PANORAMIC

# ONLINE SAFETY REGULATION 2026

**Contributing Editors**

**Jenna Rennie**, **Rory Hishon** and **Alexander Beaton**

White & Case LLP

LEXOLOGY

# Online Safety Regulation 2026

Contributing Editors

**Jenna Rennie, Rory Hishon and Alexander Beaton**

White & Case LLP

A comparative guide to online safety regulation in key jurisdictions worldwide. Topics covered include the legal framework for combating online harms; obligations for online service providers, including risk assessments and mitigation; enforcement and penalties; and disputes, including remedies and defences.

**Generated on: February 4, 2026**

# Portugal

**Ricardo Henriques**
Abreu Advogados

## Summary

## LEGAL FRAMEWORK

### Legal regime

**1** Does your jurisdiction have a legal regime governing or addressing online safety? If so, how does it operate?

Portugal operates a multi-tiered regulatory framework for online safety. At its foundation lies the European Union's Digital Services Act (Regulation (EU) 2022/2065 (DSA)), which applies to all providers of intermediary services, including very large online platforms (VLOPs) or search engines (VLOSEs).

Additional intermediary-service obligations relevant to online safety arise under Decree-Law No. 7/2004 of 7 January, which transposed the e-Commerce Directive. In parallel, sector-specific online safety requirements to audiovisual services under the Audiovisual Media Services Directive (EU) 2018/1808, as transposed by the Television and On-Demand Audiovisual Services Act (Law No. 27/2007 of 30 July).

In parallel, Portugal applies sector-specific online safety obligations to audiovisual services under the Audiovisual Media Services Directive (EU) 2018/1808, as transposed by the Television and On-Demand Audiovisual Services Act (Law No. 27/2007). Notably, the rules applicable to video-sharing platform providers require that audiovisual commercial communications be clearly identifiable and comply with substantive restrictions, including prohibitions on hidden advertising and subliminal techniques, as well as safeguards against harmful content: particularly concerning minors (eg, content likely to cause physical, mental or moral harm, or that exploits children's inexperience or credulity).

**Law stated - 20 January 2026**

### Online harms covered

**2** Which online harms are covered under the relevant legislation and how are these harms defined?

Under the DSA, online harms are not defined as a closed set of prohibited content categories. Instead, it addresses harms through a risk-based approach: VLOPs and VLOSEs must identify, assess and mitigate systemic risks linked to the design and use of their services, including the dissemination of illegal content and actual or foreseeable negative effects on fundamental rights, civic discourse, public security, public health and individuals' physical or mental well-being.

In parallel, in the audiovisual framework sets sector-specific protections for video-sharing platforms. Law No. 27/2007 addresses, in particular, content that may impact the physical, mental or emotional development of minors, and also content that may impair the physical, mental or moral development of minors, content involving incitement to violence or hatred and certain prohibited commercial practices (including manipulative subliminal techniques). Decree-Law No. 7/2004 remains relevant as it also references unlawful and criminal content affecting human dignity, public order and the protection of minors, including

child sexual abuse material, incitement to hatred or violence and, in certain circumstances, serious violations of sexual privacy.

**Law stated - 20 January 2026**

## Online services covered

**3** | Which online services are covered under the law and how are these services defined?

Both the DSA and Decree Law No. 7/2004 apply to defined categories of information society services: that is, services normally supplied for remuneration, at a distance, by electronic means and at the individual request of the service recipient. Within this framework, they cover several types of intermediary services, including online platforms and online search engines, through the following categories:

- mere conduit: the transmission of information in a communication network or the provision of access to such a network (eg, internet service providers);
- caching: the automatic, intermediate and temporary storage of information provided for the sole purpose of making onward transmission to other recipients more efficient (eg, content delivery networks); and
- hosting: the storage of information provided by and at the request of the service recipient (eg, social media platforms).

In the digital audiovisual sector, Law No. 27/2007 also regulates virtual audiovisual commercial communications, on-demand audiovisual services and video sharing platforms. Video sharing platforms are defined as services whose principal purpose (or essential functionality) is to provide user-generated videos or programmes to the public, organised by the platform provider, for information, education, information or entertainment, via electronic networks.

**Law stated - 20 January 2026**

## Territorial scope

**4** | What is the territorial scope of the relevant law?

The DSA, as the E-Commerce Directive, applies to intermediary services offered to recipients in the EU, including where the provider is not established in the EU. Differently, Law No. 27/2007 is applicable to video-sharing platform services when the provider is established in Portugal under the Audiovisual Media Services Directive.

**Law stated - 20 January 2026**

## Codes of practice

**5** |

Are there any codes of practice or other non-binding guidelines or recommendations relating to online safety in your jurisdiction?

Under the DSA, the European Commission and the European Board for Digital Services have promoted voluntary codes of conduct relevant to online safety, such as the Revised Code of Conduct on Countering Illegal Hate Speech Online (Code of Conduct+). The Code of Conduct+ is intended to strengthen the handling of content qualifying as illegal hate speech under EU and national law and, while adherence is voluntary, it may support platforms in demonstrating compliance with DSA risk-mitigation obligations relating to the dissemination of illegal content.

Portugal also participates in the Better Internet for Kids (BIK+) initiative, and has developed complementary soft-law and awareness programmes, particularly in relation to minors and digital literacy.

**Law stated - 20 January 2026**

## Harmful versus illegal content

**6** How does the law in your jurisdiction distinguish between harmful and illegal content?

The DSA defines illegal content as information that, in itself or in relation to an activity, does not comply with union law or the law of a member state. This concept is central in delineating the scope of providers' content moderation and enforcement decisions under the DSA.

By contrast, harmful content is not formally defined in the DSA. It is commonly understood as content that may produce adverse effects on users. Given the inherent vagueness of this category, relying on it as a basis for removal decisions may raise freedom of expression concerns and, in practice, leave significant discretion to online service providers to identify and remove content they deem harmful. The European Commission has emphasised that illegal content should be distinguished from harmful content in the context of online content moderation.

**Law stated - 20 January 2026**

## Extremist and terrorism-related content

**7** How does your jurisdiction regulate the dissemination of extremist and terrorism-related content online?

Under the DSA, terrorism content qualifies as illegal content. In addition, the regulation provides for an exceptional crisis response mechanism under which VLOPs and VLOSEs may, following a recommendation from the European Board for Digital Services, be required to adopt proportionate and time-limited measures to address serious cross-border threats, including terrorism.

More specifically, the dissemination of terrorist content online is regulated by Regulation (EU) 2021/784, which requires hosting service providers to comply with removal or blocking orders issued by competent authorities. The Regulation also contains safeguards, including an exclusion for content disseminated for educational, journalistic, artistic or research purposes, or for the prevention or countering of terrorism, based on an assessment of the actual purpose of the dissemination.

In addition, Law No. 60/2025 of 22 October granted the government a legislative authorisation to adopt implementing legislation and designate the Judiciary Police as the competent authority to issue removal or blocking decisions, subject to subsequent validation by a Court decision within 48 hours.

**Law stated - 20 January 2026**

### Disinformation versus misinformation

**8** How, if at all, does the law in your jurisdiction distinguish between misinformation and disinformation online? Does it include malinformation?

Portuguese law does not establish a general, binding legal classification defining misinformation, disinformation and malinformation. Instead, the DSA addresses these issues through a systemic-risk framework, particularly concerning risks to society and democracy, and fundamental rights.

Law No. 27/2021 of 17 May (Portuguese Charter of Human Rights in the Digital Age) previously contained a statutory definition of disinformation in its article 6, but those provisions have since been repealed.

The text described disinformation as false or misleading narrative created, presented and disseminated to obtain an economic advantage or deliberately deceive the public, where it may cause public harm (including impacts on democratic political processes, public policy-making and public goods). It also provided listed examples (such as manipulated or fabricated texts or videos, inbox-flooding practices and networks of fictitious followers); and established a complaint mechanism involving the media regulator. This approach raised concerns, particularly from a freedom of expression perspective, regarding the design and potential implications of the mechanism.

**Law stated - 20 January 2026**

## OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

### General obligations

**9** What general legal obligations relating to safety are imposed on providers of online services, including providers of online intermediary services?

Under the Digital Services Act (Regulation (EU) 2022/2065 (DSA), providers of online services must comply with orders issued by the competent judicial or administrative authorities to act against illegal content. They must also ensure that their terms and

conditions are clear, accessible and transparent, including information on content moderation policies, the use of automated tools and human review, and the functioning of internal complaint handling mechanisms.

Online platforms are further required to explain the main parameters of their recommender systems in a clear manner and provide users with options to modify those systems. In addition, the DSA prohibits the design or operation of interfaces that deceive, manipulate or otherwise impair users' ability to make free and informed decisions.

Specific transparency obligations apply to online advertising. Platforms must clearly identify advertisements as such, disclose the person on whose behalf the advertisement is displayed (and the payer, where different) and provide meaningful information about the main targeting parameters, including how users may modify them.

Last, platforms that enable consumers to conclude distance contracts with traders must ensure trader traceability by requesting and storing essential identification information.

**Law stated - 20 January 2026**

## Risk assessments and mitigation

**10** Are there any specific legal obligations for online service providers to conduct risk assessments and mitigate risks to safety?

The DSA systemic risk management obligations apply primarily very large online platforms (VLOPs) and search engines (VLOSEs). They must self-assess any systemic risks in the EU that stem from how their services are designed, functioning or operating.

Risk assessments must be carried out at least once a year and be proportionate to the scale and reach of the service, the likelihood of risk materialising, and the severity of its potential impact. The DSA identifies specific categories of systemic risks to be considers, including the dissemination of illegal content and actual or foreseeable negative effects on civic discourse and electoral processes. Where risks are identified, VLOPs and VLOSEs are required to adopt targeted mitigation measures addressing the specific systemic risks identified.

**Law stated - 20 January 2026**

## Protection of minors and age verification

**11** Are there any specific legal obligations to protect minors online? If so, what measures are required or advised, such as age verification?

Although the DSA does not set a minimum age to access social media, it places strong emphasis on the protection of minors. Where services are likely to be accessed by children, online platforms must adopt appropriate and proportionate measures to safeguard children's rights and well-being. This includes ensuring that terms and conditions are clear, plain and age-appropriate, as well as implementing protective measures such

as age-appropriate design, risk mitigation, and age-verification and parental control mechanisms.

The European Commission has supplemented these obligations with Guidelines on ensuring a high level of privacy, safety and security for minors online, setting out core principles such as (1) proportionality and appropriateness, (2) protection of children's rights, (3) privacy-, safety- and security-by-design, and (4) age-appropriate design.

Comparable child protection obligations are also reflected in the audiovisual framework under Law No. 27/2007, regarding video-sharing platform services. In addition, Law No. 58/2019 of 8 August, which implements the GDPR, sets a sector-specific age threshold of 13 years for the validity of a child's consent in relation to the direct offer of information society services. Portuguese law also restricts minors' access to adult content, including the sale of pornographic material or obscene products to persons under 18 (Decree-Law No. 10/2015 of 16 January).

**Law stated - 20 January 2026**

## Civil and human rights

**12** Are there any obligations for online service providers to balance civil and human rights, such as privacy rights and freedom of expression, with safety regulations? If so, what measures are required or advised?

The DSA is structured to protect fundamental rights, including freedom of expression and information, privacy and data protection. These rights are recognised both under the Charter of Fundamental Rights of the European Union and the Portuguese Constitution. In parallel, Law No. 27/2021 reinforces these protections in the digital context, including freedom of expression in online environments, the right to digital privacy and data protection and the need to safeguard children in cyberspace.

At the same time, the legal framework acknowledges that these rights are not absolute and may be subject to lawful limitations where necessary to address illicit conduct, such as hate speech, terrorism-related content or child sexual exploitation. Accordingly, online service providers are expected to embed rights-respecting design, due process and proportionality principles into their safety and content-governance practices.

**Law stated - 20 January 2026**

## Disinformation and misinformation

**13** Are there any specific legal obligations to combat disinformation and misinformation online? If so, what measures are required or advised?

Under the DSA, online platforms, especially VLOPs and VLOSEs, must identify, assess and mitigate systemic arising from the design and operation of their services, including risks affecting civic discourse and democratic processes (which may encompass disinformation). Where relevant risks are identified, providers are expected to adopt

proportionate mitigation measures, which may include adjustments to service design and features, changes to advertising and recommendation/d targeting systems, and enhanced transparency and cooperation measures.

In addition, the 2022 Code of Practice on Disinformation provides a voluntary co-regulatory framework to support and structure platform's efforts to limit the spread and amplification of disinformation, without creating binding obligations.

**Law stated - 20 January 2026**

### Notice and takedown

**14** | Is there a legislative 'notice and takedown' mechanism or similar in your jurisdiction? If so, how does it operate?

A notice and takedown mechanism exists in Portugal via the directly applicable DSA. Hosting services providers, including online platforms, must implement an accessible mechanism enabling individuals and entities to report allegedly illegal content. Upon receipt of notice, hosting providers must act without undue delay, assess the legality of the content and take appropriate measures where necessary. They must also inform the notifier of their decision and outline available redress options. Where action is taken against content or a service recipient (including removal, disabling access, restriction of visibility, suspending of service or account termination), the provider must issue a statement of reasons to the affected recipient, setting out the factual and legal grounds and indicating possibilities for appeal.

In practice, a provider is treated as having 'actual knowledge' once it receives a sufficiently precise and substantiated notice (typically including the specific URL/location of the content, an explanation of why it is illegal and the notifier's contact details).

The affected recipients and notifiers may challenge the decisions made by the online platform provider through an effective internal complaint-handling system for a minimum period of six months. In addition, disputes may be referred to certified online out-of-court dispute settlement bodies, whose decisions are not binding. These remedies do not affect the right to challenge the platform's decisions before the courts.

**Law stated - 20 January 2026**

## ENFORCEMENT AND PENALTIES

### Enforcement

**15** | How is the online safety regime enforced in your jurisdiction?

Nationally, the Digital Services Coordinator (DSC) in the provider's main place of establishment exercises wide supervisory and enforcement powers over the Regulation. For very large online platforms (VLOPs) and search engines (VLOSEs), the European Commission plays a central enforcement role, with powers to supervise compliance and

take action, either exclusively for certain obligations or alongside the DSC, particularly where infringements may have cross-border or EU-wide implications.

In parallel, the Digital Services Act (Regulation (EU) 2022/2065 (DSA)) also affirms that users can assert their rights in court, including seeking pecuniary compensation for damages caused by infringing providers.

**Law stated - 20 January 2026**

## Authorities

**16** Which authorities are responsible for enforcement? What is the basis, nature and extent of their enforcement powers?

Portugal's designation of competent authorities for DSA purposes has recently evolved. The government initially designated the National Communications Authority (ANACOM) as both a competent authority and Portugal's DSC. At the same time, the government introduced a multi layered institutional framework by also appointing the Regulatory Authority for the Media and the General Inspectorate for Cultural Activities as competent authorities.

However, the underlying Decree-Law did not clearly define the powers of each authority or establish operational coordination mechanisms, and the DSA does not provide detailed guidance for a multi-authority national model. This approach attracted criticism due to the legal uncertainty and potential jurisdictional overlap it created.

In July 2025, the government issued a draft implementing law that centralises DSA functions in ANACOM, which would act as both competent authority and DSC. If approved, ANACOM will hold enforcement powers enabling it to, *inter alia*, order the cessation of infringements, adopt proportionate corrective measures, and impose fines and periodic penalty payments.

**Law stated - 20 January 2026**

## Penalties and liability

**17** What are the potential fines or penalties for non-compliance? Are there risks of liability for employees or directors of online service providers?

Under the Portuguese Draft Law implementing the DSA, intermediary service providers may be subject to fines of up to 6% of their worldwide turnover from the previous financial year. Where the offender is a natural person, the same ceiling applies, calculated by reference to the individual's total income from the previous year.

Lower penalties apply in specific cases, such as the provision of incorrect, incomplete, or misleading information, failure to respond to information requests, or refusal to submit to an inspection. In those cases, fines may reach up to 1% of the providers' global turnover or, where applicable, 1% of the natural person's annual income. DSCs may also impose

periodic penalty payments of up to 5% of the provider's average daily worldwide turnover or income per day.

For VLOPs and VLOSEs, the European Commission may impose fines of up to 6% of global turnover.

Overall, the DSA's penalty regime is structured to hold intermediary service providers accountable for non compliance. The draft implementing framework does not expressly provide for personal liability of employees or directors.

**Law stated - 20 January 2026**

## DISPUTES

### Claims

**18** What claims relating to online safety are available and most common in your jurisdiction?

In Portugal, online safety-related claims are commonly pursued by individuals or legal persons through simplified dispute-resolution mechanisms, such as Justices of the Peace, and where the claim relates a consumer relationship. When the claim involves a consumer relationship, consumer arbitration centres are typically the preferred mechanism for alternative dispute resolution.

**Law stated - 20 January 2026**

### Procedure

**19** What is the procedure for claimants to bring actions relating to online safety in your jurisdiction?

Claimants may, in addition to pursuing actions before national courts or arbitration centres, access the out-of-court dispute settlement mechanism established under the Digital Services Act (Regulation (EU) 2022/2065 (DSA)).

Where a claimant considers that an intermediary service provider has failed to comply with its obligations under the DSA, a written complaint may be submitted to the National Communications Authority (ANACOM). ANACOM is responsible for assessing admissibility of the complaint under the DSA and, if appropriate, may forward it to the DSC of another member state where the provider is established, potentially prompting a formal investigation by that authority.

Importantly, the DSA does not grant dispute-resolution powers to DSCs. If the matter is not resolved directly with the provider, claimants may pursue judicial proceedings in Portuguese courts or resort to certified alternative dispute resolution bodies. These avenues operate without affecting providers' obligations to maintain internal complaint-handling systems and notice-and-action mechanisms under the DSA.

**Law stated - 20 January 2026**

### Remedies

**20** What interim and substantive remedies may be imposed in relation to online safety claims?

Generally, affected parties can request interim relief from Portuguese courts if there is a threat of serious or irreversible harm. In online safety cases related to DSA obligations, such measures might involve suspending certain platform activities.

Substantive remedies derive from article 54 DSA, which recognises the right to seek compensation for damage caused by infringements of the Regulation. In practice, such claims will generally stem from contractual liability, based on breaches of a platform's terms and conditions. Under Portuguese civil law, the contractual liability is subject to a presumption of blame on the infringing party, thereby shifting the burden of proof to the service provider.

**Law stated - 20 January 2026**

### Defences and exemptions

**21** Does your jurisdiction provide any defences or exemptions from liability for online safety claims? If so, how do they operate and which online services providers may avail of them?

Providers offering mere conduit, caching, and hosting online services benefit from a liability exemption in relation to third-party content they transmit or store, provided that specific statutory conditions are not met (the 'safe harbour' regime).

Hosting providers are not liable for storing information supplied by users when they lack actual knowledge of its illegal nature. Alternatively, once they obtain such knowledge or awareness, they must act promptly to remove or disable access to the unlawful content.

These exemptions require providers to remain neutral and passive, without controlling the content. In line with EU law, intermediary services are not subject to a general duty to monitor or actively seek illegal activity unless they voluntarily take measures that align with legal safeguards and fundamental rights.

**Law stated - 20 January 2026**

## UPDATE AND TRENDS

### Key trends and future developments

**22** What are the most noteworthy recent trends and developments in online safety regulation in your jurisdiction? What developments are expected in the coming year?

Looking ahead, the regulatory agenda in Portugal is expected to be shaped by the following developments. The Digital Services Act (Regulation (EU) 2022/2065 (DSA))'s implementation and enforcement architecture (2025-2026). Portugal awaits the approval of the Draft Law No. 25/XVII/1 implementing the DSA. A second notable development is the move to formalise domestic procedures for the Terrorist Content Online (Regulation (EU) 2021/784). At EU level, and indeed globally, child online safety remains a major policy priority, including discussions in the European Parliament advocating a minimum age of 16 for access to social media platforms.

**Law stated - 20 January 2026**

**Ricardo Henriques** ricardo.henriques@abreuadvogados.com

Abreu Advogados

**Read more from this firm on Lexology**