Authority for Consumers & Markets

Public

Consultation version of DSA Guidelines

Due diligence obligations for digital services

Markets that work well for people and businesses

ACM/UIT/609343

Summary: DSA Guidelines regarding due diligence obligations for digital services

The Digital Services Act (DSA) aims to ensure a safe, predictable, and trustworthy online environment, in which the rights of all recipients of intermediary services are protected. In these Guidelines, ACM provides additional explanations and practical examples to guide intermediary service providers on various obligations arising from the DSA. The aim is to promote compliance with the obligations.

When are you an intermediary service provider?

You are an intermediary service provider if you provide a digital service that, at the request of recipients of your service, enables information to be stored, transmitted, and/or disclosed to third parties. The DSA imposes various obligations on the following intermediary services:

- **Mere conduit service**

This is a service that transmits information provided by a recipient of the service via a communication network or provides access to a communication network.

Examples of mere conduit services: internet access services, internet exchange points, wireless local networks, virtual private networks, and voice over IP services.

- **Caching service**

This is a service that transmits information provided by a recipient of the service via a communication network, where the information is stored automatically, temporarily, and briefly to make the transmission of information to other recipients of the service more efficient.

Examples of caching services: content delivery networks and proxy services.

- **Online search engine**

This is a service that enables users to enter queries in order to perform searches of, in principle, all websites or all websites in a particular language.

- **Hosting service**

This is a service that consists of storing information at the request of recipients of the service, such as websites, photographs, or applications.

Examples of hosting services: Cloud computing, web hosting, search engine advertising services, electronic marketplaces, social networks, and video-sharing platforms.

- **Online platform**

This is a hosting service that stores and disseminates information to the public at the request of the recipient of the service.

Examples of online platforms: B2C online marketplaces, social networks, and app stores.

- **B2C online marketplace**

This is an online platform that offers consumers the possibility of concluding a distance contract with a trader.

What obligations does the DSA impose on intermediary service providers?

The DSA imposes various obligations on intermediary service providers. Since the DSA has a tiered system of obligations, not all obligations apply to intermediary service providers. In these Guidelines, ACM provides guidance on these obligations, which can be broadly classified within the themes below.

Theme 1 — Addressing illegal content

The DSA places various responsibilities on online intermediary service providers to combat illegal content because, consciously or unconsciously, they play a role in its dissemination. Illegal content is a broad concept that can take many different forms. It can refer to content that in itself violates the law, such as child pornography or discriminatory content, but also content where the illegality is not inherent in the information itself, but in the way in which it is disseminated. Examples include scams, malware, and the sale of counterfeit products. The DSA does not impose a general monitoring obligation on intermediary services but creates a system of due diligence obligations to prevent illegal content and render it inaccessible as quickly as possible. The DSA thus aims to strike a balance between limiting the risks of disseminating illegal content, the resources of online intermediary service providers, and the rights of recipients of the service, because imposing restrictions on recipients of the service can also have significant negative consequences. The DSA therefore imposes the following obligations:

Intermediary service providers must:

- Include in their terms and conditions intelligible information on restrictions they impose with regard to information provided by recipients of their service.
- Such information includes information on policies, procedures, measures, and tools used for content moderation.

Hosting service providers must:

- Enable individuals or organizations to notify illegal content on their service by means of a user-friendly mechanism.
- Make decisions on such notices in a timely, diligent, non-arbitrary, and objective manner.
- Give recipients of their service clear reasons for their decisions to impose restrictions. They must also state the available possibilities for redress.

Online platform providers (excluding micro and small enterprises) must:

- Suspend recipient of their service who frequently provide manifestly illegal content. The same applies to recipient of their service who frequently submit manifestly unfounded complaints.
- Process and deal with notices from trusted flaggers (certified organizations that identify illegal online content) concerning the presence of illegal content as a priority and as quickly as possible.

Theme 2 — Protection of minors

The DSA aims to ensure a safe and transparent online environment to protect vulnerable recipient of services, such as minors. In addition to the general due diligence obligations, the DSA imposes two due diligence obligations on intermediary service providers that are explicitly intended to protect minors.

Intermediary service providers must:

Explain the conditions for both the use of the service and the restrictions on the use of the service in a way that minors can understand. This applies if the intermediary service is primarily aimed at, or is predominantly used by, minors.

Online platform providers (except micro and small enterprises):

Must take measures to ensure a high level of privacy, safety, and protection of minors. This applies if the online platform is accessible to minors.

Must not display advertising based on profiling if they are aware with reasonable certainty that their service is being used by minors.

Theme 3 — Rights of recipients

As an intermediary service provider, you may decide to impose restrictions on the use of your service. For example, if you suspend a recipient's account after you have determined that the recipient of the service has provided illegal content or has violated the terms and conditions. Since such decisions have a major impact on recipients, the DSA enables recipients to object, for example by filing a complaint. To this end, the DSA imposes the following obligations.

Intermediary service providers must:

Include information on the operation of the internal complaint handling system in their terms and conditions.

Hosting service providers must:

- Inform individuals and organizations that notify illegal content of the decision concerning the handling of the notice.
- Provide recipients of the service a statement of reasons if they decide to restrict recipients' use of their service.

Online platform providers (excluding micro and small enterprises) must:

- Record the decisions (including statement of reasons) to restrict the use of their service in the European Commission database: https://transparency.dsa.ec.europa.eu/.
- Give recipients of their service access to an effective internal complaint handling system where complaints can be submitted electronically and free of charge.
- Inform recipients of their service that it is possible to have disputes about decisions settled by certified out-of-court dispute settlement bodies.
- Handle complaints in a timely, non-discriminatory, careful, and non-arbitrary manner.
- Include information in their terms and conditions on the key parameters used in their recommender systems and how these can possibly be adjusted or influenced by recipients of the service.

Theme 4 Trustworthiness of Business-to-Consumer (B2C) online marketplaces

B2C online marketplace providers must comply with specific rules to create a safe, trustworthy, and transparent online environment. These measures not only serve to protect consumer interests, but also help discourage traders from offering products or services that violate applicable rules and regulations.

B2C online marketplace providers (excluding micro and small enterprises) must:

- Ensure the traceability of traders using their platform.
- Implement measures to establish and verify the identity of traders. In doing so, the provider must make every reasonable effort to assess the trustworthiness of the information provided by traders.
- Design and organize the online interface in such a way that traders are able to comply with transparency obligations under Union law.
- Facilitate clear and accessible information provision for consumers concerning products and services.

Contents

Summary: DSA Guidelines regarding due diligence obligations for digital services 2

1 Introduction 7
1.1 For whom are these Guidelines intended? 8
1.2 Reader's guide 14

2 Intermediary service providers 15
2.1 What requirements does the DSA set for your terms and conditions? 15
2.1.1 Availability, form, and content of the terms and conditions 15
2.1.2 Form of terms and conditions aimed at minors 18
2.1.3 Enforcement of terms and conditions 19
2.1.4 Additional requirements concerning terms and conditions for VLOPs and VLOSEs 20

3 Hosting service providers 20
3.1 What additional requirements does the DSA impose on hosting service providers? 21
3.1.1 Notice and action mechanisms 21
3.1.2 Statement of reasons for imposing restrictions due to illegal content 23

4 Online platform providers 25
4.1 What additional requirements does the DSA impose on online platform providers? 25
4.1.1 Measures and protection against misuse 25
4.1.2 Trusted flaggers 28
4.1.3 Internal complaint handling system and out-of-court dispute settlement 29
4.1.4 Prohibition of dark patterns 32
4.1.5 Transparency in advertising and recommender systems 34
4.1.6 Protection of minors 37

5 B2C online marketplace providers 38
5.1 What additional requirements does the DSA impose on B2C online marketplace providers? 38
5.1.1 Traceability of traders 38
5.1.2 Design focused on compliance 40
5.1.3 Right to information 42

Annex I: Other obligations 44
Orders from authorities 44
Points of contact 44
Legal representation 45
Notification of criminal offenses 45
Transparency reporting obligations 46

Annex II: Overview of DSA articles 48

1 Introduction

1. The use of digital services, such as social networks and online marketplaces, has increased steadily in recent years. This applies both to individuals who use these digital services to share content on social networks and to companies that offer their goods and services through online marketplaces. A characteristic of these digital services – also called intermediary services – is that they play a role in transmitting, storing, or disseminate information from their recipients.

2. Several European laws have been adopted in recent years to regulate the digital economy. One of these is the Digital Services Act (hereafter: DSA).[1] The DSA harmonizes the existing rules applicable to intermediary services. It aims to ensure a safe, predictable, and trustworthy online environment, addressing the dissemination of illegal content and the societal risks posed by the spread of disinformation or other content and better protecting the fundamental rights of all recipients of intermediary services.

3. The DSA does not prescribe when content is illegal[2]; this follows from applicable national or Union law. Other supervisors, investigative authorities, or the courts may be responsible for assessing whether content violates applicable national or Union law and thus constitutes illegal content. Examples include civil courts judging whether certain content breaches copyright, the Netherlands Food and Consumer Product Safety Authority (hereafter: NVWA) ensuring that traders comply with product safety legislation or the Dutch Data Protection Authority (hereafter: DPA) monitoring the lawfulness of the processing of personal data and GDPR compliance. The Public Prosecution Service is responsible for investigating and prosecuting criminal offenses on the internet, in cooperation with the police and other investigative services.

4. The DSA does prescribe when intermediary services are not liable for illegal content provided by the recipients of their service and what duties of care they have with regard to actual or potential illegal content. Intermediary service providers cannot avoid liability if they play an active role that gives them knowledge or control of such information.

5. It should be noted, however, that the DSA includes the ‘Good Samaritan’ principle. In short, a liability exemption can be invoked if investigations are conducted in good faith, if other measures have been taken against illegal content, or if legislation is complied with, including the due diligence requirements of the DSA. These activities do not involve such an active role that could lead to knowledge or control of illegal information. This is expressly stated in the DSA to create legal certainty and not to discourage voluntary activities aimed at combating illegal content.[3]

6. The first intermediary service providers designated by the European Commission as very large online platforms or very large online search engines on 25 April 2023 have been required to comply with the DSA since 25 August 2023.[4] All other intermediary service providers are required to comply with the rules of the DSA applicable to them from 17 February 2024.

7. Intermediary service providers must also comply with the obligations under the Digital Markets Act (hereafter: DMA)[5] if they have been designated by the European Commission as a gatekeeper under the DMA.[6] This also applies to intermediary service providers that fall within the scope of the Platform-to-Business Regulation (hereafter: P2B Regulation)[7] and are therefore required to comply with various transparency obligations towards their business recipients.[8] The DSA also clearly interfaces with consumer law, which is currently supervised in the Netherlands by the Authority for Consumers and Markets (hereafter: ACM). This applies, for example, to oversight of the use of dark

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065.
[2] Information provided by recipients on your intermediary service contains illegal content if the information itself is illegal under the applicable law or if the information is related to illegal activities (Recital 12 DSA).
[3] Recital 26 DSA.
[4] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925.
[6] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1150.
[8] You fall within the scope of the P2B Regulation if you are a provider of an online search engine and if you are a provider of an online intermediary service. You are a provider of an online intermediary service if you meet the cumulative criteria in Article 2(2) of the P2B Regulation; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1150.

patterns, as well as oversight of the (information)rules for online marketplaces, providers of online services and sellers of products or (digital) services to consumers.[9]

8. The DSA expressly does not affect (1) other European rules relating to other aspects of the provision of intermediary services in the internal market or (2) rules specifying and supplementing the DSA. This concerns not only the DMA, the P2B Regulation, and consumer law, but also, for example, European rules on product safety, protection of personal data, and the prohibition of criminal conduct.[10] In the Netherlands, the Minister of Economic Affairs and Climate Policy (hereafter: EZK) has published a bill for online consultation in which ACM is designated as the Digital Services Coordinator (hereafter: DSC) and the supervisor of compliance with a large part of the obligations under the DSA.[11] Besides ACM, the Dutch DPA is also entrusted with supervising the DSA. This is limited to oversight of Article 26(3) (advertising on online platforms) and Article 28(2) of the DSA (protection of minors).[12]

9. In preparation for this possible future task, ACM has held discussions with various market participants and other stakeholders. In these discussions, ACM heard from intermediary service providers about their preparations for applying the rules of the DSA and the issues they encountered. These discussions revealed that market participants do not always know how they can meet the obligations and that they needed guidance. ACM has therefore drawn up the 'DSA Guidelines regarding due diligence obligations for digital services' (hereafter: these Guidelines).

10. These Guidelines explain the DSA obligations that ACM will supervise and provides guidance for intermediary service providers on various obligations. In its guidance, ACM provides additional explanatory information on the obligations and practical examples that help in complying with the obligations. These Guidelines may also be useful for consultants, lawyers, and trade organizations.

11. Based on the discussions with market participants and its own survey, ACM decided to provide guidance on the provisions of Articles 14, 16, 17, 20, 21, 22, 23, 26, 27, 28, 30, 31 and 32 of the DSA. ACM emphasizes that intermediary service providers must also comply with **all** other articles in the DSA that apply to their service but on which ACM does not provide guidance in these Guidelines.

12. Complying with these Guidelines does not guarantee that the relevant obligations under the DSA or digital and other legislation such as the P2B Regulation, DMA, or GDPR are fulfilled. It remains the responsibility of the intermediary service provider to comply with the legal standards of the DSA and other regulations. The ultimate interpretation of the DSA rests with the courts.

1.1 For whom are these Guidelines intended?

13. These Guidelines are intended for intermediary service providers that have their principal place of business in the Netherlands or whose legal representative resides or is established in the Netherlands, regardless of where the recipients who use these services are located.[13] A principal place of business exists in the Netherlands if the provider has its head office or registered office in the Netherlands and the main financial functions and operational control are also exercised there.[14]

14. In the paragraphs below, ACM explains the different types of intermediary services.

---

[9] Examples of consumer protection regulations that interface with the DSA are the Unfair Commercial Practices Directive (UCPD), which has been implemented in Book 6, Title 3, Section 3A of the Dutch Civil Code. There is also Directive 2000/31/EC (E-commerce Directive), which has also been implemented in the Dutch Civil Code, including in Book 6, Articles 227b to and in Book 3, Articles 15d and 15e. There are also interfaces with Directive (EU) 2019/2161 (Modernization Directive), which has been implemented in the Dutch Civil Code, including in articles of Book 6, Title 3A and 5, Section 2B. See for example https://www.acm.nl/nl/publicaties/acm-publiceert-vuistregels-voor-online-platformen and https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer.
[10] Article 2(4) DSA.
[11] The online consultation on the Dutch DSA bill has been completed. For the state of affairs as of 18 January 2024, see https://www.internetconsultatie.nl/uitvoeringswetdsa/b1.
[12] Article 3.2(1), DSA bill; https://www.internetconsultatie.nl/uitvoeringswetdsa/document/11605.
[13] Section 5.3.1.2 draft Explanatory Memorandum of the DSA; https://www.internetconsultatie.nluitvoeringswetdsa/document/11606.
[14] Recital 123 DSA.

Intermediary service providers

15. An intermediary service is primarily an information society service.[15] An information society service is a service that is normally offered for remuneration, by electronic means, at a distance, and at the individual request of a recipient of that service.[16] For the purposes of this definition the following is meant by:

    i. „at a distance": a service that is provided without the parties being simultaneously present,
    ii. „by electronic means": a service that 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,
    iii. „ at the individual request of a recipient of services": a service that is provided through the transmission of data on individual request.

16. Services that require the physical presence of the provider and the recipient, are not covered by this definition, for example medical examinations or treatment at a doctor's surgery using electronic equipment. Services that are provided via electronic means, that also have material content, are also not covered by the definition. For example, the purchase of rail tickets through ticket dispensing machines.[17]

17. When you provide an information society service that is also an intermediary service, the DSA is applicable to the service you provide. Intermediary services within the meaning of the DSA cover a wide range of activities that take place online and are constantly changing to ensure fast, safe, and secure transmission of information and guarantee ease of use for all participants in the online environment.[18] A characteristic of intermediary services is that they play a role in transmitting, storing, and sometimes also disseminating information from their recipients. They are usually limited to technical and automatic processing of the information provided by the recipient.[19] A **recipient** of a service may be a consumer, business recipient, or another type of recipient.[20]

[15] See first paragraph Article 3(g)
[16] Article 3(a) DSA; Article 1(1)(b) of Directive (EU) 2015/1535.
[17] In Annex I of Directive (EU) 2015/1535 more examples are provided of services that are not considered to be information society services.
[18] Recital 29 DSA.
[19] This is to avoid civil liability for the recipients' information; see Articles 4, 5, and 6 DSA.
[20] Recital 2 DSA.

18. The DSA distinguishes different categories of intermediary services (see Figure 1) based on the activities that make up those services. Given the diverse nature of these activities, the DSA comprises a tiered system of obligations for the different categories of intermediary services.[21]

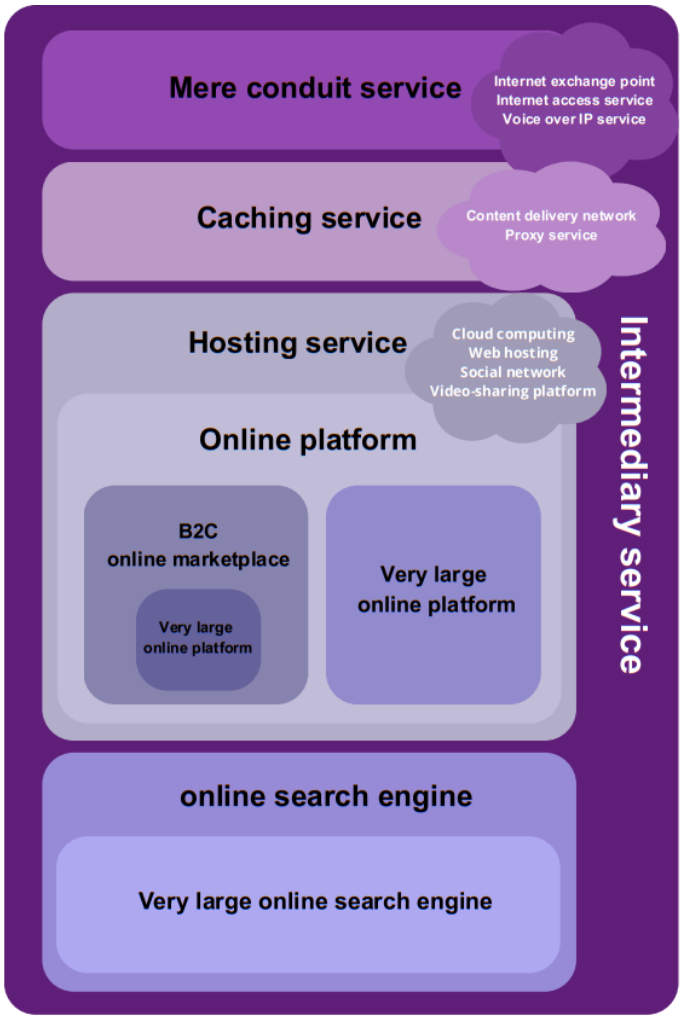

Figure 1: Categories of intermediary services

19. If you offer different types of intermediary services, separately or in the form of a 'hybrid' intermediary service[22], this may mean that you must comply with obligations that apply to different categories of intermediary services. It is possible that some of your services will fall under one category of intermediary services, but others do not, or that one of your services will fall under different categories. The rules in the DSA always apply only to the services within their scope.[23]

20. If your service may possibly fall within the scope of the DSA, it is important that you carefully survey the activities and technical functions of your service(s) and conduct a legal analysis to determine which categories apply to you. It is also pertinent to assess whether you are a micro or small enterprise.[24] You can then determine which obligations under the DSA you must comply with. Please note that you should carry out this analysis whenever your business grows, or you make changes to your service(s) that cause your activities and technical functions to evolve.

21. You are an intermediary service provider if you offer an information society service, that also falls within at least one of the categories described below:

[21] Recital 19 DSA.
[22] By 'hybrid' intermediary service, ACM means a digital service that consists of different types of intermediary services.
[23] Recital 15 DSA.
[24] The definition can be found in paragraph 31.

22. **Mere conduit service:** a service that consists of transmitting information provided by a recipient of the service via a communication network[25], or the provision of access to a communication network.[26] Examples of mere conduit services include internet exchange points, wireless access points, virtual private networks, DNS (resolution) services, top-level domain name registries, registration authorities, certification bodies issuing digital certificates, voice over IP, and other interpersonal communication services.[27]

23. **Caching service:** a service consisting of the transmission of information provided by a recipient of the service via a communication network, such information being stored automatically, temporarily, and on an interim basis to make the subsequent transmission of that information to other recipients of the service more efficient.[28] A characteristic of caching services is that they play a crucial role in the smooth and efficient transmission of information over the internet. Examples of caching services include providing content delivery networks, reverse proxies, and content modification proxies.[29]

24. **Hosting service:** a service that consists of storing information, such as websites, photographs, or applications, at the request of recipient of the service.[30] Examples include cloud computing, web hosting, paid search engine advertising services, and services that enable online sharing of information and content, including file storage and sharing.[31] A subcategory of hosting services on which the DSA imposes additional obligations are online platforms.[32]

25. For the following subcategories of intermediary services, specific obligations apply under the DSA.

Online search engine providers

26. **Online search engine**: an intermediary service that enables users to enter queries in order to perform searches of, in principle, all websites or all websites in a particular language. The entered query may be on any subject, in the form of a keyword, voice request, phrase, or other input. The result of the query can be returned in any format in which information related to the requested content can be found.[33]

Online platform providers

27. **Online platform:** a hosting service that not only stores information provided by recipients of the service at their request, but also disseminates such information to the public, at the request of recipients of the service.[34] Disseminating information to the public must not be a minor or incidental characteristic associated with another service. Nor must it be a minor functionality of the main service that cannot be used without the main service for objective technical reasons.[35]

28. Dissemination to the public means the provision of information to a potentially unlimited number of people at the direct request of the recipient of the service providing the information. This means that the information is made easily accessible to recipients of the service in general, without the recipient of the service who provided the information having to do anything further. It is not important whether persons (third parties) actually consult the information.[36] If it is only possible for recipients of the service to gain access to the information by registering or after obtaining consent, 'dissemination to the public' is also deemed to occur if the registration is automatic. This means that there is no human decision or selection of access.[37] This is the case, for example, when creating an account for a social

[25] The DSA Regulation itself does not contain a definition of 'communication network'. A definition of 'electronic communication network' can nevertheless be found in the European Electronic Communications Code. Article 2(1) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJEU 2018, L 321).
[26] Article 3(g)(i) DSA.
[27] Recital 29 DSA.
[28] Article 3(g)(ii) DSA.
[29] Recital 29 DSA.
[30] Article 3(g)(iii) DSA.
[31] Recital 29 DSA.
[32] For further explanation, see paragraph 27.
[33] Article 3(j) DSA.
[34] Article 3(i) DSA.
[35] Recital 13 DSA.
[36] Recital 14 DSA and section 2.4.5 of Explanatory Memorandum of the DSA.
[37] Section 2.4.5 of Explanatory Memorandum of the DSA.

network. Examples of online platforms are B2C online marketplaces[38], app stores, social networks, and sharing economy platforms.

29. In the following cases a service is not considered to be an online platform under the DSA:

- An online newspaper that also enables comments to be left under the published news items. The possibility of posting comments, which are disseminated by the provider at the request of the writers, is only an incidental characteristic of the main service, namely the publication of news under the editorial responsibility of the publisher.[39]
- Cloud computing or web hosting services where the dissemination of specific information to the public is a minor or incidental characteristic or functionality of the services. In addition, where these services serve only as infrastructure, such as underlying infrastructure storage and computing services of an internet-based application, website, or online platform, they cannot in themselves be deemed to disseminate information to the public. This concerns the information that is stored or processed by them at the request of the recipient of the application, website, or online platform hosted by these providers.[40]
- Interpersonal communication services[41] that enable communication between a finite number of people determined by the sender of the communication. A characteristic is that the people who initiate the communication determine who the recipients are.[42] Examples of interpersonal communication services include traditional telephone calls between people, e-mails, and private messaging services.[43] An online platform may be deemed to exist when information can be made available to a potentially unlimited number of recipients not determined by the sender of the communication, such as through public groups or freely accessible channels.

30. **NB**: the fact that you do not offer an online platform does not preclude you being a provider of a hosting service and hence required to comply with the obligations applicable to hosting service providers.

31. The DSA obligations applying specifically to online platform providers (see Chapter 4 of these Guidelines) do not apply to you if you are a micro or small enterprise.[44] You are a small enterprise if your company has fewer than 50 employees and generates a turnover of less than EUR 10 million per year[45] and a micro undertaking if your company has fewer than 10 employees and generates a turnover of less than EUR 2 million per year.[46] If your company grows and no longer meets these conditions, you must comply with the obligations for online platform providers following twelve months after losing this status.

B2C online marketplace providers

32. **B2C online marketplace**: an online platform that offers consumers the possibility of concluding distance contracts with traders.[47] A distance contract is defined as a contract between a trader and a consumer that is concluded without the simultaneous physical presence of both parties.[48] These contracts are offered as part of an organized system for distance sales or services in which only

[38] Recital 13 DSA.
[39] Recital 13 DSA.
[40] Recital 13 DSA.
[41] As defined in Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (EECC); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972.
[42] Idem; paragraph 17.
[43] Recital 14 DSA and Recital 17 EECC.
[44] Article 19(1) DSA.
[45] Article 2(2) DSA and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361.
[46] Article 2(3) DSA and eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361.
[47] In these Guidelines, we use the term Business-to-Consumer (B2C) online marketplaces to describe these types of online platforms, but this is not a definition from the DSA.
[48] Article 2(7) of 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 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083.

means of distance communication, such as the internet, are used up to and including the time of conclusion of the contract.

33. A consumer is a natural person who acts for purposes outside their trade, business, craft, or profession.[49] A trader means any natural person or any legal entity under private or public law that acts, directly or through another person acting in their name or on their behalf, in the exercise of their trade, business, craft, or professional activity.[50]

34. A characteristic of a B2C online marketplace is that the provider of the marketplace offers other traders the opportunity to offer goods and services to consumers on their platform. When a provider only offers their own goods and services to consumer, then it is not considered to be a B2C online marketplace. This is also the case when a provider only facilitates transactions between consumers.

35. The obligations under the DSA that are specifically aimed at B2C online marketplace providers (see Chapter 5 of these Guidelines) are not relevant to you if you are a micro or small enterprise.[51]

Very large online platforms and very large online search engines

36. A very large online platform (hereafter: VLOP) or a very large online search engine (hereafter: VLOSE) is an online platform or online search engine that reaches a significant part of the population of the European Union (hereafter: EU) and has been designated as such by the European Commission. The service has such reach when the number of monthly active recipients of the service, calculated as the average over a six-month period, exceeds a threshold of 45 million.[52] The European Commission (hereafter: EC) may establish further rules regarding the requirement of active recipients.[53] The EC took a first decision on 25 April 2023 designating 17 VLOPs and two VLOSEs.[54] On 20 December 2023 designated another 3 VLOPs.[55]

37. The number of active recipients of the service must be taken into account when determining the reach of your service. Active recipients of the service are all recipients who actually come into contact with the service at least once in a certain period, because they are exposed to information that is disseminated via the online interface[56] of the online platform.[57] Examples include viewing or listening to the content and providing information.[58] The active recipient of the service does not have to be a registered user of your service.

38. In the case of online search engines, the number of active recipients of the service comprises those who view information on the online interface. Owners of websites that are displayed on the online interface are therefore not active recipients of the service, as they are not actively using the service. Where recipients of the service access the service through different online interfaces, such as websites or apps, including if they access the service through different URLs or domain names, they must be counted as one active recipient of the service wherever possible.[59]

---

[49] Article 3(c) DSA.
[50] Article 3(f) DSA.
[51] Article 19(1) DSA and paragraph 31 of these Guidelines.
[52] Article 33(1) DSA.
[53] The European Commission may adopt delegated acts concerning the active recipient threshold pursuant to Recital 76 and Article 33(2). The European Commission may also adopt delegated acts concerning the precise methodology for determining the number of active recipients. More information on determining the number of active recipients is provided in the present document in anticipation of any delegated act. See: https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-recipient-numbers (last accessed on 15 November 2023)
[54] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413
[55] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6763
[56] 'Online interface' means any software, including a website or a part thereof, and applications, including mobile apps (Article 3(m) DSA).
[57] In Case T-348/23 *Zalando v Commission* and Case T-367/23 *Amazon Services Europe v Commission,* the Court of Justice will further examine the criteria used by the Commission to identify a very large online platform or a very large online search engine.
[58] Recital 77 DSA.
[59] Recital 77 DSA.

1.2 Reader's guide

39. The DSA has a tiered system of obligations. This means that in addition to the obligations that apply to all intermediary services, additional obligations apply to certain categories of intermediary services. For example, hosting service providers must meet more obligations than providers of mere conduit services, and within the hosting services category additional obligations apply to online platform providers.

    These Guidelines are arranged in a way that reflects this tiered structure (see Figure 2). In each chapter, ACM explains various DSA obligations that apply to a specific category of intermediary services and provides tools to help comply with the obligations.

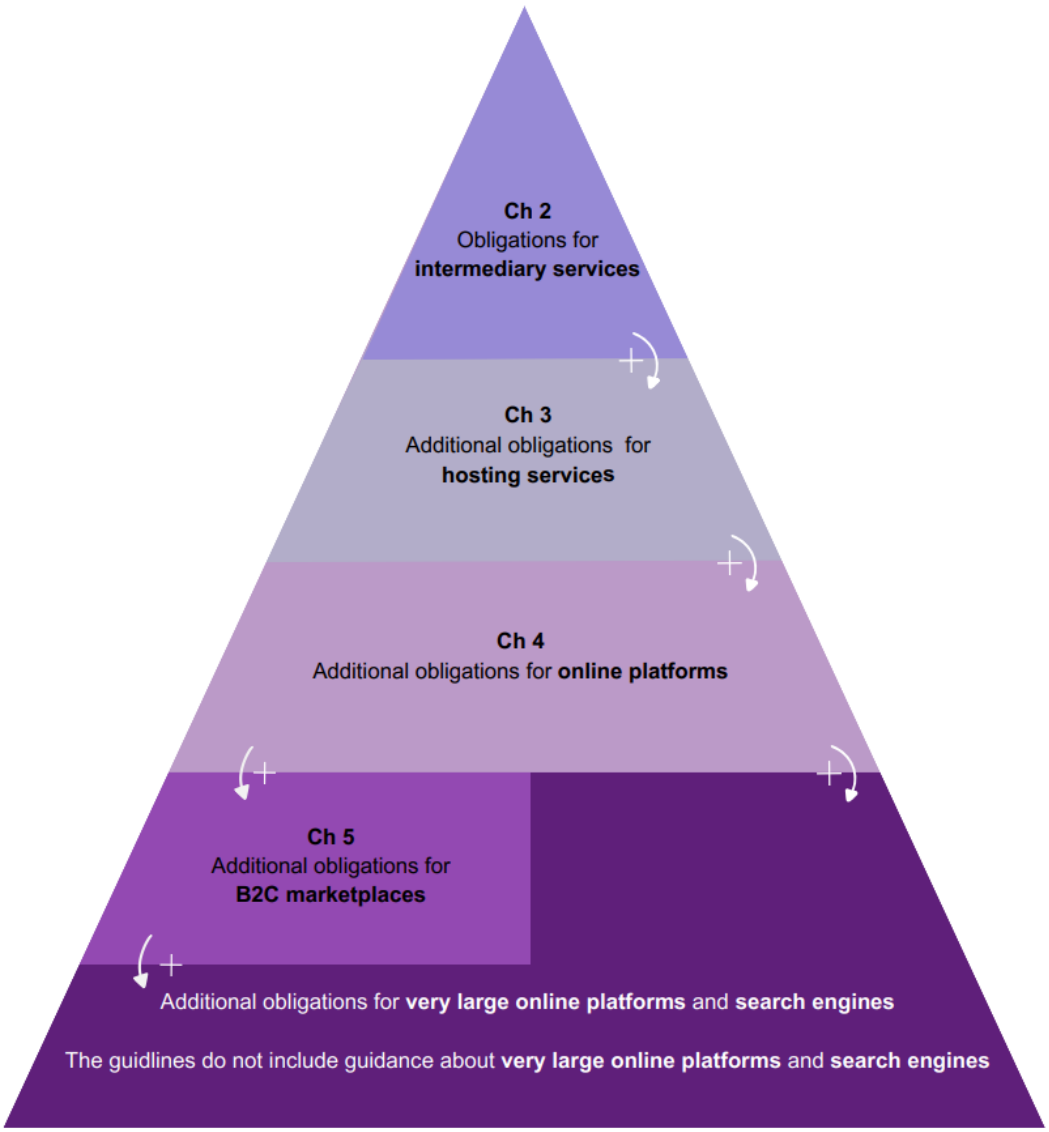

Figure 2: Tiered structure of DSA obligations

40. In conclusion, ACM considers in Annex I the other obligations that will fall within its supervision but are not covered in these Guidelines. Annex II provides an overview of the obligations applicable to intermediary services.

2 Intermediary service providers

41. Do you provide an intermediary service? Such as one or more of the following intermediary services (see paragraph 15 and so forth):

    - Mere conduit
    - Caching
    - Online search engine (including if your online search engine is a VLOSE)
    - Hosting service
    - Online platform (including if your online platform is a VLOP)
    - B2C online marketplace (including if your B2C online marketplace is a VLOP)

    If so, this chapter is relevant to you, regardless of the size of your company.

42. As an intermediary service provider, you are required to comply with various obligations under the DSA to promote a transparent and safe online environment. All intermediary service providers must comply with the obligations included in Articles 11 to 15 of the DSA. One such obligation is Article 14 of the DSA, which sets requirements for the content of your terms and conditions.

43. The rules that apply to recipients wishing to use an intermediary service are often included in terms and conditions. Terms and conditions will often have been drawn up unilaterally. Article 14 of the DSA sets requirements for the content, form, application, and enforcement of the terms and conditions of intermediary service providers. These requirements are intended to ensure greater transparency, protect recipients of the service, and prevent unfair or arbitrary outcomes.[60]

44. Below, ACM explains the requirements of Article 14 and provides you with guidance on drawing up your terms and conditions for recipients of your service. The obligations in Articles 11 to 13 and Article 15 are considered briefly in Annex I.

2.1 What requirements does the DSA set for your terms and conditions?

2.1.1 Availability, form, and content of the terms and conditions

45. In your terms and conditions, you must include information on any restrictions on the use of your service that you may impose on recipients of your service. This specifically concerns restrictions on the ability of recipients of your service to provide information.[61]

46. In your terms and conditions, you must include information on policies, procedures, measures, and tools you can use for content moderation, including algorithmic decision-making and human supervision. Your terms and conditions must also include information on the procedure of your internal complaint handling system if you have one. If you are an online platform provider, you are required under Article 20 of the DSA to make an internal complaint handling system available to recipients of your service (see section 4.1.3).

47. You must set out this information in clear, plain, intelligible, user-friendly, and unambiguous language. It is also important that the information is publicly available in an easily accessible and machine-readable format.[62]

48. If you make significant changes to your terms and conditions, you must inform recipients of your service accordingly.[63]

[60] Recital 45 DSA.
[61] Article 14(1) DSA.
[62] Article 14(1) DSA.
[63] Article 14(2) and Recital 45 DSA.

ACM's guidance

49. As an intermediary service provider, you can restrict the use of your service, for example by suspending or terminating accounts or restricting the visibility of information provided by recipients of your service.[64] For example, you can restrict the visibility of photographs, videos, documents, or posts provided by recipients of your service. In your terms and conditions, you must provide information not only on the possible restrictions, but also on the possible reasons for imposing them. This information must be up to date[65] so that it is always clear to recipients of your service what kind of restrictions you can impose and when.

50. If you use content moderation (both algorithmic decision-making and human supervision) on the information provided by recipients of your service, you must include information in your terms and conditions on the tools you use for this purpose. [66] This concerns the activities, automated or otherwise, that you carry out in particular with the aim of detecting, identifying, and addressing illegal content or information that is incompatible with your terms and conditions.[67]

51. Information provided by recipients on your intermediary service, may contain illegal content if the information is inherently illegal under the applicable law or because the information is related to illegal activities. Hate speech, terrorist content, and unlawful discriminatory content are examples of information that is inherently illegal. Examples of information that is illegal because it is related to illegal activities include the sale of non-compliant counterfeit products, online stalking, distribution of malware, and the illegal sale of live animals.[68] You could consider referring to applicable law, such as the Dutch Criminal Code, in your terms and conditions on restricting illegal content.

52. In addition to information on the tools you use for content moderation, you must also provide information in your terms and conditions on the measures you take in this regard. Any restrictions you impose may impact the availability, visibility, and accessibility of illegal content or information provided by the recipient of your service that violates your terms and conditions. Examples of such restrictions are: [69]
    - Demotion (measures that impact the visibility, availability, and accessibility of illegal content or information that violates your terms and conditions);
    - Demonetization (measures that eliminate or reduce recipients' financial incentive to provide illegal content or information that violates your terms and conditions);
    - Disabling access to illegal content or information that violates your terms and conditions;
    - Removal of illegal content or information that violates your terms and conditions; and
    - Termination or suspension of the recipient's account.

53. You should be aware that regulations other than the DSA also impose requirements on your terms and conditions, such as the requirements that consumer law imposes on the terms and conditions of all traders that conclude contracts with consumers and the P2B Regulation that imposes requirements on the terms and conditions of online intermediary services applicable to business users.[70]

[64] Article 17(1) DSA.
[65] Recital 45 DSA.
[66] Recital 45 DSA.
[67] Article 3(t) DSA.
[68] Recital 12 DSA and section 2.4.2 of Explanatory Memorandum of the DSA.
[69] Article 3(t) DSA.
[70] More information on the requirements these regulations impose on the terms and conditions between you and consumers can be found on ACM website https://www.acm.nl/nl/verkoop-aan-consumenten/de-koop-sluiten/algemene-voorwaarden-aanbieden. You can also consult the P2B Guidelines at https://www.acm.nl/system/files/documents/acm-guidelines-for-promoting-a-transparent-and-fair-online-platform-economy-for-businesses.pdf; this guidance focuses on terms and conditions between you and your business users.

Lack of information on restrictions

A video platform provider decides to restrict the visibility of a video shared by a recipient on the platform. In this case, this means that the video is not visible in the search results. According to the video platform provider, the video contains content that violates the platform's terms and conditions. The terms and conditions do not include any information to the effect that providing this type of content results in restricted visibility, nor on the reasons.

Explanation: In this example, the requirements of the DSA are not met. The DSA states that intermediary service providers must provide information in their terms and conditions on restrictions that they may impose on the use of their service. The terms and conditions must also provide information on the reasons for imposing such a restriction and what its impact is. Since this information was not provided, the recipients of the service could not have known that the video contained content that violated the terms and conditions and what the consequences are.

54. To ensure that recipients of your service understand the information in your terms and conditions on the restrictions you may impose and the reasons for doing so, you must ensure that the information is set out in clear and easy-to-understand language. This means that the way in which you have drafted the information must not mislead recipients of your service.[71] You are permitted to use graphic elements such as icons or images in your terms and conditions to represent the main elements.[72]

55. The extent to which the information in your terms and conditions concerning the restrictions you can impose is described in intelligible language depends on the category of recipients to which the information is addressed. What is clear and intelligible to the average trader may not be to the average consumer. It is important that you take this into account when drafting the information in your terms and conditions.[73] To find out to what extent the information is clear and intelligible, you could consider having it examined.[74]

56. Using short sentences and simple language where possible can also help to make your terms and conditions more understandable. It is also better to avoid the use of double negatives. In the case of consumers, for example, adding a summary with visual icons could help them better understand the information.[75] It also helps if you do not make the information too long. ACM also offers tools in other guidelines[76] to make your terms and conditions more understandable.

57. It is also important that the information is drafted in a language that is understandable to recipients of your service. If your service is mainly aimed at traders based in the Netherlands, you could consider making this information available at least in Dutch or English.[77] If your service is aimed at Dutch consumers, you could consider drafting it at least in Dutch. If you are a provider of a VLOP or

[71] The prohibition on misleading the recipient corresponds to the prohibition of misleading commercial practices set out in Article 6:193b of the Dutch Civil Code.
[72] Recital 45 DSA.
[73] If your terms and conditions are drafted in English, you could, for example, use the Gunning Fog Index to estimate the number of years of formal education a reader needs to understand the text: http://gunning-fog-index.com/.
[74] See Digital Regulation Cooperation Platform: Basic principles for effective transparency; https://www.acm.nl/system/files/documents/basic-principles-effective-transparency.pdf.
[75] For more information on improving consumers' understanding of the information, see the ACM study entitled Effective online transparency, Studies on improving online information for consumers. See: https://www.acm.nl/sites/default/files/documents/onderzoeken-naar-verbetering-online-informatieverstrekking-aan-consumenten.pdf.
[76] The Guidelines on the protection of the online consumer (https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer#about-these-guidelines) and the P2B Guidelines (https://www.acm.nl/system/files/documents/acm-guidelines-for-promoting-a-transparent-and-fair-online-platform-economy-for-businesses.pdf).
[77] See paragraph 38 of P2B Guidelines; https://www.acm.nl/system/files/documents/acm-guidelines-for-promoting-a-transparent-and-fair-online-platform-economy-for-businesses.pdf

VLOSE, you must publish your terms and conditions in all official languages of the Member States of the European Union in which your services are offered.[78]

58. The information on the restrictions you may impose on the information provided by recipients on your service must be publicly available, easily accessible, and in a machine-readable format. Publicly available means that recipients can access the terms and conditions without having to log into a user portal, for example. You could consider indicating in a structured manner on a core page on your website what information recipients can find in the terms and conditions[79] and referring to the location, for example by including hyperlinks to relevant documents and/or web pages. [80] This will help make your terms and conditions more accessible and understandable. Here too, it is important that you consider the category of recipients to whom the information is addressed.

59. The information you make available is deemed to be in a machine-readable format if you do so in document form and in a manner that does not impede the reuse of information. This could include making the terms and conditions available in PDF format on your online interface.

60. If you decide to amend your terms and conditions, you must inform recipients of your service of significant changes by appropriate means.[81] Examples of significant changes include changes to the terms and conditions governing the information permitted on your service or other changes that may directly impact recipients' ability to use your service.[82] One way in which you can inform recipients of your service about these changes is by e-mail, for example.[83]

2.1.2 Form of terms and conditions aimed at minors

61. If you provide an intermediary service that is primarily aimed at or predominantly used by minors, you must explain the conditions governing both the use of your service and possible restrictions on the use of your service in a way that minors can understand.[84]

ACM's guidance

62. The term 'minors' refers to recipients of your service below the age of 18.

63. Your intermediary service is for example aimed at minors if the terms and conditions explicitly permit the use of your service by minors. This is the case, for example, if the terms and conditions state that recipients of the service must be aged 12 or over. In addition, your intermediary service is for example aimed at minors if the design and/or marketing of your service is aimed at attracting minors.

64. This obligation also applies if your service is actually used predominantly by minors. An example of this is where the majority of recipients of your service are minors even though you have stated an age limit of 18 in the terms and conditions.

65. You must explain the conditions governing the use of the service and the restrictions on the use of the service in a way that minors can understand. The language required for minors to understand the terms and conditions will depend on the age group of your underage recipients.[85] When providing

[78] Article 14(6) DSA.
[79] See Digital Regulation Cooperation Platform: Basic principles for effective transparency; https://www.acm.nl/system/files/documents/basic-principles-effective-transparency.pdf.
[80] See paragraph36 of P2B Guidelines; https://www.acm.nl/system/files/documents/acm-guidelines-for-promoting-a-transparent-and-fair-online-platform-economy-for-businesses.pdf
[81] For changes that you wish to make to the terms and conditions applying to business users, you must apply a notice period of at least 15 days pursuant to the P2B Regulation. See Article 3(2) P2B Regulation.
[82] Recital 45 DSA.
[83] If you offer an intermediary service that also falls within the scope of the P2B Regulation, additional requirements apply under Article 3(2) of the P2B Regulation with regard to informing traders of changes to the terms and conditions. If you offer your service to consumers, you must also take into account the requirements of consumer law applying to the terms and conditions. You can find these requirements in Section 3 of Book 6 of the Dutch Civil Code. The ACM website contains guidance on these requirements for your terms and conditions, see: https://www.acm.nl/nl/verkoop-aan-consumenten/de-koop-sluiten/algemene-voorwaarden-aanbieden
[84] Article 14(3) DSA.
[85] https://www.acm.nl/system/files/documents/basic-principles-for-advertising-and-marketing-directed-at-children-online.pdf

information on the terms and conditions, you can take into account the youngest age category of minors to whom your service is directed or who predominantly use your service, for example with regard to the developing abilities, skills, and interests that match this age category.[86]

66. To make the conditions on restrictions for minors understandable, you can consult the guidance on the implementation of the Code for Children's Rights, which was drawn up on behalf of the Ministry of the Interior and Kingdom Relations.[87]

67. In addition to the terms and conditions, you could consider informing minors in another way about the conditions on the use of your service and associated restrictions. For example, you could share this information by means of pop-ups on your interface. This could help inform minors, as this target group will likely not often read the terms and conditions.

Understandable terms and conditions for minors

A 13-year-old recipient of an online platform wants to know what they are allowed to say on the online platform. The service is aimed at recipients aged 12 and over. The terms and conditions state what language is prohibited on the online platform under the heading ‘online content moderation’. The description of prohibited forms of language refers only to two articles in the Dutch Criminal Code, namely defamation (Article 261) and slander (Article 262).

Explanation: In this example, the information in the terms and conditions does not meet the requirements of the DSA. Although the terms and conditions provide information on the possibility of restricting recipients’ content, these terms and conditions will not be immediately clear to a 13-year-old recipient due to the use of terms such as ‘online content moderation’, ‘libel’, and ‘slander’. Furthermore, the reference to relevant regulations means that legal terms are used to explain when content can be restricted. The use of legal terms makes it unclear to minors what policy the online platform applies with regard to restrictions and when content will be blocked.

2.1.3 Enforcement of terms and conditions

68. When applying and enforcing the restrictions you have set out in your terms and conditions, you must act diligent, objectively, and proportionately, with due regard for the rights and legitimate interests of all those involved.[88]

69. The rights and legitimate interests of all those involved are deemed to include the fundamental rights of the recipients of your service, such as freedom of expression, freedom, and pluralism of the media, and other fundamental rights and freedoms as set out in the Charter of Fundamental Rights of the European Union (hereafter: Charter).[89]

ACM’s guidance

70. You must design, apply, and enforce the restrictions set out in your terms and conditions in a non-arbitrary and non-discriminatory manner. An arbitrary manner could include applying irregular restrictions on the use of your service or imposing different sanctions for the same types of violation of the conditions. A discriminatory manner could include imposing restrictions based on personal or other characteristics of the recipient of your service. In addition, you must take into account the

[86] You can specifically take into account the guidance on the principle of ensuring transparency in a way that is understandable and accessible to children. See: Provide transparency in a way that is understandable and accessible to children – Code for Children’s Rights https://codevoorkinderrechten.nl/beginsel/zorg-voor-transparantie-op-een-voor-kinderen-begrijpelijke-en-toegankelijke-manier/.
[87] Code for Children's Rights
[88] Article 14(4) DSA.
[89] Article 14(4) DSA.

legitimate interests and rights of your recipients, including the fundamental rights established in the Charter.[90] An example of these fundamental rights is freedom of expression.[91] In this case, you can take into account international standards for the protection of human rights, such as the United Nations Guiding Principles on Business and Human Rights.

71. In order to take your decision in a diligent, objective, and proportionate manner, you should as far as possible consider the relevant circumstances known to you during your investigation. Giving the recipient clear reasons for your decision also contributes to this.[92] In terms of proportionality, you can take into account the seriousness of the violation in relation to the restriction you impose. You can also check whether the restriction imposes an excessively heavy burden on your recipient relative to the goal being pursued.[93] For example, the posting of illegal content, such as terrorist content, naturally requires stricter measures than non-compliance with a standard in a code of conduct banning advertising on a forum.

72. To comply with this obligation, it is important that you always take into account the rights and legitimate interests of all parties involved. The outcome of this weighing of interests will depend greatly on the circumstances, which means a case-by-case assessment must be made to determine whether the application and enforcement of your terms and conditions is diligent, objective, and proportionate.

2.1.4 Additional requirements concerning terms and conditions for VLOPs and VLOSEs

73. Additional requirements apply if you are a provider of a VLOP or a VLOSE. You must give the recipients of your service a concise, easily accessible, and machine-readable summary of your terms and conditions in clear, unambiguous language. This summary must include information on available remedies and redress mechanisms (such as your internal complaint handling system).[94]

3 Hosting service providers

74. If you offer a hosting service (see paragraph 24 and so forth), this chapter is relevant to you, regardless of the size of your company. Hosting services play an important role in combating illegal online content[95], or information that is undesirable because it violates terms and conditions. They provide access to information that is provided by recipients of the service and stored at the request of the recipients.[96] The DSA therefore imposes specific obligations on hosting service providers.

75. Hosting service providers must provide notice and action mechanisms to enable individuals or organizations to notify illegal content (Article 16). Hosting service providers may decide to remove information provided by a recipient or otherwise restrict that recipient. This can have significant negative consequences for that recipient, so providers are obliged to state the reasons for such decisions (Article 17). In some cases, hosting service providers are also required to notify possible criminal offenses on their service (Article 18).

76. In this chapter, ACM explains the requirements of Articles 16 and 17 and offers guidance on complying with these provisions. Article 18 is dealt with briefly in Annex I.

[90] Recital 47 DSA and for fundamental rights see the Charter of Fundamental Rights of the European Union (2012/C 326/02).
[91] Article 11 of the Charter of Fundamental Rights of the European Union (2012/C and 326/02).
[92] See Parliamentary Papers II 2001/02, 28 197, no. 3, p. 49. These requirements are justified by analogy with the principle of good administration of Article 41 of the Charter of Fundamental Rights of the European Union (2012/C and 326/02). Details can be found in sections 42 and 44 of Case C-446/18 *Agrobet CZ* EU:C:2020:369 and the case law cited there.
[93] This reasoning is analogous to that of Article 52(1) of the Charter of Fundamental Rights of the European Union (2012/C 326/02).
[94] Article 14(5) DSA.
[95] According to the DSA, illegal content means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State that is in compliance with Union law, irrespective of the precise subject matter or nature of that law (Article 3(h) DSA).
[96] Recital 50 DSA.

3.1 What additional requirements does the DSA impose on hosting service providers?

3.1.1 Notice and action mechanisms

77. As a hosting provider, you must provide a mechanism that allows individuals as well as businesses and other organizations to inform you about the presence of illegal content on your service. You must ensure that this notice mechanism is easily accessible and user-friendly. In any case, it must be possible to submit the notice entirely digitally.[97]

78. It is important that the notices you receive are accurate and sufficiently substantiated. You should therefore ensure that notices can include the following elements:[98]

- A reasoned explanation as to why the notifying party believes the information is illegal;
- The exact electronic location of the information, including the URL. If necessary, additional information must also be provided to identify illegal content, depending on the type of content and the specific type of hosting service;
- The name and e-mail address of the notifying party, except in cases where this is not required according to Articles 3 to 7 of Directive 2011/93/EU;[99]
- A statement of the notifying party's sincere belief that they are submitting a notice in good faith and that the information provided is accurate and complete.

79. If you have received a notice containing the submitter's electronic contact information, you must send a confirmation of receipt to that submitter as soon as possible.[100]

80. If, following the notice, you have taken a decision on the information to which the notice refers, you must inform not only the recipient concerned but also the person or entity submitting the notice of this decision as soon as possible. You must inform the submitter of the possibilities for redress they have in connection with your decision.[101] If you have used automated methods for the processing or decision-making relating to the notice, you must provide the submitter with the necessary information.[102]

81. You must process all notices you receive through the aforementioned mechanisms in a timely, careful, non-arbitrary, and objective manner. The same applies to taking a decision based on those notices.[103]

ACM's guidance

82. You must ensure that persons or entities have easy access to a notice and action mechanism to report information that the notifying party believes to be illegal. Your notice and action mechanisms must be clearly identifiable, located close to the information concerned, and at least as easy to find and use as notice mechanisms for content that violates your terms and conditions.[104]To ensure that your notice mechanism is clearly visible, you could, for example, place a *'Notify illegal content'* button on your homepage.

83. Your notice mechanism must allow, but not require, individuals or organizations submitting the notice to identify themselves. Indeed, for some types of notified information, the identity of the notifying party may be necessary to determine whether the information in question actually constitutes illegal

[97] Article 16(1) DSA.
[98] Article 16(2) DSA.
[99] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0083.
[100] Article 16(4) DSA.
[101] Article 16(5) DSA.
[102] Article 16(6) DSA.
[103] Idem.
[104] Recital 50 DSA.

content.[105] Your mechanism must nevertheless request the notifying party to disclose their identity to prevent abuse.[106] The decision on whether to do so ultimately rests with the notifying party.

84. The notices that can be submitted through your notice mechanism must enable you, as a provider, to take an informed and careful decision as to whether the content to which the notice relates is illegal content and whether to take it down. It is not certain in advance what kind of information a notifying party must provide for this purpose, because 'illegal content' is a broad concept. In any case, it must be possible for the notifying party to easily provide the reasons why the content in question is considered illegal.[107] It is therefore important to provide the notifying party with the necessary space to do so through your input fields and, for example, the option to add attachments.

85. In addition, the notifying party must be able to provide the exact digital location(s) of the information in the notice. In addition to the relevant web page(s), the option must also be provided to indicate the specific location on that web page where the content is located. Finally, when designing your notice mechanism, bear in mind that a notifying party must be able to share multiple items of allegedly illegal content by means of a single notice.

Incomplete notice of illegal content

A visitor to a website with stock photos finds that her photo has been included without her permission and she believes that her portrait rights are being violated. The visitor is unable to contact the website administrator. She therefore looks up which provider hosts the website. She can find the company hosting this website on the website of Stichting Internet Domeinregistratie Nederland[108] She submits a notice through the website of the hosting service provider. In her notice, she can only provide the URL of the *web page* where the illegal content is hosted. Due to the limited input fields, the notifying party cannot specify what information on the web page she considers illegal, or exactly *where* the illegal content is located on the page. When the hosting service provider then views the web page, it will find a web page containing thousands of photographs.

Explanation: In this example, the notice mechanism does not meet the requirements of the DSA. Although a URL can be provided, the notifying party cannot specifically state which information she considers illegal, nor precisely *where* the illegal information is located. The hosting service provider is thus unable to make an informed and careful decision about the allegedly illegal content because it is not clear which information – or which photo – is involved. A notice must be able to include more information than just the URL of the web page where the illegal information is located.

86. When a notice contains sufficient information for you to determine, without a detailed legal investigation, that the content is clearly illegal, you are presumed to have actual knowledge or awareness of the illegality.[109] If you then take no action, you may also be liable for the illegal content yourself.[110] Action is deemed to mean removing the content or making it inaccessible.[111]

87. If, after receiving a notice, you judge that there is illegal content, the actions you take must be strictly targeted. This means that the actions are focused on the specific components of the illegal content. If

[105] Recital 50 DSA.
[106] Except for notices concerning criminal offenses referred to in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.
[107] Recital 53 DSA.
[108] See, for example, https://www.sidn.nl/en/whois.
[109] Recital 53 DSA.
[110] Article 6 DSA. This article includes the liability exemption for hosting service providers.
[111] Recital 50 DSA.

you take down *too much* information, you may also unnecessarily restrict your recipient's right to freedom of expression and information. If you cannot delete a specific piece of information for technical or operational reasons, for example because it is stored by another hosting service, you must inform the notifying party. [112]

88. As a provider, you must also respond in a timely manner to the notices you receive. You must take into account the type of illegal content being notified and the resulting urgency to take action. For example, you may be expected to take action without undue delay if illegal content is notified that poses an acute threat to the life or safety of persons and your action may help to eliminate that threat.[113]

89. Once you have taken a decision on a notice, you must inform the notifying party as soon as possible of your decision on whether or not to take action.[114]

90. Finally, you can also choose to subscribe to the Notice and Takedown (NTD) Code. This is part of an initiative by several parties that are committed to combating the presence of unlawful information on the internet (in the Netherlands). The NTD Code does not create any new legal obligations but is intended to help parties to operate within existing legal frameworks when removing information from the internet at the request of third parties.[115]

3.1.2 Statement of reasons for imposing restrictions due to illegal content

91. As a hosting service provider, you may impose restrictions on recipients of your service if the information they have provided is illegal or violates your terms and conditions. There are various ways in which your service may be restricted. For the following four types of restrictions, you must provide the recipient with a clear and specific statement of reasons for imposing the restriction: [116]

    - Restrictions on the visibility of specific information provided by a recipient, such as by removing or blocking it, or demoting that content.
    - Suspension, termination, or other restrictions of monetary provisions.
    - Full or partial suspension or termination of the provision of your service.
    - Suspension or termination of the recipient's accounts.

92. The statement of reasons that you are required to provide must be clear and easy to understand and as precise and specific as possible. After reading your statement of reasons, the recipient must understand why you have taken this decision and be able to assess whether the grounds were correct. Your statement of reasons must always include the following information:[117]

    - Information on the type of restriction you are imposing (see the previous paragraph) and what the consequences are. If the restriction applies to a specific region or time period, you must also provide information on that.
    - The relevant facts and circumstances that you took into account when taking your decision to impose the restriction. If relevant, state, for example, whether the restriction decision was based on your own (proactive) investigation or on a notice from another party. If it is strictly necessary, you may disclose the identity of the notifying party.
    - Clear, user-friendly information on the possibilities for redress for the recipient of your service. In any case, you should consider – if applicable – information on your internal complaint handling system, the possibilities for out-of-court dispute settlement, and appeal to the courts.

[112] Recital 51 DSA.
[113] Recital 52 DSA.
[114] Recital 52 DSA.
[115] https://noticeandtakedowncode.nl.
[116] Article 17(1) DSA.
[117] Article 17(3)(a), (b), and (f) DSA.

93. You must also provide information on the following subjects to the extent that they were applicable or relevant to your decision to impose a restriction:[118]
    - If you use automated methods to take your restriction decision, you must provide information on this. You must provide information on whether your decision was taken with regard to content that you found or identified by automated means.
    - If your decision is based on the fact that the information may be illegal, you must indicate under *which legal provision* and *why* you consider that information to be illegal.
    - If your decision is based on information that violates your terms and conditions, you must state *which contractual provision(s)* that information violates and *why*.

94. You do not have to provide a statement of reasons if you do not have the electronic contact details of the recipient of your service.[119] This also applies if the illegal content refers to a large amount of misleading commercial content disseminated through your service.

ACM's guidance

95. If you decide to impose a restriction on a recipient of your service, you must inform that recipient of your decision in an easily understandable way. This applies both to situations where you believe that the information is illegal and situations where you believe that the information violates your terms and conditions.[120] A simple reference to the applicable legal provision or clause in your terms and conditions explicitly does not constitute an understandable statement of reasons.

Incomplete statement of reasons for imposing a restriction

An organization that stands up for animal rights submits a notice to a provider of hosting services. The trading of animals through the services of this hosting service provider is expressly prohibited by Article 5 of its terms and conditions. The animal rights organization has found a website on the servers of this hosting service provider where, amongst other things, pedigree dogs are sold. Following the notice, the hosting service provider suspends the provision of services to the website administrator. The reasons given for the suspension are as follows: *'We are suspending our services to you due to actions violating our terms and conditions.'*

Explanation: In this example, the reasons do not meet the requirements of the DSA. The statement of reasons does not specifically indicate *which action* constituted grounds for the restriction decision, nor on the basis of which clause in the terms and conditions the decision was taken. The statement of reasons is not sufficient to enable the recipient of the service to determine whether the decision was taken on the correct grounds. Under the DSA, the provider should have provided this information.

96. If you impose a restriction on a recipient based on a notice submitted to you, you only have to disclose the identity of the notifying party in your statement of reasons if this is strictly necessary. This will be the case if the identity of the notifying party is required in order to determine the illegality of the content. An example is where a notifying party states that certain content violates their intellectual property rights, such as trademark rights.[121]

97. This obligation to provide a statement of reasons for decisions does not apply to large amounts of misleading commercial content disseminated as a result of intentional manipulation of your service. This could include inauthentic use of the service, such as the use of bots or fake accounts or other

[118] Article 17(c), (d), and (e) DSA.
[119] Article 17(2) DSA.
[120] Recital 54 DSA.
[121] Recital 54 DSA.

deceptive practices.[122]

98. Regardless of other possibilities for redress for the recipient of your service, the recipient always has the option to go to court to challenge your decision, even if you are affiliated with a dispute settlement body or offer an internal complaint handling system.[123] A recipient can always go directly to court or directly to dispute settlement, even if there is an internal complaints procedure.[124] You must also always provide clear information on this. You may therefore choose to include a paragraph in all your decisions that lists the means by which recipients can object to the decision. You should nevertheless take into account the amount of information you provide, to avoid an information overload to recipients. You should also take into account the level of knowledge you can expect from the recipient.[125]

4 Online platform providers

99. Are you a provider of an online platform (see paragraphs 27 and so forth)? If so, this chapter is relevant to you. This chapter is also relevant to you if you are a provider of a B2C online marketplace or if you have been designated as a VLOP by the European Commission. This chapter is not relevant to you if you are a micro or small enterprise (see paragraph 31).[126]

100. In addition to the obligations discussed in chapters 2 and 3 of these Guidelines, the DSA contains additional obligations for you as an online platform provider. These include priority handling of notices from trusted flaggers concerning illegal content and suspending recipients of your service who frequently provide manifestly illegal content (Articles 22 and 23). You must also give recipients of your service access to an internal complaint-handling system and to out-of-court dispute settlement (Articles 20 and 21). You must also comply with various transparency reporting obligations, including providing information on the number of suspensions you have imposed (Article 24).

101. The use of dark patterns on online platforms is not permitted and, as a provider of an online platform, you are also required to take measures to ensure a high level of privacy, safety, and security of minors on your service (Articles 25 and 28). You must also display information on advertising on the online interface of your online platform and your recommender systems to your recipient (Articles 26 and 27).

102. In this chapter, ACM explains the requirements of Articles 20, 21, 22, 23, 25, 26, 27, and 28 and provides guidance on complying with these provisions. A brief description of Article 24 can be found in Annex I.

4.1 What additional requirements does the DSA impose on online platform providers?

4.1.1 Measures and protection against misuse

103. As an online platform provider, you must suspend for a reasonable period of time the provision of your service to recipients who frequently provide manifestly illegal content. You may only proceed with suspension after issuing a prior warning to the recipient in question.[127]

[122] Recital 55 DSA.
[123] Recital 55 DSA.
[124] See section 4.1.3 for additional information on complaint handling systems and dispute settlement for online platforms.
[125] See the guidance provided by ACM in section 2.1.1.
[126] Article 19(1) DSA.
[127] Article 23(1) DSA.

104. As an online platform provider, you must suspend for a reasonable period of time the processing of notices and complaints submitted by persons, organizations, or complainants who regularly submit manifestly unfounded notices or complaints. Before you proceed with suspension, you must warn the person, organization, or complainant in question. This specifically concerns notices submitted through your notice and action mechanisms and complaints submitted through the internal complaint-handling system.[128]

105. If you are considering suspension, you must assess on a case-by-case basis, diligently and objectively and in a timely manner, whether the recipient, person, organization, or complainant is guilty of the misuse as described in paragraphs 103 and 104. In this assessment, you must take into account **all** relevant facts and circumstances in the information available to you. This concerns at least the following:[129]

- The absolute numbers of items of manifestly illegal content or manifestly unfounded notices or complaints, submitted in a given period.
- The relative proportion thereof in relation to the total number of items of information provided or notices submitted in a given period.
- The gravity of the misuses, including the nature of the illegal content, and its consequences; and
- If this can be identified, the intention of the recipient of the service, regardless of whether the recipient is a person, organization, or complainant.

106. In your terms and conditions you must state clearly and in detail your policy on the type of misuse as described in paragraphs 103 and 104. You must give examples in your terms and conditions of the facts and circumstances that you take into account when assessing whether certain behavior constitutes misuse and the duration of the suspension.[130]

ACM's guidance

107. Recipients of your service who repeatedly post manifestly illegal content may be misusing your online platform. For example, if a recipient repeatedly provides illegal content that they knew or could have known to be illegal.[131] This also applies to submitters of unfounded notices or complaints. Information contains manifestly illegal content and notices or complaints are manifestly unfounded if this can be determined by a layperson without the need for any substantive investigation.[132] For example, if a recipient offers firearms on your online platform.

108. If this type of misuse occurs, you must suspend the provision of your service to the recipient or the processing of notices and/or complaints from the relevant submitter for a reasonable period of time.[133] To determine what a reasonable period of suspension is, you could consider, for example, the harmfulness of the illegal content or the type of unfounded notices or complaints. You must state in your terms and conditions how long a suspension can last.

109. Before you decide to proceed with a suspension, you must in all cases warn the relevant recipient or submitter of the notice or complaint. In the warning you must state the reasons for the possible suspension and the means of redress against the decision you are considering taking.[134] In the case of a recipient who frequently disseminates manifestly illegal content, if you finally decide to proceed with suspension after issuing the warning, you must give reasons for your decision in accordance with the requirements of section 3.1.2 of these Guidelines.

[128] Article 23(2) DSA.
[129] Article 23(3) DSA.
[130] Article 23(4) DSA.
[131] Section 4.3.4.4 of Explanatory Memorandum of the DSA.
[132] Recital 63 DSA.
[133] Article 23 of the DSA is without prejudice to Article 4 of the P2B Regulation, which sets rules on the restriction, suspension, and termination of the services of online intermediary service providers and their business recipients, including the notice period and the reasons for the restriction and suspension.
[134] Recital 64 DSA.

110. If you are considering suspension, your assessment must meet the following requirements[135]:

- You must assess **on a case-by-case basis** and **in a timely manner** whether misuse has been committed by the recipient or the person submitting a notice or complaint. This means, for example, that you cannot ascertain solely on the basis of past notices or assessments that manifestly illegal content is also being provided or an unfounded notice or complaint is also being submitted at the present time. A timely assessment is important in ensuring that you do not decide that content is illegal on the basis of outdated information, for example, while the recipient has stopped providing it in the meantime.
- You must conduct your assessment in a **diligent** manner. Relevant notices that you receive from trusted flaggers can help in this regard, as can notices from other recipients.
- Your assessment must be **objective**. It is important that your assessment is based on the relevant facts.
- You must take account of **all facts and circumstances** in the information available to you. This includes at least the circumstances referred to in paragraph 105.

111. In the case of manifestly illegal content relating to serious crimes[136], such as child sexual abuse material, you are free to specify stricter measures than suspension for a reasonable period of time in your terms and conditions. This also applies to taking other measures to address the provision of illegal content or other forms of misuse by recipients of your service. For example, when recipients of your service violate your terms and conditions. If you choose to do this, you must ensure that this is set out clearly and in sufficient detail in your terms and conditions. Recipients of your service can also file a complaint or initiate a dispute procedure against this type of decision.[137] You should nevertheless take into account the amount of information you provide, to avoid an information overload to recipients. You should also take into account the level of knowledge you can expect from the recipient.[138]

Suspension of a recipient's account

A trader repeatedly offers consumers hard drugs through an online store. After becoming aware of this the provider removes the advertisements where the hard drugs are being offered. The provider of the online store has sent the statement of reasons for removing the advertisements to the trader. The statement of reasons, amongst other things, mentions that if the trader continues to advertise hard drugs his account can be suspended. In the statement of reasons, the provider refers to the terms and conditions where is explained that traders who sell substances included in List I of the Opium Law (hard drugs), will be suspended for a period of 6 months. The provider of the online store has received a notice that the trader has again placed an advertisement in order to sell hard drugs, and therefore decides to remove the advertisement based on the same reasons as before.

Explanation: In this example, the provider of the online store does not meet the requirements of the DSA. The trader is providing frequently manifestly illegal content, also after the provider warned the trader that selling hard drugs is not allowed. This is not only evident from the statement of reasons the provider sent to the trader, but also from the terms and conditions of the online store. Only removing the advertisements is therefore not sufficient. When a trader frequently provides manifestly illegal content, the provider must move on to suspending the account of the trader for a reasonable period of time.

[135] Article 23(3) DSA.
[136] In addition to stricter measures concerning the use of your service itself, you could consider reporting the offense to law enforcement or judicial authorities in the case of serious crimes not covered by Article 18 of the DSA. Article 18 is discussed in the annex to these Guidelines.
[137] Recital 64 DSA.
[138] See the guidance provided by ACM in section 2.1.1.

4.1.2 Trusted flaggers

112. The DSA introduces the notion of trusted flaggers who, amongst other things, have specific expertise and competence for the purposes of detecting, identifying, and notifying illegal content.[139] As an online platform provider, you must process and decide upon notices from trusted flaggers concerning the presence of illegal content on your online platform as a priority and with undue delay. To ensure this, you must take the necessary technical and organizational measures with regard to your notice and action mechanisms.[140]

113. A trusted flagger is an organization that has been granted the status of a trusted flagger within a specific area of expertise by the DSC in the Member State in which it is established, because this organization meets certain legal requirements.[141] The EC maintains a database of all trusted flaggers.[142]

ACM's guidance

114. An organization that has been granted trusted flagger status by a DSC can submit notices about the presence of illegal content on your online platform through your notice and action mechanisms. You must process and deal with these notices as a priority and without undue delay if they relate to illegal content within the designated area of expertise of the trusted flagger. When taking the necessary technical and organizational measures to guarantee this, you could, for example, consider appointing employees within your organization, to whom trusted flaggers can directly submit notices and who serve as their permanent contact persons. You could also consider creating an interface (e.g., a web form or web portal) where trusted flaggers can submit their notices and check the status of their notices.

115. Since trusted flaggers have demonstrated to a DSC that they have expertise and competence, the processing of this type of notice can be expected to be less burdensome for you and will therefore be faster than in the case of notices from other recipients of your service. However, the average time taken to process notices from trusted flaggers may still vary. This could be due, for example, to the type of illegal content, the quality of the notices and the actual technical procedures you have implemented for the submission of notices by trusted flaggers.[143] You could also consider adhering to deadlines agreed in codes of conduct for various types of illegal content. An example is the code of conduct for countering illegal hate speech on the internet.[144] This code of conduct states that a notice of illegal hate speech will be assessed within 24 hours. With regard to combatting online piracy of sport and other live events, the EC has published a recommendation on the handling of notices about this type of illegal content.[145]

116. **NB:** the DSA does not prevent you from treating notices submitted by other individuals or organizations that have not been granted trusted flagger status by a DSC similar to notices from trusted flaggers or from otherwise cooperating with other entities. This must be in accordance with the applicable law, including the DSA[146] and the Regulation on Europol's cooperation with private parties[147]. Furthermore, the DSA does not prevent you from using trusted flaggers or similar mechanisms to act quickly and reliably against content that violates your terms and conditions. This is especially the case with regard to content that is harmful to vulnerable consumers, such as minors.[148]

[139] Trusted flaggers must also meet the other legal requirements of Article 22(2) DSA.
[140] Article 22(1) DSA.
[141] Article 22(2) DSA.
[142] Article 22(5) DSA. The database is not yet available.
[143] Recital 62 DSA.
[144] https://commission.europa.eu/document/download/551c44da-baae-4692-9e7d-52d20c04e0e2.
[145] https://ec.europa.eu/newsroom/dae/redirection/document/95428
[146] Organizations authorized to issue orders under Articles 9 and 10 of the DSA.
[147] Regulation (EU) 2016/794; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&rid=1.
[148] Recital 62 DSA.

4.1.3 Internal complaint handling system and out-of-court dispute settlement

4.1.3.1 Internal complaint handling system

117. You must give recipients of your service access to an effective internal complaint handling system.[149] You must also grant such access to persons or organizations that have notified the presence of illegal content or content that violates your terms and conditions, on your online platform.[150]

118. The internal complaint-handling system must make it possible for recipients and notifying parties to submit complaints electronically and free of charge about certain decisions you have taken after receiving a notice. Complaints can also be submitted through the internal complaint handling system against decisions you have taken because the information provided by a recipient constitutes illegal content or violates the terms and conditions of your online platform. This concerns the following types of decisions:[151]

- Decisions on whether or not to remove or disable access to the information or to restrict its visibility.
- Decisions on whether to suspend or terminate the provision of the service to recipients in whole or in part.
- Decisions on whether to suspend or terminate the accounts of recipients.
- Decisions on whether to suspend, terminate, or otherwise restrict the ability of recipients to monetise information they provided.

119. Recipients of your service and individuals or organizations who have notified the presence of illegal content on your online platform can file a complaint through the internal complaint handling system for a period of **at least six months** after a decision as referred to in paragraph 118.[152] The six-month period starts on the day on which you inform the recipient of your service of the decision in accordance with Article 16(5) or Article 17 of the DSA.[153]

120. You must ensure that the internal complaint handling system is easily accessible and user-friendly. You must also ensure that it is possible for recipients to submit sufficiently accurate and duly substantiated complaints. The internal complaint handling system should facilitate this.[154]

121. Complaints submitted through the internal complaint handling system should be handled in a timely, non-discriminatory, diligent, and non-arbitrary manner. If a complaint gives you sufficient reason to reverse a decision as referred to in paragraph118, you must do this as soon as possible.[155] This is the case if the complaint shows that:

- Your previous decision not to act on the notice was unfounded.
- Your previous decision to which the complaint relates was unfounded because the information is not illegal and/or does not violate your terms and conditions.
- There is information indicating that the complainant's behavior does not justify the measure you have taken.

122. You must notify complainants of your decision on the submitted complaint as soon as possible, together with your reasons. You must also inform complainants of alternative options to resolve the complaint, such as the possibility of out-of-court dispute settlement and other available possibilities

[149] In the transparency report that you are required to prepare and publish at least once a year, you must also include information on the complaints you have received through the internal complaint handling system (Article 15(1)(d) DSA).
[150] Article 20(1) DSA.
[151] Article 20(1) DSA.
[152] Article 20(1) DSA.
[153] Article 20(2) DSA.
[154] Article 20(3) DSA.
[155] Article 20(4) DSA.

for redress.[156] You must ensure that decisions on submitted complaints are taken under the supervision of suitably qualified staff and not solely by automated means.[157]

ACM's guidance

123. It is important that recipients of your service can easily find the internal complaint handling system.[158] For example, you could consider including a link in a prominent place on your website to the page where recipients of your service can submit a complaint and find more information on the procedure. Ensure that the possibility of submitting a complaint is not difficult for recipients to find and that your online interface does not make it unnecessarily difficult to submit a complaint. As explained in paragraph 80, hosting service providers must inform notifying parties about the possibilities for redress when communicating the decision on the notice. One such possibility for redress is the internal complaint handling system. A similar obligation applies with regard to the information that hosting service providers are required to provide to recipients as grounds for a decision to restrict the use of the service (see paragraph 92). These obligations also apply to you as a provider of an online platform.

124. To ensure that the internal complaint handling system is user-friendly, it is important that the process steps are clear and understandable for the recipient who wishes to submit a complaint.[159] For example, if a recipient has to answer a long list of questions before being able to submit a complaint, this may be perceived as not user-friendly. This may also be the case if a recipient has to complete multiple forms. Furthermore, imposing formal requirements for the submission of a complaint is not permitted.[160] An example of a formal requirement is that you require a recipient to include a reference to specific applicable legal provisions or detailed legal explanations when submitting the complaint.[161]

125. You must handle complaints in a timely manner. Depending on the complexity of the complaint, the period within which you handle the complaint may differ. The way in which you set up the complaint system can help ensure rapid handling of recipients' complaints. For example, you could consider setting up the internal complaint handling system in such a way that it is clear to recipients when submitting a complaint what minimum information you need to process it rapidly. This reduces the likelihood that you will have to request information from the complainant later in the process.

126. It is also important that the internal complaint handling system functions in a way that leads to fair results. You must therefore handle complaints in a non-discriminatory, diligent, and non-arbitrary manner. This means, amongst other things, that you treat comparable situations (complaints) in the same way. If you use automated means to handle complaints (e.g., an algorithm/AI), you must ensure that a human check is also carried out by qualified staff.[162] This helps ensure diligent handling of complaints.

[156] Article 20(5) DSA.
[157] Article 20(6) DSA.
[158] Pursuant to Article 14(1) DSA, you are obliged to provide information on the procedure of your internal complaint handling system (see section 2.1.1). The P2B Regulation also includes obligations on the operation of the internal complaint handling system and the information to be provided on it in the terms and conditions of an online platform provider. See Article 11 of the P2B Regulation.
[159] See section 2.1.1 for guidance on preparing your information in clear and intelligible language.
[160] Recital 58 DSA.
[161] Recital 58 DSA.
[162] Recital 58 DSA.

Access to internal complaint handling system

A social network provider decided three months ago not to delete a post on the platform after assessing a notice about the presence of illegal content. The decision received by the person submitting the notice states the following:

"Dear notifying party X,

After reviewing your notice, we have determined that the post does not contain any illegal content. The post will therefore not be deleted."

The person who submitted the notice does not agree with this decision and still believes that the platform should delete the post. The person submitting the notice wishes to file a complaint against the platform's decision. The decision does not include any information on the available possibilities for redress and no information can be found on the platform's website about the internal complaint handling system. After contacting the platform, the person submitting the notice is told that complaints must be submitted within one month and that the internal complaint handling system cannot be used by notifying parties.

Explanation: In this specific example, the requirements of the DSA are not met. A notifying party who disagrees with your decision not to delete information on your platform must be able to file a complaint against this decision. You must inform the notifying party of this possibility when communicating your decision that the notice is unfounded. You must give the notifying party access to an internal complaint handling system for a period of at least six months starting on the day on which you informed the notifying party of your decision. You must also ensure that the internal complaint handling system is easily accessible and user-friendly. In this example, the notifying party cannot find any information on the platform's website about the internal complaint handling system. To make it easier to find to the internal complaint handling system, the platform could, for example, have considered including a link to the internal complaint handling system in a prominent place on the website.

4.1.3.2 Out-of-court dispute settlement

127. Recipients against whom the decisions referred to in paragraph 118 are directed may choose to have disputes concerning these decisions settled by an out-of-court dispute settlement body (hereafter: dispute body) that is certified by a DSC in one of the Member States. This also applies to individuals or organizations that have notified the presence of illegal content on your online platform.[163] You must also ensure that you inform the recipients of your service in a clear and user-friendly manner about the access they have to out-of-court dispute settlement.[164] This information must be easily accessible on your online interface.[165]

128. Which certified dispute body is authorized to settle a dispute depends on the content of the decision to which the dispute relates and/or the online platform that took the decision. A dispute settlement body is certified by the DSC to settle disputes in one or more specific areas of expertise, relating to illegal content or the application and enforcement of the terms and conditions of one or more types of online platforms.[166]

129. If recipients or notifying parties decide to use out-of-court dispute settlement, they do not lose the right to take the dispute to court.[167]

[163] This article is without prejudice to Directive 2013/11/EU and alternative consumer dispute settlement procedures and bodies established under that Directive (Article 21(9) DSA).
[164] Pursuant to Article 17(3)(f) DSA, you must include information on the possibilities for redress, such as out-of-court dispute settlement, in the reasons for a decision imposing a restriction on the use of your service by a recipient.
[165] Article 21(1), DSA.
[166] Article 21(3)(b) DSA.
[167] Article 21(1), DSA.

130. Both parties must cooperate in good faith with the certified dispute settlement body chosen to resolve the dispute. You may refuse to cooperate with such a dispute settlement body if a dispute has previously been settled regarding the same information and the same grounds for alleged illegality or incompatibility of content.[168]

131. The dispute settlement body may charge you and the complainant costs for handling the dispute. If the dispute is resolved in favor of the complainant, you will have to bear the costs incurred by the complainant.[169]

ACM's guidance

132. Instead of submitting a complaint through the internal complaint handling system against the decisions referred to in paragraph 118, recipients of your service may also choose to initiate a dispute procedure with a dispute body certified by a DSC. This also applies to recipients of your service who are not satisfied with the outcome of the handling of their complaint through the internal complaint handling system. A recipient does not need to have used the internal complaint handling system in order to start a dispute procedure and/or initiate legal proceedings.[170] You cannot therefore demand this of recipients of your service.

133. As provider of an online platform, you must inform recipients of your service in a clear and user-friendly manner about the access they have to out-of-court dispute settlement.[171] For guidance on informing recipients in a clear and user-friendly manner, see section 2.1.1 of these Guidelines. This information must also be easy for recipients to find on your online interface, such as your website or in your app. For example, you could consider including a link in a prominent place on your website to the EC website where the list of certified dispute settlement bodies is published.[172] It is important that you cooperate with the dispute settlement procedure in good faith. You can do this, for example, by submitting information that is relevant to the smooth running of the dispute procedure or by preventing the procedure from being unnecessarily delayed.

134. In some cases, you may refuse to cooperate with out-of-court dispute settlement procedures. This is the case if the same dispute has already been resolved by a court or other competent dispute body, or if the dispute is still being processed there. A similar dispute is deemed to have existed if, in particular, the dispute involves the same (i) information, (ii) reasons for taking the decision, (iii) consequences of the decision, and (iv) reasons given for contesting the decision.[173]

4.1.4 Prohibition of dark patterns

135. You must not design, organize, or manage your online interface and underlying systems in a manner that misleads or manipulates your recipients, or otherwise materially disrupts or undermines their ability to make free and informed decisions.[174]

136. This prohibition of dark patterns includes practices that are not already covered by the Unfair Commercial Practices Directive (UCPD) or the General Data Protection Regulation (GDPR).[175] The UCP Directive has been transposed into Dutch law and the GDPR is directly applicable in the Netherlands.[176]

[168] Article 21(2) DSA.
[169] Article 21(5) DSA.
[170] Recital 59 DSA.
[171] Under the P2B Regulation, there are also obligations concerning the operation of out-of-court dispute settlement and the information that must be provided on this in the terms and conditions of the online platform provider. See Article 12 of the P2B Regulation.
[172] The European Commission website is not yet unavailable.
[173] Recital 59 DSA.
[174] Article 25(1) DSA.
[175] Article 25(2) DSA.
[176] You can find the relevant articles in Book 6, Title 3, Section 3A of the Dutch Civil Code.

137. The European Commission can issue guidelines on the application of this prohibition on dark patterns to specific practices.[177]

ACM's guidance

138. Dark patterns exist on the online interfaces of your online platform when you use practices that materially disrupt or impede your recipients' ability to make free and informed choices or decisions. It is immaterial whether this is done deliberately or otherwise. These practices induce your recipients to engage in undesirable practices or take undesirable decisions that have negative consequences for them. An example of a dark pattern is the non-neutral display of choices by giving certain choices more weight by means of visual, auditory, or other components when you ask your recipient to take a decision.[178]

139. The prohibition of dark patterns in the DSA applies to practices that are not already covered by the prohibition of dark patterns under the Dutch Civil Code or the GDPR. The practices covered by the prohibition in the Dutch Civil Code are aimed at practices that materially disrupt the economic behavior of consumers.[179] Substantial distortion of the consumer's economic behavior occurs when a commercial practice is used to appreciably limit the consumer's ability to make an informed decision. The consequence of this is that the consumer decides to affect a transaction that they otherwise would not have chosen.[180] To find out more about the provisions relating to the prohibition of dark patterns under the Dutch Civil Code, you can consult the ACM Guidelines on the protection of the online consumer.[181] ACM supervises the rules on unfair commercial practices in the Netherlands.

140. The rules of the GDPR also apply with regard to the prohibition of dark patterns. The GDPR concerns the protection of natural persons in connection with the processing of their personal data.[182] The European Data Protection Board has published guidance on the prohibition of dark patterns under the GDPR, focusing on social media.[183]

141. The prohibition of dark patterns under the DSA is broader than under other legislation because it applies to both consumers and business recipients. Furthermore, the scope of the prohibition under the DSA is broader and/or slightly different than consumers who transact online with traders, and or natural persons who decide on the processing of their personal data. An example are dark patterns that are displayed to business recipients of your service.

142. The prohibition of dark patterns does not mean that you are not permitted to interact with the recipients of your service. Advertising practices that comply with EU rules are not dark patterns.[184] You are allowed to persuade recipients into using your online platform, however you are not allowed to mislead or influence them to use your online platform in a way than they would have otherwise done. For examples of legitimate practices and practices that are misleading, you can check the Guidelines on the protection of the online consumers.[185]

---

[177] Article 25(3) DSA.
[178] Recital 67 DSA.
[179] For the Dutch implementation of the prohibition of dark patterns, see Article 6:193b (2) of the Dutch Civil Code. This is based on Article 5(2)(b) of 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 of the Council, Directives 97/7/EC, 98/27/EC, and 2002/65/EC of the European Parliament and of the Council of Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').
[180] Article 2(e) of the Unfair Commercial Practices Directive.
[181] https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer
[182] Recital 14 of 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).
[183] See Dutch Data Protection Authority: Nieuwe EDPB-guidelines over dark patterns en samenwerking toezichthouders https://www.autoriteitpersoonsgegevens.nl/actueel/nieuwe-edpb-guidelines-over-dark-patterns-en-samenwerking-toezichthouders (last accessed on 15 November 2023)
[184] Recital 67 DSA.
[185] https://www.acm.nl/nl/publicaties/voorlichting-aan-bedrijven/acm-leidraad/leidraad-bescherming-online-consument

4.1.5 Transparency in advertising and recommender systems

4.1.5.1 Transparency in advertising

143. If you display advertising on your online interface, you must ensure that your recipients can ascertain, in real time, in a clear, concise, and unambiguous manner, for each specific advertisement shown to them:[186]

- That the information is advertising. Your recipient should be able to ascertain this on the basis of conspicuous markings.
- The natural person or legal entity on whose behalf the advertisement is shown.
- The natural person or legal entity who paid for the advertising if that person or entity is different from the natural person or entity referred to in the previous point.
- The most important parameters used to determine the recipients to whom the advertising is shown. Information must also be provided on the possibility of changing those parameters. This information must be directly accessible from the displayed advertisement and must contain easily accessible and useful information.

144. You must also provide a functionality for your recipients that enables them to declare whether the content they provide on your online platform is or contains commercial communication. If your recipient so declares, you must ensure that other recipients can ascertain this clearly and unambiguously and in real time, including with the aid of conspicuous markings.[187]

145. You must not display advertising to your recipients based on profiling using special categories of personal data.[188] Profiling refers to any form of automated processing of personal data in which certain personal aspects of your recipient are evaluated on the basis of personal data. This could include analyzing or predicting professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.[189] Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special categories of personal data also include genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sexual behavior or sexual orientation.[190]

ACM's guidance

146. If you display advertising on your online interface, you must provide information on it. Amongst other things, this information must make clear what the most important parameters are that are used to determine the recipients to whom the advertising is shown. You must provide a meaningful explanation of the logic behind the parameters, even when the parameters are based on profiling.[191] This explanation must therefore include information on the method used to display the advertising, for example whether it is contextual advertising or other types of advertising. Contextual advertising refers to advertising that is only linked to the content on the online interface. This does not take into account other characteristics of the visitor, such as previous visits to the website or areas of interest. In addition, the explanation must contain information on the means available to the recipient to change the parameters.[192]

147. This information must be viewable by your recipients in a clear, concise, and unambiguous manner and in real time. The information must be accessible directly through the online interface on which the advertisement is displayed.[193] This means the information must be eye-catching, which can be

[186] Article 26(1) DSA.
[187] Article 26(2) DSA.
[188] Article 26(3) DSA and Article 9 GDPR.
[189] Article 4(4) GDPR.
[190] Article 9(1) GDPR.
[191] Recital 68 DSA.
[192] Recital 68 DSA.
[193] Article 26 and Recital 68 DSA.

achieved *inter alia* by means of standardized visual or sound features. The information must also be clearly recognizable for the average recipient of your service and be adapted to the nature of the online interface of your service.[194] Also in this case you should take into account the amount of information you provide, to avoid an information overload to recipients. You should also take into account the level of knowledge you can expect from the recipient.

148. As an online platform provider, you could choose to place an icon with the word 'advertising' next to any form of online advertising on your interface. The icon could then enable recipients to open an information menu with all the required information. This information could already include an integrated method to change the parameters or a link to a page with a clear explanation of how to change the parameters.

Transparency concerning advertising

A provider offers an online form where recipients can share beauty and care tips with each other. Recipients can follow different topics that they find interesting. For each topic, they see the posts about that topic from other recipients. Many of the posts contain reviews of products that the recipients of the service have used. Some recipients are paid to use a product and then post a review of it on the forum. The terms and conditions state that this is not prohibited, but that the recipient must make clear that someone paid for the review, it therefore constitutes as advertising. The provider offers no functionality to show in the review that it's an advertisement.

Explanation: In this example, the provider does not meet the requirements of the DSA. It is good that the provider clearly indicates in its terms and conditions that recipients share a review that was paid for, must clearly indicate that it is advertising. On the basis of the requirements of the DSA, the provider itself must also offer the functionality to these recipients to indicate that the content is advertising. A recipient must be able to identify this information easily, including with the aid of conspicuous markings. Hence it is not sufficient for the provider to simply include the rule in the general terms and conditions. The provider could for example offer recipients the possibility to add a "Sponsored" icon above their review.

4.1.5.2 Transparency of recommender systems

149. If you use recommender systems, you must state in your terms and conditions in clear and intelligible language the most important parameters that your recommender systems use. In addition, you must provide information on any options for your recipients to change or influence these parameters.[195]

150. The most important parameters explain why certain information is presented to your recipients. The parameters include at least:[196]

- The main criteria for determining the information presented to your recipient; and
- The reasons for the relative importance of those parameters.

151. If you have several options available for recommender systems that determine the relative order of information shown to a recipient, you must provide a functionality that enables your recipient to select and change their preferred option at any time. This functionality must be directly and easily accessible on the specific part of your online platform's online interface where the information is prioritized.[197]

ACM's guidance

152. In addition to transparency obligations with regard to the parameters used for online advertising, you must also be transparent about the recommender systems you use. You are using a recommender

[194] Recital 68 DSA.
[195] Article 27(1) DSA.
[196] Article 27(2) DSA.
[197] Article 27(3) DSA.

system if you are using a system for presenting or prioritizing specific information.[198] A recommender system is a fully or partly automated system that works, amongst other things, on the basis of a search query initiated by your recipient, or otherwise determining the relative order or importance of the information displayed. An example of a recommender system is the priority display of products on an online platform ordered from the lowest to the highest price.

153. The information you provide on your recommender system must include the main criteria that determine what information is suggested to your recipient, as well as the reasons for the respective importance of these criteria.[199] You can also provide information on how different parameters relate to each other. This includes information such as which parameters carry the most weight and the options your recipients have to change or influence the parameters.[200] This information must also be provided when you prioritize on the basis of profiling the online behavior of your recipients.

154. The main parameters relate to all general criteria, processes, and specific signals incorporated into algorithms or other adjustment or demotion mechanisms used for ranking.[201] Examples of important parameters are:[202]

- The indicators used to measure the quality of goods or services of business recipients (e.g., consumer reviews),
- The use of editors who can influence the ranking of those goods or services (e.g., 'deals of the day', 'top picks'),
- The amplitude of the impact of remuneration on ranking, and
- Elements that are not or are only slightly related to the good or service itself, such as the presentation characteristics of the online offer (e.g., display on mobile telecommunication devices).

155. You must present that parameter information in an easy-to-understand way so that your recipients understand how information is prioritized for them.[203] An explanation of how information can be presented in an easy-to-understand way can be found in paragraphs 54 to 57.[204] It is important that you do not use misleading names for sorting options, for example using 'sort by relevance' or 'sort by popularity' when you are sorting (*inter alia*) by payment amount.[205]

Transparency of recommender systems

A provider of an online platform enables traders to offer holiday accommodations to other recipients. Traders can have their accommodations promoted by the platform at an additional cost. The promotion of these holiday accommodations means that they are recommended higher in search results that recipients see. The website and the terms and conditions of the online platform state only that the recommender system sorts the search results by relevance.

A recipient is looking for a holiday accommodation and carries out a search based on their preferences. The first results they see are the holiday accommodations promoted against payment by the online platform.

Explanation: In this example, the information on the recommender system does not meet the requirements of the DSA. The provider only indicates that the recommender system sorts by

[198] Article 3(s) DSA.
[199] Recital 70 DSA.
[200] https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer
[201] See paragraph 61 P2B Guidelines, and the Guidelines on transparency of ranking pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC1208(01).
[202] Idem.
[203] Recital 70 DSA.
[204] For more guidance on stating the most important parameters clearly and understandably, see ACM: Guidelines on the protection of the online consumer and the P2B Guidelines
[205] https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer

relevance, but not that the results are partly determined by the investments that traders have made to promote their accommodations. Moreover, the wording 'sort by relevance' is misleading, as the results are also sorted by the amount of payment for promotion. The provider must clearly indicate when search results are promoted accommodations.

4.1.6 Protection of minors

156. If your online platform is accessible to minors, you must take appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on your service.[206]

157. You must not display advertising on your interface based on profiling using personal data of the recipient of the service if you have grounds to believe with a reasonable degree of certainty that a recipient of your service is a minor.[207] Profiling refers to any form of automated processing of personal data in which personal aspects of your recipient are evaluated on the basis of personal data, in particular with the aim of analyzing or predicting their health, personal preferences, interests, trustworthiness, behavior, location, or movements.[208] The Dutch DPA will supervise this obligation concerning profiling.

158. This article does not require you to process additional personal data to assess whether the recipient of the service is a minor.[209]

ACM's guidance

159. Your platform can be deemed accessible to minors in three cases, namely when: [210]
- Your terms and conditions allow minors to use your service,
- Your service is aimed at, or used primarily by, minors, or
- You know by other means that some recipients of your service are minors, for example because you already process personal data of the recipients of your service for other purposes and that data shows their age.

160. As a provider of an online platform accessible to minors, you must take measures to protect minors.[211] This could include designing your online interface by default in a way that ensures the highest level of privacy, safety, and security for minors. An example of such a measure is setting the default option for privacy preferences as strictly as possible.[212] You could consider setting standards to protect minors and restricting access to certain types of harmful content by age category. You could also consider implementing parental controls. You could also set parental control for minors to 'on' as the default setting, for example in the application of your online platform. In addition, you could subscribe to codes of conduct to protect minors. You could also consider using age verification for access to your online platform.

161. When taking measures to protect minors, you must also take into account best practices and available guidance, such as that provided in the Commission communication on 'A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)'.[213] In addition, you could also take into account the principles of the Code for Children's Rights[214] and the associated

[206] Article 28(1) DSA. After consulting the European Board for Digital Services, the European Commission may draw up guidelines to assist online platform providers in taking appropriate and proportionate measures to ensure a high level of privacy, safety, and protection of minors within their service.
[207] Article 28(2) DSA.
[208] Article 4(4) GDPR.
[209] Article 28(3) DSA.
[210] Recital 71 DSA.
[211] In addition to taking measures to protect minors under the DSA, you must also comply with rules in other regulations that aim to protect minors. An example of such regulations is Article 6:193i(e) of the Dutch Civil Code. This provision prohibits the direct exhortation of children to buy advertised products or persuade their parents or other adults to buy advertised products for them.
[212] See basic principles for advertising and marketing directed at children online https://www.acm.nl/system/files/documents/basic-principles-for-advertising-and-marketing-directed-at-children-online.pdf
[213] Recital 71 DSA and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212.
[214] https://codevoorkinderrechten.nl/beginsel/zorg-voor-transparantie-op-een-voor-kinderen-begrijpelijke-en-toegankelijke-manier/.

implementation options and you could participate in self-regulation initiatives to protect minors. Although participation in and implementation of voluntary standards and codes of conduct can assist in complying with the DSA, this does not mean that you automatically meet the requirements of the DSA.[215]

162. If you take measures to protect minors, they must be appropriate and proportionate. You could consider taking measures that afford a sufficient degree of protection to minors without unnecessarily restricting the rights of children online.[216]

5 B2C online marketplace providers

163. If you are a provider of a B2C online marketplace (see paragraphs 32 to 35), this chapter is relevant to you. If you are a micro or small enterprise (see paragraph 31), this chapter does not apply to you.[217]

164. In addition to the obligations discussed in Chapters 2, 3, and 4, the DSA imposes additional obligations on B2C online marketplace providers. For example, the DSA states that they must ensure that traders who use their service provide information enabling them to be traced (Article 30 DSA). They must also design and organize their online interface in such a way that affiliated traders can comply with their transparency obligations under Union law (Article 31 DSA). Finally, B2C online marketplace providers are required to inform consumers about illegal products or services on their platform (Article 32 DSA).

165. In this section, ACM explains the requirements of Articles 30, 31, and 32 DSA and offers guidance on complying with these provisions.

5.1 What additional requirements does the DSA impose on B2C online marketplace providers?

5.1.1 Traceability of traders

166. As a B2C online marketplace provider, you must ensure that the traders on your platform are traceable. Therefore, before those traders can use your platform to promote their products or services, you must ensure that you receive – if applicable to the trader in question – the following information from the trader:[218]

a. Name, address, telephone number, and e-mail address;
b. If the trader appears in a trade register, or a similar type of public register, also the name of the trade register and the registration number or other form of identification in such register;
c. Any form of self-certification to which the trader subscribes and that requires them to offer only products or services that comply with the rules of Union law; and
d. A copy of the identification document, or another form of electronic identification that uniquely identifies a natural person or legal entity;
e. Details of the payment account.

[215] Recital 104 DSA.
[216] You can find an overview of children's rights that are relevant to minors in the online environment in the overview of media literacy. See: https://www.mediawijs.be/en/kinderrechten
[217] Article 29 DSA.
[218] Article 30(1) DSA.

167. The information you receive from the trader concerning points a to c must be displayed to consumers in a clear, easily accessible, and understandable manner. You must in any case do this on the online interface (e.g., website or application) of your online platform.[219]

168. Traders can only use your services after you have made every effort to assess whether the information you have received from the trader is trustworthy and complete. You do this by using a freely accessible official online database or an online interface provided by a Member State or the Union, or by requesting the trader to provide supporting documents from trustworthy sources. However, for the purposes of the DSA, traders remain liable for the accuracy of the information they provide. [220]

169. To the extent that traders are already using your B2C online marketplace as of 17 February 2024, you must make every effort to obtain the information referred to in paragraph 166 before 17 February 2025. If traders do not provide you with that information in a timely manner, you must suspend the provision of your services to those traders until they do provide the information.[221]

170. The information you receive from traders, as described in paragraph 166, must be stored securely for a period of six months until after the termination of your contract with the trader concerned. You must then destroy that information.[222] You must only share this information with third parties if required by the applicable law, including orders sent by competent authorities.[223]

171. You may obtain sufficient indications or have reason to believe that the information you have received from a trader is incorrect, incomplete, or out of date. In that case, you must request that trader to correct or supplement that information as soon as possible. If the trader fails to do so, you must suspend your service for that trader as soon as possible until your request is fulfilled.[224] In the event of suspension, a trader must nevertheless always retain the right to file a complaint with you.[225]

ACM's guidance

172. The DSA requires that you not only request trader traceability information on your platform, but also check it for completeness and trustworthiness before admitting traders to your platform. You can use easily accessible online sources for this, such as the Dutch trade register[226] at www.kvk.nl and the VAT information exchange system. If you have any doubt about the trustworthiness or completeness of the documents provided, you are expected to ask additional questions to eliminate such uncertainty. For example, you can request supporting documents such as copies of identity documents, certified copies of payment accounts, company certificates, and trade register certificates.[227] You may choose to request the identity document of the person who is eligible to represent the trader in its legal transactions.

173. You may also opt to consult any references or independent sources to verify the documents. No disproportionate burdens will be placed on you, such as conducting extensive and costly online investigations or excessive physical on-site checks. If you have made every effort to meet these requirements, you are not expected to guarantee the trustworthiness of the information for consumers or other interested parties. [228]

[219] Article 30(7) DSA.
[220] Article 30(2) DSA.
[221] Article 30(2) DSA.
[222] Article 30(5) DSA.
[223] Article 30(6) DSA.
[224] Article 30(3) DSA.
[225] Article 30(4) DSA and section 4.1.3.
[226] NB: if you have reason to believe that information from the trade register is incorrect, you can report this to the Chamber of Commerce at: https://www.kvk.nl/en/report-a-change/reporting-incorrect-information-of-third-parties/.
[227] Recital 73 DSA.
[228] Idem.

174. The DSA requires you, as a provider of a B2C online marketplace, to keep the information provided by the traders securely or a period of six months after the end of the contractual relationship with the trader concerned. To keep this information safe, you could consider taking security measures, such as data encryption, access control, and authorization protocols. By storing and securing the data, it remains possible for consumers and other interested parties to bring claims against traders or to comply with orders regarding the trader. The information thus also remains accessible to government agencies or private individuals with a legitimate interest. This obligation is without prejudice to any obligations to retain certain content for a longer period under other Union law or national law in compliance with Union law. [229]

Untraceable trader

A B2C online marketplace for the sale of electronics receives a request from trader Y to join its marketplace. Y sells stereo systems. Y must provide information before joining, including their address and a copy of their ID document. Y can start selling even before the online marketplace provider has checked the information provided by Y. Things soon go wrong: after dozens of messages from disappointed consumers in the online marketplace, it turns out that Y is selling cheap counterfeit products. When consumers try to seek redress, it turns out that the data provided by Y is incorrect. Y's address and contact details and ID document appear to be false. Therefore, it is not possible for the marketplace provider nor the affected consumers to contact Y.

Explanation: In this example, the online marketplace provider does not meet the requirements of the DSA. The provider should first have assessed whether the information provided by trader Y was trustworthy and complete, and only then decided whether trader Y should have access to the online marketplace. As this did not happen, the affected consumers cannot take action against trader Y, who is acting in violation of the law.

5.1.2 Design focused on compliance

175. Traders selling products or services must meet obligations concerning pre-contractual information, compliance, and product safety information. You must design your online interface in such a way as to provide traders with the ability to meet those obligations. Traders must in any case be able to provide the following information to recipients on your online marketplace:

- Their name, address, telephone number, and e-mail address.[230]
- All information necessary for the clear and unambiguous identification of the products or services promoted to consumers through the online marketplace;
- Any sign that identifies the trader, such as trademarks, symbols, or logos; and
- Where applicable, the information on labeling and marking in accordance with applicable Union law rules on product safety and compliance.[231]

176. Before allowing traders to offer their products or services on your online marketplace, you must make every effort to assess whether the traders on your platform have provided the information referred to in paragraph 175. After you have subsequently admitted traders to your platform, you must also make reasonable efforts to conduct random checks in an official, freely accessible, and machine-readable online database or interface to determine whether the offered products or services have been classified as illegal or meet the product requirements of Union law.[232]

[229] Recital 72 DSA.
[230] Article 31(1) DSA.
[231] Article 31(2) DSA.
[232] Article 31(3) DSA.

ACM's guidance

177. Traders have information obligations to consumers under various laws. If traders offer products or services on your platform, you must accordingly offer them the space to actually provide that information. You must therefore keep this in mind when designing and organizing your online interface. In particular, this could include information under legislation concerning:

- Pre-contractual information for online sales;[233]
- Essential or compulsory product information;[234]
- Mandatory markings such as the CE mark;
- Specific provisions for information society services[235]; and
- Indication of prices.[236]

178. You must make every effort to verify that the traders using your services have uploaded all information to your online interface in accordance with the applicable law. To ensure this, you can opt, for example, to use checklists[237] that the trader can complete for each product or service, indicating how they will fulfill the information obligations. In this way you maintain an overview and can relatively easily check whether and how the mandatory information is actually provided. You must not allow merchants to offer products or services on your platform as long as this information is incomplete. However, you are not obliged to generally monitor the products or services offered by traders on your platform, or to actively search for facts, in particular to assess the accuracy of the information provided by traders.[238]

179. Your online interfaces must be user-friendly and easily accessible for traders and consumers. To ensure that traders can actually provide all the required information, it is essential to provide them with the space and resources to do so. Examples include:

- A user-friendly, well-structured layout for displaying information on the website, which promotes clarity and understandability.
- Making sufficient space available to provide textual explanations.
- Offering the ability to refer to underlying source files or evidence showing that the service/product is legitimate, if relevant.
- Providing the option to upload relevant images or videos, for example an image of a product certification on the product.
- Providing checklists or step-by-step wizards to help traders provide the required compliance information.
- Enabling document versioning to ensure the latest information is available, for example where a trader renews their own certification and wishes to upload it.
- Providing language translation options to reach a wider audience and facilitate international trade.

[233] See Book 6 of the Dutch Civil Code, Title 5, Section 2b (3) (Provisions for distance contracts and off-premises contracts) and (5) (Additional provisions for distance contracts), implementing Directive 2011/83/EU, Articles 6 and 8.
[234] See Book 6 of the Dutch Civil Code, Title 3, Section 3A (Unfair commercial practices), Articles 193d, 193e, and 193f, implementing Directive 2005/29/EC, Article 7.
[235] See Book 3 of the Dutch Civil Code, Title 1, Section 1A (Legal aspects of electronic communication within property law), Articles 15d (1) and (2), 15e (1) and (2) implementing Directive 2000/31/EC, Article 7.
[236] Product Price Indication Decree, Articles 3 and 5, implementing Directive 98/6/EC, Article 3.
[237] See, for example: https://www.acm.nl/nl/verkoop-aan-consumenten/checklist-online-verkoop.
[238] Recital 74 DSA.

Restrictions on product information

Jewelry seller Z is active on an online marketplace for handmade jewelry. Z would like to demonstrate to her consumers the quality and authenticity of the materials used by showing detailed images of certificates, gemstone reports, and the production process. These are important items demonstrating the quality of her products. However, the online marketplace provider only allows one photo per product. This prevents Z from providing essential information to potential consumers. As a result, consumers cannot form an idea of the quality and authenticity of the products that Z sells.

Explanation: In this example, the design of the online marketplace does not meet the requirements of the DSA. When selling these products, it is important to demonstrate a number of essential product characteristics by means of images. The limited ability afforded by the online marketplace in allowing only one photo per product prevents jewelry seller Z from providing consumers with the information demonstrating the quality and authenticity of the jewelry.

180. As a B2C online marketplace provider, you must also randomly check whether products are illegal by using accessible online databases and tools. Examples of resources that can help you with this are:

- **Use of official government databases:** Online marketplace providers can work with government bodies and gain access to official government databases that list prohibited products and traders. An example of such a database in the Netherlands is the 'NVWA Productwaarschuwingen en Terugroepacties' database managed by the Dutch Food and Consumer Product Safety Authority (NVWA). This contains information on products that do not comply with legal requirements and safety standards.

- **Using automated tools:** Providers can use advanced technologies, such as web crawlers and text analysis algorithms, to scan websites and product listings for suspicious content. This can help identify illegal products or fraudulent traders.

- **Access to consumer complaints and alerts:** Monitoring consumer complaints and warnings on social media and online forums can help providers identify problematic products or traders. Timely and adequate viewing of notices that you receive yourself based on your notification system also helps with this. This consumer feedback can provide valuable insights.

5.1.3 Right to information

181. If you become aware, by any means whatsoever, that an illegal product or service is (or was) offered by a trader on your platform, you must notify consumers who purchased the product or service through your service[239] of the following:[240]

- The fact that the product or service is illegal;
- The identity of the trader; and
- All relevant means of obtaining redress.

182. This obligation to inform consumers applies only to consumers who have purchased the product or service in the **six months prior** to the time at which you became aware of the illegality.[241] If you do not have the contact details of all the consumers concerned, you must make the information easily publicly accessible on your online interface.[242]

[239] Article 32(1) DSA.
[240] NB: the DSA requires you to supply this information. Additional rules may apply if both the sale and the purchase of a particular product or service are punishable.
[241] Article 32(1) DSA.
[242] Article 32(2) DSA.

ACM's guidance

183. You can publish the information on the sale of illegal products or services through your platform in an easily accessible way on your online interface, for example by creating a special section on your website with a clear title such as 'Important information on illegal sales', in which consumers and others can find the necessary information. You can refer to this special section on the login/landing page of your website by placing a clearly visible banner containing a message such as: *'Important: if you have recently purchased product X, please read this:* (etc.)'.

Lack of information

A trader on an online marketplace sells yellow rubber ducks. The provider of the online marketplace receives several reports that children have become ill after playing with the ducks. After investigation, it is found that the ducks do not have a CE marking. This marking is mandatory for toys and represents a declaration by the manufacturer that its products have been tested against all applicable EU legislation requiring this marking and comply, amongst other things, with health and safety requirements.

Consumers who have already purchased the product are notified by the online marketplace provider using the contact details in their account. Some consumers have not entered any contact details. Since the provider cannot reach them individually, the provider decides to leave it at that.

Explanation: In this example, the online marketplace provider does not meet the requirements of the DSA. Since it is not possible to inform *all* consumers individually that they have purchased an illegal product, the supplier must make the information on the illegal rubber ducks, the identity of the trader, and the possibilities for redress available to the public in another easily accessible way on its online interface. For example, by placing a clearly visible banner on the login/landing page, containing a message such as: *'Important: if you have you recently purchased yellow rubber ducks, please read this: (etc.)'.*

Annex I: Other obligations

184. This annex contains an overview of Articles 9 to 13, 15, 18, and 24 of the DSA. These articles concern orders from authorities, the designation of contact points and a legal representative, notification of criminal offenses, and transparency reporting obligations. This annex sets out briefly what is stipulated in the DSA in this regard. This annex does not contain any additional guidance from ACM.

Orders from authorities

185. If you are an intermediary service provider, Articles 9 and 10 DSA apply to you, and you may receive orders from authorities (such as the Public Prosecution Service) to counter illegal content.

186. As an intermediary service provider, you may be able to rely on liability exemptions for illegal content on your service if you meet the conditions of Articles 4, 5, or 6 DSA. The liability exemptions are without prejudice to the ability of a judicial or administrative authority to require you, as an intermediary service provider, to stop or prevent an illegal practice, even if the conditions of those exemptions are met.[243]

187. However, as an intermediary service provider, no *general* obligations can be imposed on you to monitor the information you transmit or store, nor to actively investigate facts or circumstances that indicate illegal activities[244]. This does not apply to monitoring obligations in a specific case. As an intermediary service provider, you may therefore receive orders from authorities under Articles 9 and 10 DSA to:

- Take action against one or more specific elements of illegal content.[245] In such cases you must inform that authority of any effect given to the order without undue delay, specifying if and when effect was given to the order; and/or
- Provide specific information on one or more specific recipients of the service.[246] In such cases you must inform that authority of any effect given to the order without undue delay, specifying if and when effect was given to the order.

Points of contact

188. If you are an intermediary service provider, Articles 11 and 12 apply to you and, to facilitate smooth and efficient communication on the application of the DSA, you must designate the following contact points:

- **Points of contact for the Member State authorities, the Commission, and the European Board for Digital Services:** This central contact point must allow direct communication by electronic means with these parties. The information required to identify and communicate with this contact point must be made available, easily accessible, and kept up to date. This information must also state the language(s) in which communication is possible; communication must in any event be possible in Dutch. [247]

- **Points of contact for recipients:** This central contact point must allow direct and rapid electronic communication with recipients in a user-friendly manner, partly by offering them the possibility of choosing the means of communication – which must not be based solely on automated tools. Information that is required by participants to easily identify and

[243] Article 4(3), Article 5(2), and Article 6(4) DSA.
[244] Article 8 DSA.
[245] Article 9(1) DSA.
[246] Article 10(1) DSA.
[247] Article 11 DSA.

communicate with this contact point must be made available, easily accessible, and kept up to date. [248]

Legal representation

189. If you are an intermediary service provider without an establishment in the Union, but you offer services in the Union, Article 13 DSA applies to you, and you must designate a legal representative in one of the Member States where you provide your services.[249]

190. If you designate a legal representative in the Netherlands, these Guidelines apply to you (see paragraph 13). You do this by designating a legal entity or natural person in the Netherlands in writing to act as your legal representative. This legal representative must at least be mandated:

- To be addressed, in addition to or instead of you, by the competent Member State authorities, the Commission, and the European Board for Digital Services on all matters necessary for receipt, compliance with, and enforcement of decisions taken in connection with the DSA.
- To guarantee efficient and timely cooperation with the Member State's competent authorities, the Commission, and the European Board for Digital Services and to comply with such decisions.

191. The legal representative you have designated may be held liable for any non-compliance with obligations under the DSA, without prejudice to your liability and legal claims that can be initiated against you as a provider.

192. The name, postal address, e-mail address, and telephone number of your legal representative in the Netherlands must be shared with ACM. In addition, you must ensure that such information is also public, easily accessible, accurate, and up to date.

Notification of criminal offenses

193. If you are a provider of a hosting service, Article 18 of the DSA applies to you. This sets out what you must do if you become aware of information giving rise to a suspicion that a criminal offense has been, is being, or is likely to be committed.

194. In the case of a criminal offense that threatens the life or safety of a person or persons, you are required to promptly inform the law enforcement or judicial authorities of the Member State(s) concerned of your suspicion. The Member State concerned may be the Member State (i) where it is suspected that the criminal offense has taken place, is to be taken place, or to be likely to take place, (ii) where the suspected perpetrator resides or is located, or (iii) where the victim of the suspected offender resides or is located. If it is not possible to identify the Member State concerned with reasonable certainty, you must inform the police or Europol, or both.[250]

195. In such cases, you must provide all relevant information at your disposal, including:

- If necessary, the content involved;
- If available, the time when the content was published, including the time zone; and
- The explanation for your suspicion and the information necessary to locate and identify the relevant recipient[251].

[248] Article 12 DSA.
[249] Article 13 DSA.
[250] Article 18(2) DSA.
[251] Recital 56 DSA.

Transparency reporting obligations

196. To ensure transparency and accountability, Articles 15 and 23 of the DSA require intermediary service providers to publish various reports.

197. If you are an intermediary service provider (excluding micro and small enterprises) (see paragraph 31), you must publish an easily comprehensible report at least once a year on the content moderation you engaged in in an easily accessible manner in a machine-readable format, that includes information on:

- The number of orders received from Member State authorities, categorized by the type of illegal content concerned, the Member State issuing the order, and the average time needed to notify the issuing authority or other authority specified in the order of its receipt, and to give effect the order.
- The content moderation carried out on your own initiative, including:
  - The use of automated tools,
  - The measures taken to provide training and support for the persons entrusted with content moderation,
  - The number and type of measures taken that affect the availability, visibility, and accessibility of information provided by the recipients of the service and
  - The ability of recipients to provide information by means of the service, and other related restrictions of the service.
  - The reported information must be categorized by the type of illegal content or violation of the terms and conditions of the service provider, the detection method, and the type of restriction applied. This information must be meaningful and understandable.
- The number of complaints received through the internal complaint-handling systems in accordance with the terms and conditions (see paragraphs 117 - 126);
- Any use of automated means of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and possible error rate of the automated means in fulfilling those purposes and the safeguards applied.[252]

198. If you are a hosting service provider (excluding micro and small enterprises), you must also publish in addition to the foregoing, in the same manner:

- The number of notices submitted through the notice and action mechanisms (see paragraphs 77 – 89), categorized by the type of allegedly illegal content concerned, the number of notices submitted by trusted flaggers, and the action taken pursuant to the notices, by differentiating:
  - Whether the action was taken on the basis of the law or on the basis of the terms and conditions;
  - The number of notices processed using automated tools; and
  - The average time needed to take the action.[253]

199. If you are an online platform provider (excluding micro and small enterprises), you must also publish in addition to the foregoing, in the same manner:

- The basis for the complaints received through the internal complaint handling systems (see paragraphs 117 - 126), decisions taken with regard to those complaints, the average time needed to take those decisions and the number of cases in which those decisions were reversed.[254]

[252] Article 15(1)(a) to (e) DSA.
[253] Article 15(1)(b) DSA.
[254] Article 15(1)(d) DSA.

- The number of disputes submitted to the out-of-court dispute settlement bodies (see paragraphs 127 - 134), the outcome of the dispute settlement and the median time needed for completing the dispute settlement procedures, as well as the share of disputes in which you have implemented the body's decisions;
- The number of suspensions you have imposed to protect against abuse (see paragraphs 103 - 111), distinguishing between suspensions imposed for providing manifestly illegal content, submitting manifestly unfounded notices, and the submission of manifestly unfounded complaints.[255]

200. In addition, as an online platform, you must submit the decisions and reasons in accordance with Article 17 (see paragraphs 91 - 98) to the European Commission for inclusion in a publicly accessible, machine-readable database managed by the Commission. [256] In order to keep the database continuously updated, you must submit the decision and statement of reason after a decision has been taken without undue delay, in a standard format, to allow for real-time updates where technically possible and proportionate to the means you have at your disposal.[257] The information you provide must not contain any personal data.[258]

201. As a provider of an online platform and online search engine (excluding micro and small enterprises), you are required from 17 February 2023 and at least every six months thereafter to publish in a publicly available part of your online interface information on the average number of active recipients of your service in the Union. You calculate this by taking the average over the past six months, but further instructions for this calculation may yet be determined by the European Commission.[259] In addition, you are required to immediately share the average number of visitors and additional information on the calculation, including the calculation basis, with the European Commission or the DSC whenever they request it.[260]

[255] Article 24(1) DSA.
[256] Article 24(5) DSA. The European Commission database can be accessed at https://transparency.dsa.ec.europa.eu/.
[257] Recital 66, DSA.
[258] Article 24(5) DSA.
[259] Article 24(2) DSA.
[260] Article 24(3) DSA.

Annex II: Overview of DSA articles

Article	Subject	IS (Cumulative obligations)	HO (Cumulative obligations) ST	OP (Cumulative obligations)	B2C (Cumulative obligations)
9 and 10	Claims from competent authorities	•	•	•	•
11 and 12	Electronic contact points	•	•	•	•
13	Legal representative	•	•	•	•
14	Terms and conditions	•	•	•	•
15	Transparency report I	•	•	•	•
16	Notice and action procedures		•	•	•
17	Duty to state reasons for usage restrictions		•	•	•
18	Criminal offense reporting obligation		•	•	•
20	Internal complaint scheme			•	•
21	Out-of-court dispute settlement			•	•
22	Trusted flaggers			•	•
23	Measures against abuse			•	•
24	Transparency report II			•	•
25	Prohibition of dark patterns			•	•
26	Transparency obligation and prohibition of online advertising			•	•
27	Transparency obligation for recommender systems			•	•
28	Protection of minors			•	•
30	Traceability of traders				•
31	Compliance by design				•
32	Right to information on illegal products or services				•

Table 1: DSA obligations that intermediary service providers must fulfill. NB: the additional obligations that VLOPs and VLOSEs must fulfill (Articles 34 to 42) are not included in this table.

IS = Providers of intermediary services
HOST = Providers of hosting services
OP = Providers of online platforms
B2C = Providers of B2C online marketplaces