%) seeking outside legal advice.

*Figure 8. Approaches used by authorities to address questions at the intersection of multiple EU regulatory areas (n=56)*

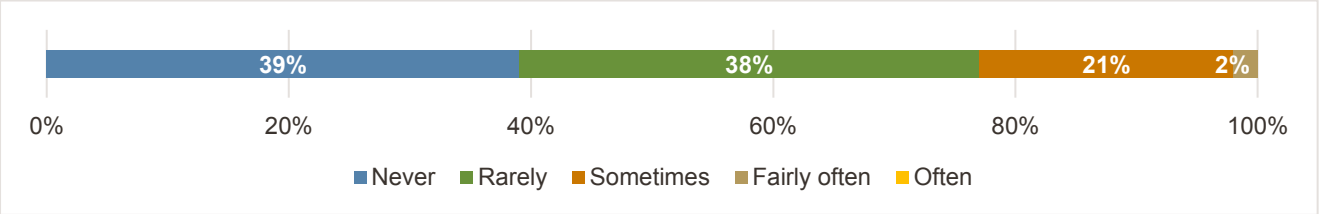



*1.2.4. Frequency of conflicts of competence between authorities*

The survey also explored **how often authorities found themselves in conflict with another authority**, particularly when both deemed themselves competent or approached the same actors and facts under separate Union law instruments. The results show that such conflicts are relatively uncommon for most authorities surveyed.

Most respondents (77%) reported either never or rarely finding themselves in a conflict of competence. A smaller proportion, 12 authorities (21%), reported that such conflicts occur "sometimes," while one authority (2%) indicated that conflicts of competence occur "fairly often".

*Figure 9. Reported frequency of competence conflicts between authorities under separate Union law instruments (n=56)*




Out of the 56 respondents, only 25 authorities provided detailed accounts of the types of conflicts of competence they have experienced, along with references to the relevant legislation and provisions. The responses reveal a spectrum of experiences, ranging from the absence of direct conflict to nuanced overlaps and interpretative challenges across regulatory domains, creating overlaps that require coordination to prevent duplicate or conflicting enforcement. Specifically:

**Data Protection and Privacy (GDPR, ePrivacy Directive):** Several authorities recounted negotiations with privacy-protection bodies over whether certain cookie-related measures that fall under the ePrivacy Directive's consent requirements or the GDPR's personal-data provisions.

Two authorities detailed repeated debates with youth-protection regulators over the design and enforcement of age-verification systems under Article 28 of the DSA, each emphasising either child-safety or data-protection safeguards (neither provided particulars of specific cases or identified the counterpart bodies).

One authority (from Slovakia) remains in an ongoing process to resolve competences under the ePrivacy Directive, though it did not specify which measures are still in contention. Another described conflicting interpretations of the legal framework for using US-based cloud services in light of GDPR obligations, without naming the interlocutor.

One authority (from Estonia) highlighted a gap in jurisdiction, noting data protection issues fall outside their remit and expressed concern about perceived inaction by the Data Protection Inspectorate.

**Data protection and consumer protection:** Two authorities identified a clear convergence between consumer-protection and data-protection regimes. One described how operators marketing services as "free" in exchange

for personal data – without obtaining explicit prior consent – risk falling foul of both the Unfair Commercial Practices Directive (2005/29/EC) (misleading omissions under Article 7) and the GDPR's consent requirements (Article 6(1)(a) and Article 7). The other recounted a conflict over spam regulation in which unsolicited electronic communications were subject both to the EECC's consent and information obligations (and corresponding national implementing rules) and to the GDPR's transparency and lawful-basis provisions; thanks to direct cooperation with the national Data Protection Authority, that tension has been successfully resolved in practice.

**Consumer protection**: One authority pointed out that its horizontal consumer-protection mandate under the Unfair Commercial Practices Directive (2005/29/EC) can sweep in exactly the same business practices that sectoral regulators oversee under specialised rules—yet it did not specify which sectoral bodies were involved. Similarly, in Latvia, the consumer-rights centre reported that enforcement of "dark patterns" under consumer law frequently coincides with the DSA's manipulation-technique provisions.

Italy's communications authority noted that, since the DSA's entry into force, other regulators competent under consumer-protection and unfair-practice statutes have begun to act on matters overlapping with DSA obligations – particularly on user interface design and misleading commercial terms – but offered no specific cases.

In Ireland, the national competition and consumer authority reported that traders face both consumer-law investigations and DSA inquiries in parallel, in part because the Irish DSC's working groups and DSA Wiki remain inaccessible to the consumer authority, creating "silos of information" and hampering coordinated action.

Other sectoral overlaps:

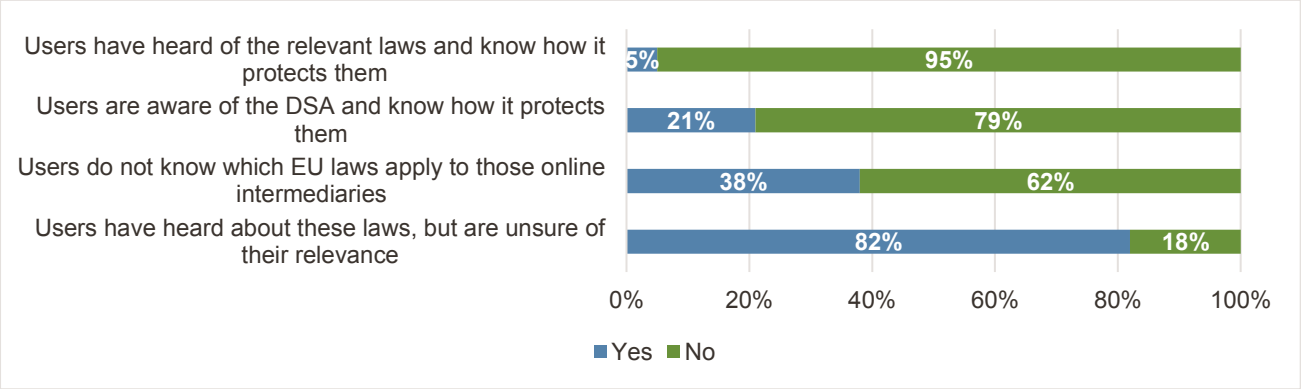
- One Czech authority explained that video-sharing platforms classified as very large online platforms under the DSA trigger simultaneous oversight by three bodies: the national audiovisual regulator (under its video-sharing-services law), the national Digital Services Coordinator (under DSA) and the European Commission, each empowered to take different actions.
- Belgium's postal and telecommunications regulator (BIPT) listed three specific overlaps: the e-Commerce Directive versus the DSA on online marketplaces; the Audiovisual Media Services Directive versus the DSA on video-sharing platforms; and Article 105(4) of the EECC versus the Unfair Terms in Consumer Contracts Directive (93/13/EEC) on unilateral contract changes.
- One authority from Finland pointed to challenges in product classification, such as distinguishing between novel foods, medicines, cosmetics, and medical devices, each governed by different EU legislation. To manage potential overlap with the UCPD and DSA transparency obligations, a horizontal consumer-protection authority reported having consolidated its teams and using single-lead investigations. Other mitigating practices reported by authorities include drafting national memoranda of understanding and joint notices to clarify any potential overlap and avoid duplication, as well as establishing permanent working groups.
- Finally, a Spanish ministry described conflicts of competence between its consumer-protection and sectoral regulators in the transport, telecommunications and financial sectors when abusive contractual clauses arise alongside DSA requirements.

*1.2.5. User awareness of Union law protections for online intermediary services*

Authorities were asked to evaluate users' awareness of the protections afforded to them under Union law when using online intermediary services.

While most authorities (82%) agree that users have at least heard of the laws that apply to them, they remain unsure of their relevance (18% disagree). Over one-third (38%) believe users do not know which EU rules apply to online intermediaries, and only one-fifth (21%) consider users aware of the DSA's protections. A mere 5 % feel that users both know the laws and understand how they protect them.

*Figure 10. Perceived understanding of Union law among users of online platforms (n=56)*

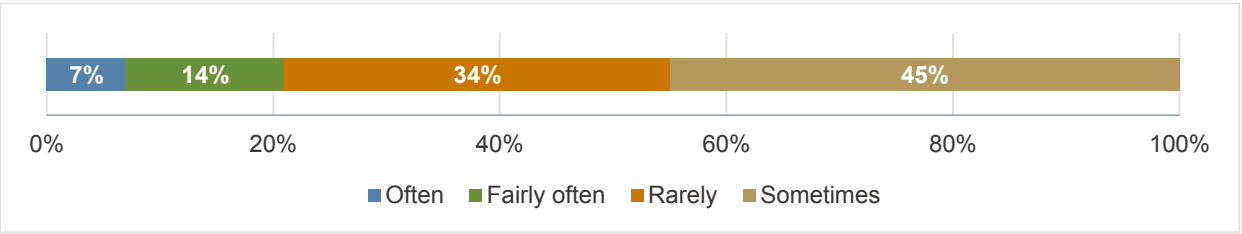



### *1.2.6. Incidence of misdirected user complaints among regulatory authorities*

Authorities were asked how often users file complaints, reports, or queries at an authority that is not competent to address their issue.

A fifth of authorities (21%) indicated "often" or "fairly often" receiving complaints, reports, or queries for which they are not competent. Almost half (45%) reported that this happened "sometimes" while a third (34%) considered that misdirected complaints happened "rarely".

*Figure 11. Frequency of misdirected user complaints to authorities (n=56)*




Fourteen authorities provided further detail in open comments on the frequency and nature of users filing complaints with the wrong authority. Among them, three authorities indicated that while they do receive some misdirected complaints, these are rarely concrete cases that clearly fall outside their remit. Instead, users often express dissatisfaction with enforcement or misunderstand which authority is responsible, particularly in complex areas such as online marketplaces.

Four authorities described established processes for handling misdirected complaints, including routine forwarding to other competent bodies such as national DSCs, consumer protection agencies, or the European Commission. One authority noted, "*These complaints are often transferred to the national Digital Services Coordinator as the complaints usually fall into its competency*." Another authority highlighted the benefit of internal structures, stating, "*80% of all complaints received do not constitute a breach of DSA but possibly of consumer law. Hence, they need to be forwarded to the team that deals with consumer protection within ACM*."

Quantitative data provided by five authorities illustrate the scale of the issue:

- One authority reported that, in 2024, over 40,000 inputs or notices were received, with 55 complaints transferred to other authorities by the Consumer Ombudsman.
- Another authority recorded 43 complaints or queries during 2024 and 70 since the beginning of 2025.
- One authority reported having received three DSA-related complaints, all of which were forwarded to the Digital Services Coordinator.
- Another noted fewer than 10 misdirected DSA queries since the DSA's entry into force.

- The Irish CCPC signposted 40 helpline contacts to the Irish Digital Services Coordinator since 2023, and 523 to the Irish Data Protection Commission, illustrating the breadth of issues users raise with the wrong body.
- Three authorities highlighted the complexity of complaints, noting that some cases are only partially within their competence, particularly where issues overlap with criminal law (e.g., hate speech or fraud). One authority observed, "*For example, in case of hate speech, the victim has to file a complaint with the police to seek criminal prosecution of the offender – while our authority may at the same time check whether the online platform fulfilled its duties under the DSA*."

*1.2.7. Most frequently competent authorities for misdirected user complaints*

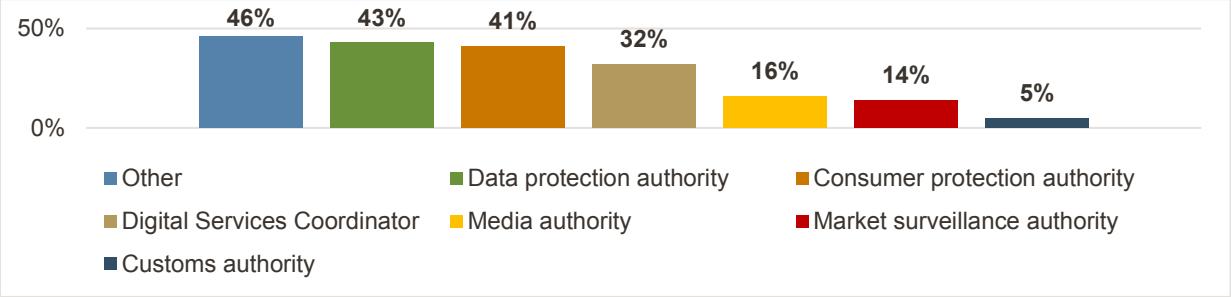
Respondents were asked to identify which other authorities are most often the correct contacts when users mistakenly reach out to the wrong authority. Please note that this question allowed for multiple selections; therefore, the total percentage may exceed 100%.

When asked which other authorities are most frequently competent instead, data protection authorities (43%) and consumer protection authorities (41%) were the most commonly cited, followed by Digital Services Coordinators (32%). Media authorities, market surveillance authorities, and customs authorities were cited less often (16%, 24% and 5% respectively).

Notably, nearly half of the respondents (46%) selected "Other," with 21 authorities providing further details in open comments:

- Law enforcement and criminal justice bodies: A significant majority – 13 out of 21 authorities (61%) – explicitly mentioned police forces, law enforcement agencies, or authorities involved in criminal proceedings as the appropriate bodies for certain complaints.
- Sector-specific and financial authorities: Six authorities pointed to sector-specific regulators or financial bodies as the appropriate destination for certain complaints.
- Regional and executive authorities: Two authorities noted that, in some cases, executive powers have been delegated to regional authorities, making them the competent body to act.

***Figure 12. Distribution of authorities most frequently identified as competent for misdirected user complaints (n=56)***




*1.2.8. Main causes for authorities being contacted instead of the competent authority*

**Authorities were invited to suggest in open comments the main reasons why they are contacted instead of the competent authority**. 52 authorities responded, often mentioning more than one reason. The most prevalent ones were: lack of user awareness (32 authorities), the complexity and overlap of regulatory frameworks (18 authorities), and misunderstandings about specific competences and legislation (15 authorities). The expectation that a single authority can address all digital issues (13 authorities), national and sectoral contexts (8 authorities) and unclear definitions were also identified (7 authorities).

These findings were further elaborated in the comments provided by authorities, who described the main causes in more detail:

**Lack of user awareness and legal knowledge**: The most frequently cited cause is users' insufficient knowledge of which rules apply to their specific cases and which authority is competent. Authorities repeatedly noted that users "*do not have sufficient knowledge about legislation and competent authorities on national level*" and that "users are not informed in detail about the competences of the authorities." This is compounded by the complexity of the digital regulatory landscape, with many users unaware of the distinction between, for example, the DSA, GDPR, and sector-specific regulations.
A few authorities mentioned ongoing efforts to improve public awareness, such as dedicated contact forms, public campaigns, and information services. However, they acknowledged that "levels of awareness and understanding are nascent and vary," and that improving user understanding is a long-term process.

**Complexity and overlap of regulatory frameworks**: Many authorities highlighted the "*complex and often interwoven landscape of regulatory oversight and competence*" as a major source of confusion. The introduction of the DSA, in particular, has increased the complexity, with users struggling to distinguish between breaches of the DSA, illegal content, and other regulatory issues. As one authority put it, "*the narrative of the DSA is very hard to explain to an average user/consumer, in combination with the fact that the societal expectations of the DSA are very high (usually without proper in-depth* knowledge *of the specific obligations under the DSA)*."

**Users' tendency to seek a single point of contact**: Authorities have observed that users often expect one authority to handle all issues related to digital platforms, regardless of the nature of the complaint. This leads to authorities being contacted for matters outside their remit, such as criminal offences, consumer disputes, or data protection issues. One authority noted, "*users often prefer to have a single point of contact for all types of services, regardless of the nature of their complaint*."

**Misunderstanding of specific competences and legislation**: There is widespread confusion about the boundaries of different authorities' competences and the specific legislation that applies. For example, users may file a complaint about a closed account as both a DSA and GDPR issue, or may not understand the difference between sectoral and general consumer protection rules. As one authority explained, "*the fact that consumers don't know which legislation applies and which authority supervises the relevant legislation*" is a recurring issue.

**National and sectoral contexts**: Some authorities pointed out that their broad remit or prominent public profile leads users to contact them by default. For example, the CCPC in Ireland is widely perceived as the primary source of information on consumer rights, while the Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection in Austria is well known for consumer protection issues. In some countries, the division of executive powers between national and regional authorities adds another layer of complexity.

**Unclear or evolving definitions**: Authorities also cited uncertainty about what constitutes an "*intermediary service*" or which procedures and outcomes are available under the DSA. This lack of clarity further contributes to misdirected complaints.

**Expectation of immediate action**: Some authorities noted that users expect rapid moderation or intervention, particularly regarding individual pieces of content, without realising that the authority's mandate may focus on systemic issues rather than individual cases.

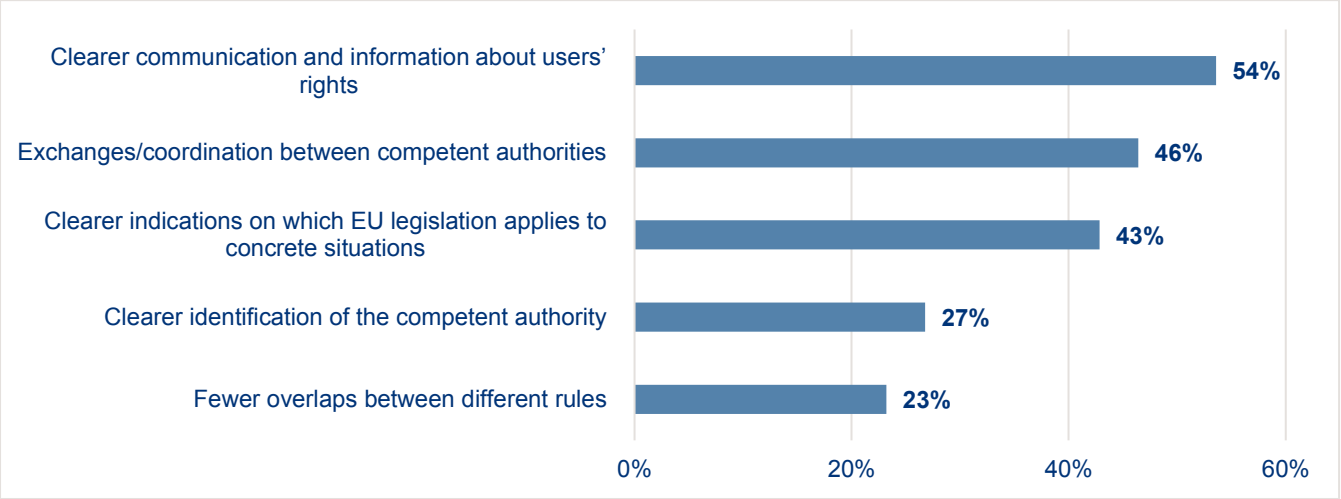
#### *1.2.9. Factors to facilitate the correct applicability, supervision, and enforcement of EU rules on online services*

Respondents were provided with a list of options and asked to identify the most important factors to facilitate the correct applicability, supervision, and enforcement of EU rules on online services.

The most significant factor identified by authorities was clearer communication and information about users' rights, which was selected by 30 authorities (54%). Exchanges and coordination between competent authorities were also highlighted as a major factor, with 26 authorities (46%) identifying this as important.

Clearer indications on which EU legislation applies to concrete situations were identified by 24 authorities (43%), while the need for clearer identification of the competent authority was raised by 15 of them (27%). 13 authorities (23%) pointed to the need for fewer overlaps between different rules.

*Figure 13. Most important factors for effective enforcement of EU rules on online services (authorities' perspectives) (n=56)*




### *1.2.10. Conflicting, contradictory, or overlapping provisions resulting from the DSA and other Union law instruments*

Authorities were asked whether they had identified any conflicting, contradictory, or overlapping provisions resulting from the DSA and its interplay with other Union law instruments. Out of 56 authorities, 28 reported having identified overlapping provisions, while 6 authorities indicated the presence of conflicting or contradictory provisions. Among them, 27 authorities provided further details in open comments, mentioning the following overlaps:

**Unfair Commercial Practices Directive (UCPD):** Nine authorities (32%) flagged the overlap between the DSA's prohibition of manipulative interface design (Article 25) and the UCPD's ban on misleading and aggressive commercial practices (Article 5). One authority further specified that the current wording of Article 25 of the DSA fails to distinguish clearly between dark patterns under the DSA and unfair commercial practices under the UCPD, leaving uncertainty as to which regulator – consumer-protection or data-protection – should take the lead.

**General Data Protection Regulation (GDPR):** Seven authorities (25%) described friction between DSA obligations and GDPR requirements, particularly where the same conduct triggers both sets of rules. In several cases, reuse of user data through recommender systems (Article 27 of the DSA) was said to overlap with GDPR transparency and consent provisions (Articles 6–7), prompting concurrent investigations by Digital Services Coordinators and Data Protection Authorities. Others pointed to confusion over whether notice-and-action duties under Article 18 of the DSA conflict with GDPR breach-notification obligations. Two respondents welcomed the forthcoming European Data Protection Board guidelines on DSA–GDPR interplay but did not supply concrete examples of dual enforcement.

**Audiovisual Media Services Directive and National Media Laws (AVMSD):** Four authorities (14%) highlighted that video-sharing platforms designated as very large online platforms under the DSA also fall within the scope of the AVMSD (Directive 2010/13/EU) as transposed into national law. Each body – the national audiovisual regulator, the Digital Services Coordinator and the European Commission – holds its own powers. In addition, five authorities raised the protection-of-minors provisions in Article 28 of the DSA, noting that national youth-protection frameworks and AVMSD child-safety rules both apply. One further respondent observed a regulatory gap for smaller platforms that do not qualify as VLOPs and sit outside AVMSD coverage.

**e-Commerce Directive**: Two authorities expressed uncertainty about the country-of-origin principle in Directive 2000/31/EC and its interaction with the DSA's liability exemptions for intermediaries not established in the host Member State. Two respondents mentioned these overlaps without specifying the procedural conflicts or case examples involved.

**Platform-to-Business Regulation (P2B):** Two authorities pointed to potential conflicts between transparency and traceability provisions in the DSA (notably Articles 26, 27 and 30) and the new Platform-to-Business Regulation (EU 2024/900), particularly Articles 19(1)(b) and (c).

**Consumer Rights Directive (CRD):** One authority noted that Article 12 of the DSA on points of contact mirrors Article 6(1)(c) CRD on pre-contractual information and Article 5(1) ECD; that recommender-system transparency under Article 27 DSA corresponds to Article 6a(1)(a) CRD; and that trader-traceability obligations in Article 30 DSA overlap with Articles 6 and 6a CRD on seller identity.

**General Product Safety Regulation (GPSR):** One authority cautioned that Article 22 of the GPSR, which governs the safety of products placed on the market, overlaps with the DSA's obligations for very large online platforms to monitor and mitigate systemic risks. It explained that, in cases of unsafe products sold online, it is unclear whether the Commission or a national market-surveillance authority should take the lead on corrective measures.

**AI Act**: A single respondent observed that "dark patterns" are defined both in the AI Act (Regulation 2024/1689) and the DSA, creating enforcement uncertainty as to whether Digital Services Coordinators, Data Protection Authorities or the newly designated AI regulators should police AI-driven manipulative design. No specific AI-powered platform cases were cited.

**Audiovisual Media Freedom Act and Political-Advertising Rules**: One authority flagged overlaps between DSA content-monitoring provisions and the Audiovisual Media Freedom Act's rules on removal of harmful content (Article 18), as well as between DSA advertising requirements and national political-advertising-transparency obligations.

**Brussels I Regulation**: One respondent questioned how the service-and-compliance orders under Articles 9–10 of the DSA should be transmitted and enforced in light of Brussels I Regulation rules on cross-border service of judicial and extrajudicial documents. Without practical examples, it remains unclear whether delivery via the DSA's electronic contact point satisfies the Regulation's service-of-documents requirements.

*1.2.11. Suggestions to facilitate the applicability and clarity of the EU regulatory Framework*

A total of 40 authorities provided suggestions aimed at improving the applicability of the EU regulatory framework for online intermediary services and clarifying its interplay with other Union law. The responses received highlight several recurring themes and practical recommendations:

**Clearer communication, guidance and practical examples**: The most common theme, mentioned by 22 authorities, was the need for clearer, more accessible communication and guidance from the European Commission and other EU bodies. Respondents repeatedly called for the publication of practical guidelines, interpretative documents, and concrete examples to help both authorities and service providers understand how the DSA and other relevant legislation should be applied in practice.

**Enhanced coordination/cooperation among authorities**: Coordination and cooperation between competent authorities, both at the national and EU levels, was highlighted by 17 authorities. Suggestions included the establishment of formal cooperation frameworks, joint interpretation efforts, and harmonised methodologies to ensure consistency in enforcement and avoid duplication or gaps in oversight.

**Clarification of competences/roles and central contact points**: Eleven authorities specifically requested more clarity regarding the division of competences and the roles of different authorities, including the establishment of central contact points and the mapping of responsibilities.

**Streamlining/harmonising definitions across legal instruments**: Ten authorities emphasised the importance of streamlining and harmonising definitions across different legal instruments, with several noting that the frequent use of phrases such as "*without prejudice to the GDPR*" does not resolve practical conflicts or overlaps.

**More case law, best practices, and practical examples**: Several authorities also mentioned the need for more case law, practical examples, and best practice sharing to support consistent interpretation and application.

**Other specific suggestions**: Other suggestions included strengthening cross-border enforcement, clarifying the handling of notice mechanisms, and ensuring that the needs of specific sectors (such as agri-food, education, and media) are taken into account. A small number of authorities noted that it was too early to provide detailed suggestions, as practical experience with the DSA was still limited.

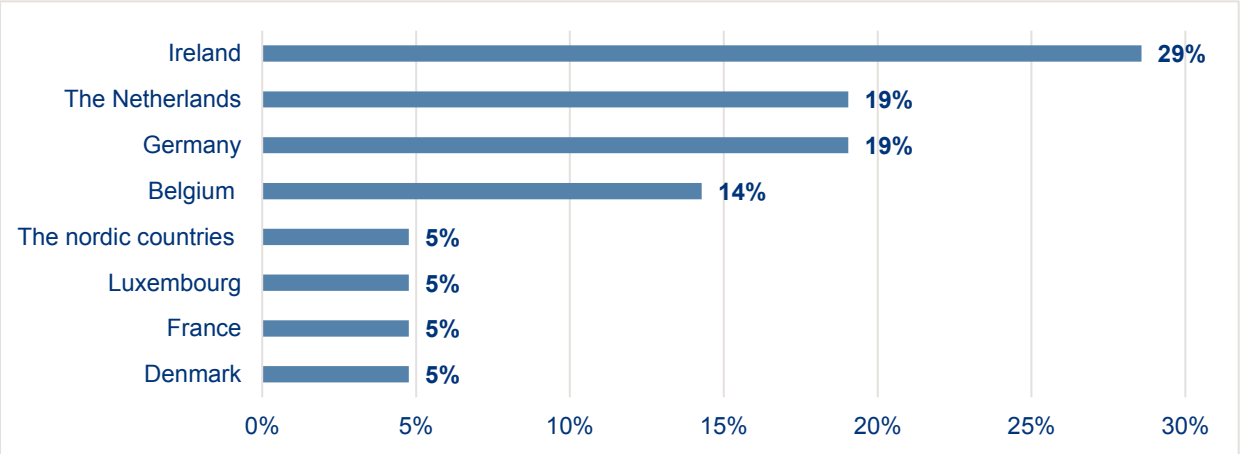
### 1.3. Online intermediaries, in particular VLOPs and VLOSEs

#### *1.3.1. Profile of respondents*

A total of 21 intermediaries responded to the survey and one additional VLOP responded via email with a position paper.

The survey received responses from a range of platforms and business associations, with the majority of respondents based in Ireland (6, 29%), followed by Germany and the Netherlands (4 each, 19%), Belgium (3, 14%), and single respondents from Denmark, France, Luxembourg, and the Nordic countries[169].

***Figure 14. Distribution of respondents by Member State of main establishment (n=21)***

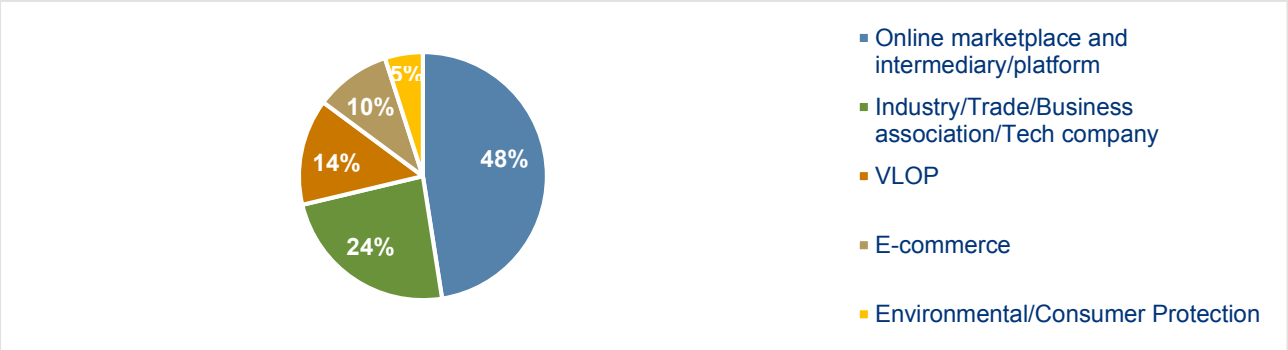



Nearly half of the respondents (10, representing 48%) self-identified as online marketplaces or intermediary/ platform services. 5 respondents (24%) self-identified as industry, trade, business associations, or technology companies. 3 respondents (14%) self-identified merely as VLOPs. E-commerce services were self-identified by 2 respondents (10%), and one respondent (5%) reported being from the environmental/consumer protection sector.

Despite the self-identification of the respondents, in practice, 11 respondents (52%) are VLOPs, designated as such by the European Commission.

[169] One respondent represented multiple organisations and provided "Nordic countries" as their response. This includes the Danish Chamber of Commerce, the Swedish Chamber of Commerce, the Finnish Commerce Federation, the Federation of Norwegian Enterprises, and the Federation of Trade and Services (Iceland).

*Figure 15. Distribution of respondents by self-identified type of service (n=21)*




In terms of operational scope, the majority of respondents indicated EU-wide coverage (15 out of 21). A smaller number of respondents operated at the national level (3). There were also multi-country platforms (2), whose services spanned several Member States but did not claim full EU-wide reach.

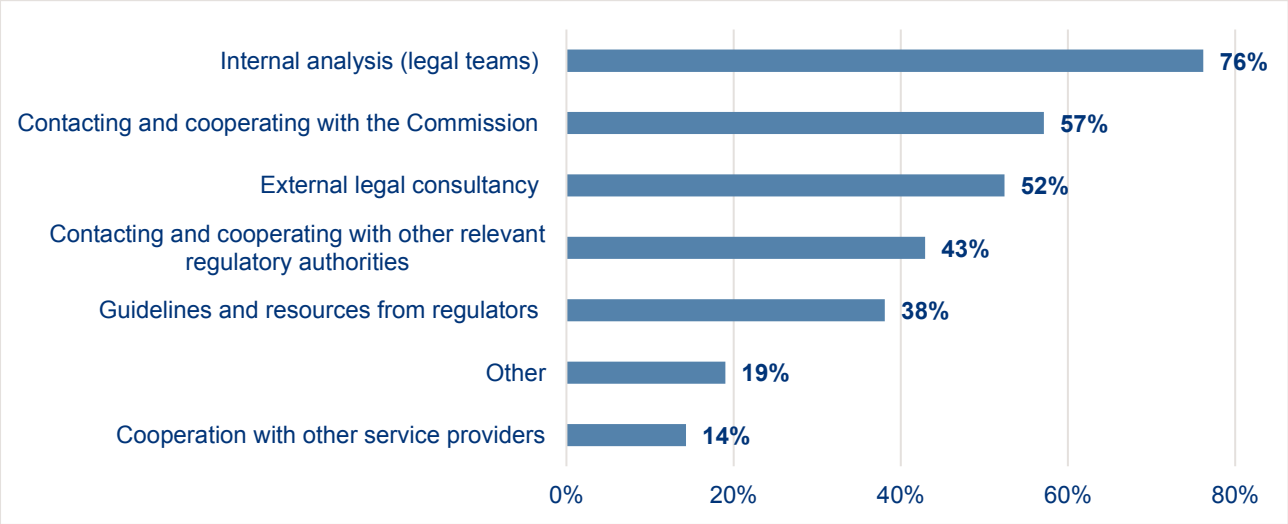
*1.3.2. Approaches to situations at the interface of several EU regulatory areas*

Respondents were asked about the main ways in which they or their members approach current and emerging situations or practices at the interface of several regulatory areas and Union law instruments.

Among the different options available, the most common approach selected was internal analysis by legal teams, cited by 16 out of 21 respondents (76%). A majority also reported contacting and cooperating with the European Commission (12 respondents, 57%) and using external legal consultancy (11 respondents, 52%).

Contacting and cooperating with other relevant regulatory authorities was mentioned by 9 respondents (43%), and Guidelines and resources from regulators by 8 respondents (38%). A smaller number of respondents reported cooperation with other service providers (3 respondents, 14%).

*Figure 1616. Approaches used by providers to address multi-regulatory situations (n=21)*

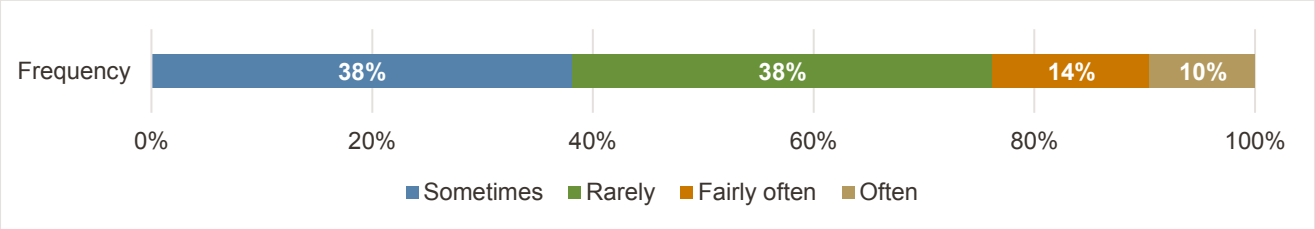



*1.3.3. Frequency of conflicts of complaints submitted to the wrong department/contact point*

Respondents were asked how often a complaint, report, or query filed by users to enforce their rights online is submitted to the wrong department, compliance unit, or contact point and needs internal reassignment or re-submission.

The most common responses were “sometimes” and “rarely,” each selected by 8 out of 21 respondents (38%). A smaller proportion of respondents reported that this happens “fairly often” (3 respondents, 14%) or “often” (5 respondents, 10%).

*Figure 1717. Reported frequency of complaints submitted to the wrong department or contact point (n=21)*




Out of the 21 respondents, only 9 provided further detail in open comments. The responses reveal a range of experiences:

**Quantitative insights**: Two respondents provided figures. One, an online marketplace, reported that "in 35–40 percent of the notices, the stated subject of the violation is incorrect. As a result, the cases need to be rerouted." They also noted that "in 25% of the notices submitted by sellers, they submit the notice to the wrong contact point." Another, a technology- and- digital- services respondent, stated that misdirected complaints occur "4–10 times a week".

**Qualitative insights**: One VLOP noted that authorities occasionally bypass official channels by contacting employees directly or reaching out to subsidiaries, which can add complexity and increase processing times.

Another online intermediary described a positive development, explaining that the legal clarity introduced by the DSA has enabled their organisation to enhance transparency and improve processes for users. As a result, they have observed a general decrease in the number of user submissions that are incorrectly assigned internally.

Two respondents indicated that the issue of misdirected complaints is not relevant to their operations. For example, a business association stated that they do not deal with such complaints and have no information on the topic, while a technology and digital services association reported that this does not apply to them. Similarly, one online intermediary service provider simply stated "Never," indicating that they do not experience misdirected complaints. Another VLOP noted that they do not track misdirected complaints in the ordinary course of business, so specific figures are not available.

Finally, one online intermediary highlighted the challenge of distinguishing between regulatory complaints and general customer service queries. They explained that platforms often receive a wide array of user communications through shared complaint channels, which are sometimes overrun with non-DSA-related queries, such as customer service issues like reservations or account management.

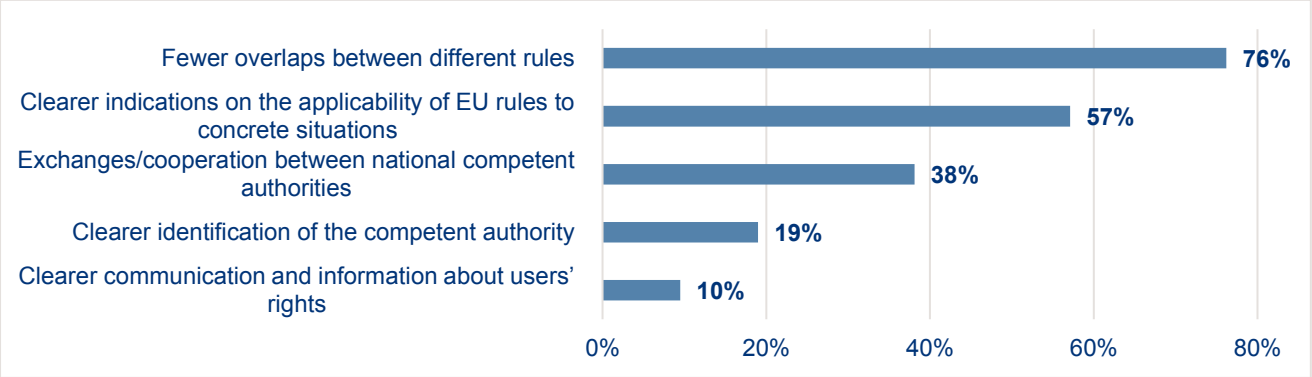
### *1.3.4. Factors to facilitate correct applicability, supervision, and enforcement*

VLOPs and other platforms were asked to assess what is most important to facilitate the correct applicability, supervision, and enforcement of EU rules on online services.

Respondents most frequently highlighted the need for fewer overlaps between different rules (76%) and clearer indications on the applicability of EU rules to concrete situations (57%).

Exchanges and cooperation between national competent authorities was also identified as important by over a third of respondents (38%) and the need for clearer identification of the competent authority (19%) and clearer communication and information about users' rights (10%).

*Figure 18. Most important factors for effective enforcement of EU rules on online services (n=21)*



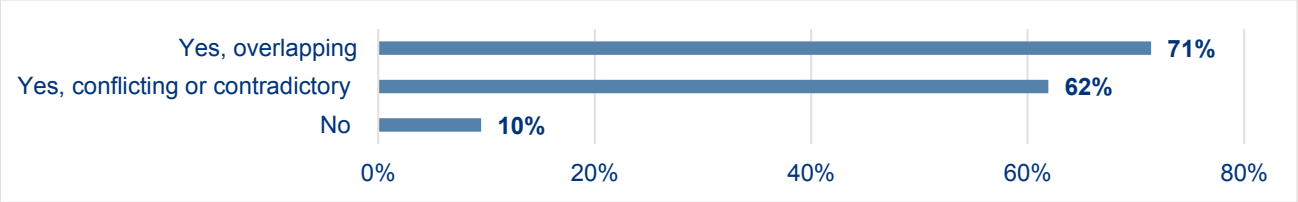

*1.3.5. Identification of conflicting, contradictory, or overlapping provisions*

VLOPs and other platforms were presented with a multiple-choice question asking whether they have identified any conflicting, contradicting, or overlapping provisions resulting from the DSA and its interplay with other Union law instruments.

Most respondents (15, representing 71%) indicated that they had identified overlapping provisions, while 13 respondents (62%) reported conflicting or contradictory provisions. Only 2 respondents (10%) stated that they had not encountered any such issues.

Among the 21 responses received, 6 respondents provided specific examples illustrating the practical difficulties created by these overlaps and inconsistencies.

*Figure 19. Prevalence of overlapping and conflicting provisions identified by online platforms under the DSA (n=21)*




In open comments, six respondents' provided concrete examples:

**General Product Safety Regulation (GPSR):** Two online marketplaces and one e-commerce retailer pointed to tensions between the DSA's contact-point and traceability obligations and those in the GPSR:

The first marketplace noted that DSA Articles 11–12 (central contact points for authorities and consumers) overlap with GPSR Articles 22(1) and (2), both requiring platforms to appoint designated points of contact. It also flagged DSA Article 31 vs. GPSR Article 22(9), where the mandatory "responsible economic operator" contact details differ.

The second marketplace observed confusion under DSA Articles 3 and 6 (definition and limited liability of marketplaces) and GPSR Articles 4 and 22 (manufacturer/importer/distributor duties), as well as misalignment between illegal content notices (DSA) and safety recall notices (GPSR). The e-commerce respondent described duplicative "Know-Your-Business-Customer" rules under DSA Article 31 and GPSR Article 22, which impose parallel trader-verification and product-traceability burdens.

Both online marketplaces reported interpretative conflicts between DSA Article 25 (prohibition of dark patterns) and GDPR/EDPB guidelines (dark-patterns definitions), together with national financial-services distance-contract rules. One emphasised fragmentation of "dark patterns" obligations across the DSA, GDPR and UCPD.

**Consumer Rights Directive (CRD):** One marketplace cited overlaps of DSA Article 27 (recommender-system transparency) with CRD Article 6a(1)(a) on pre-contractual information and with UCPD misleading-practices

rules. Another respondent (the industry association) proposed that forthcoming Digital Fairness legislation may contradict existing CRD/DSA consumer-information standards on personalisation and design.

**Platform-to-Business Regulation (P2B):** One online marketplace observed that DSA Article 27 (recommender systems) and P2B Article 5 both impose ranking-transparency duties that are not fully aligned, creating uncertainty over which framework takes precedence.

**Customs and Trade-Related Instruments:** The industry association and the e-commerce retailer each warned that the Union Customs Code reform's "deemed importer" status for marketplaces[170] contradicts DSA Articles 2 & 6 (marketplace liability) and GPSR's exclusion of marketplaces from the product-safety chain. Both urged alignment of future trade-law reforms with the DSA liability regime.
The online-platform respondent also highlighted DAC7's customer-due-diligence data-collection requirements as parallel—but not identical—to DSA Article 11 electronic-contact-point obligations, leading to repeated requests for slightly different data fields.

**Fitness Check of EU consumer law on digital fairness / forthcoming Digital Fairness Act:** The industry association and the e-commerce respondent flagged that measures on dark patterns, addictive design and subscription management that may be proposed in the forthcoming "Digital Fairness Act" could duplicate or exceed what DSA Articles 25–28 already cover, risking over-legislation and enforcement confusion.

**Audiovisual Media Freedom Act (EMFA):** The industry association reported that the EMFA treats self-declared media service providers differently under content-moderation rules, allowing 24-hour challenges outside the DSA's systemic-risk regime—presenting a direct conflict over moderation standards for the same content.

**Protecting Minors (DSA Article 28):** Both the e-commerce retailer and the tech/digital association called for a risk-based approach, noting that uniform age-verification and default-restriction duties impose disproportionate burdens on low-risk or payment-based platforms.

**Transparency and Reporting Obligations:** The e-commerce respondent and the tech/digital association criticised the DSA's transparency-report templates (Articles 15 & 42) as overly granular and resource-intensive, advocating a tiered, risk-proportionate model.

**Artificial Intelligence Act:** The tech/digital association identified a mismatch between the AI Act's broad definition of "systemic risk" (Art 3(65)) and the DSA's more circumscribed risk-assessment requirements (Art 34), resulting in duplicated or misaligned harm-assessment processes.

**Short-Term Rental Regulation (STR):** The tech/digital association also noted that the STR Regulation's information-and-takedown procedures (Arts 5–6) lack the procedural safeguards of DSA Article 11 (use of platforms' electronic contact points), creating enforcement inconsistency.

*1.3.6. Compliance costs linked to overlapping/inconsistent obligations*

Respondents were asked if they could point to any internal estimations of compliance costs linked to obligations deemed to be overlapping and/or inconsistent with others. Most respondents indicated that they either do not have such figures available or have not conducted formal analyses isolating these costs. Some noted the complexity and resource intensity required to produce such estimates, noting that the effort itself would further strain limited resources. Only a few provided quantitative estimates or qualitative insights.

Despite the absence of exact figures, several respondents highlighted that a significant portion of internal resources—particularly legal, IT, and compliance teams—are devoted to navigating overlapping regulations. Estimates provided by a few respondents suggest that between 15% to 20% of IT resources are currently devoted to implementing new legislation, often at the expense of innovation. One respondent noted that GDPR-DSA overlaps now consume around 5-15% of the working capacity of their internal lawyers, with expectations that

[170]The Customs reform proposal is currently under negotiation.

this could rise to 20-30% as familiarity with the DSA increases. Others similarly reported significant increase in overall compliance costs directly attributable to new digital regulations, particularly the DSA. Industry sources cited by respondents suggest that up to 30% of EU tech companies' resources may be consumed by compliance due to regulatory complexity and overlapping rules.

Many respondents described the significant indirect costs associated with overlapping obligations, including increased legal and compliance resource allocation, duplicated internal review processes, and delays in decision-making due to uncertainty about which legal instrument takes precedence. Several highlighted that the lack of clarity and legal certainty results in longer compliance processes, potential escalations with authorities, and ultimately, a negative impact on user experience and innovation. These challenges were reported as particularly acute in areas requiring rapid responses, such as product safety and content moderation.

The burden of overlapping and inconsistent regulations was seen as a structural barrier, especially for European digital and e-commerce companies and start-ups with fewer resources compared to large international competitors. Several organisations also pointed out that unclear or contradictory obligations increase legal risk and the potential for non-compliance, which can result in sanctions or disputes despite best efforts to comply.

VLOPs and other platforms provided suggestions aimed at facilitating the applicability of the EU regulatory framework for online intermediary services or to clarify its interplay with other Union law. Respondents overwhelmingly called for clearer, more harmonised, and practical regulation, with improved guidance, coordination, and ongoing dialogue to address the complexities and overlaps in the current EU digital regulatory landscape:

**Harmonisation and streamlining of rules**: A prominent theme to emerge from the 21 responses was the need for greater harmonisation and streamlining of the regulatory landscape. Fourteen providers expressed concern about the proliferation of overlapping and, at times, contradictory obligations resulting from the DSA and other EU legal acts. They noted that platform responsibilities are currently dispersed across multiple legislative instruments, which can lead to legal uncertainty and increased compliance burdens. Several respondents called for clearer delineation of responsibilities and a more harmonised approach to rulemaking, which would help to reduce unnecessary duplication and administrative complexity.

**Clearer guidance and communication**: Respondents highlighted the importance of clear, practical guidance and communication from the European Commission and relevant regulators. Many called (12 respondents) for the publication of detailed FAQs, best practice documents, and explanatory notes to assist providers in navigating the complex interplay between the DSA and other EU rules. While the DSA's aim of creating a harmonised framework was widely welcomed, respondents stressed that its effectiveness depends on the availability of timely and practical interpretative support. Regular updates and clarifications were also suggested as valuable, particularly as the regulatory environment continues to evolve.

**Coordinated enforcement**: Another recurring suggestion was the need for more coordinated enforcement and supervisory mechanisms across Member States. Several providers (9) advocated for a "one-stop shop" approach, especially for cross-border services, to streamline compliance and reduce the risk of inconsistent enforcement. It was argued that a coordinated approach to supervision would not only benefit service providers operating in multiple jurisdictions but also enhance legal certainty and user trust across the EU.

**Assessment/review of existing frameworks**: Seven respondents also urged the Commission to assess and review the effectiveness of the existing regulatory framework before introducing new requirements. There was a clear caution against the risk of regulatory overreach, with calls for new rules to be outcome-oriented, practical, and mindful of the cumulative burden on businesses. Some noted that the current complexity makes it difficult to quantify compliance costs but emphasised that the impact on resources and innovation is significant.

**Flexibility and proportionality**: The principle of proportionality and flexibility was another important theme. Six respondents emphasised that the regulatory framework should be adaptable to the size, nature, and business

model of different online intermediary services. There were calls for rules that are not only proportionate to the risks posed but also flexible enough to accommodate technological and market developments.

**Regular dialogue with stakeholders:** Five respondents advocated for ongoing dialogue and engagement between regulators, service providers, and other stakeholders. Regular exchanges were seen as essential to identify practical challenges, share solutions, and ensure that the regulatory framework remains relevant and effective in a rapidly changing digital landscape.