

DIGITAL SERVICES IN PORTUGAL: ENFORCEMENT LAW APPROVED



NEWS,
LATEST,
CURRENT TOPICS

“THE REGIME IS RELEVANT, FIRST AND FOREMOST, TO SO-CALLED PROVIDERS OF INTERMEDIARY SERVICES, THAT IS, ENTITIES WHICH, IN THE CONTEXT OF PROVIDING DIGITAL SERVICES, TRANSMIT, STORE OR HOST INFORMATION PROVIDED BY THEIR USERS, A CATEGORY WHICH MAY INCLUDE ACCESS OR DATA TRANSMISSION SERVICES, HOSTING SERVICES, ONLINE PLATFORMS AND MARKETPLACES.”

WRITTEN BY



LÍDIA SILVESTRE
Partner



MARGARIDA TEMPERA
Junior Associate

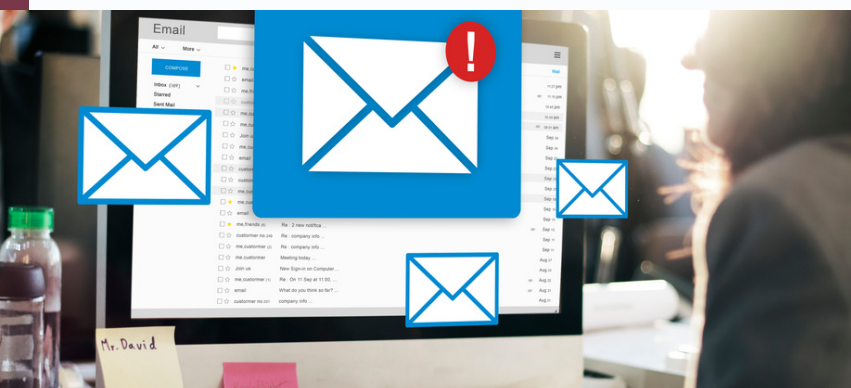
Law 12-A/2026 of 15 April has made it possible to enforce, in Portugal, the Digital Services Regulation, commonly referred to as the Digital Services Act or DSA, applicable since 17 February 2024, now establishing the national framework necessary to determine who supervises compliance with the relevant obligations, what means are available to the authorities to act and what consequences may result from non-compliance with those obligations.

The distinction is important because the national enforcement law does not replace the DSA or, as a general rule, create a new set of obligations for companies, but rather enables the obligations already laid down in the Regulation to be supervised and sanctioned in a more structured manner in Portugal, with compliance with those obligations now supported by clearly identified competent authorities, specific supervision and complaint procedures and an expressly defined administrative offence regime.

The regime is relevant, first and foremost, to so-called **providers of intermediary services**, that is, entities which, in the context of providing digital services, **transmit, store or host information provided by their users**, a category which may include access or data transmission services, **hosting services, online platforms and marketplaces**, although the specific obligations that apply vary according to the nature of the service provided and, in certain cases, the size of the operator.

For that reason, the first step for any company carrying out this type of activity should be to determine whether the service it provides falls within the scope of the DSA and, if so, into which category it falls, since the set of obligations with which it must comply depends on that classification.

Once the scope of application has been established, the main change introduced by the enforcement law lies in the supervision model, since ANACOM (*Autoridade Nacional de Comunicações- Portuguese National Communications Authority*) is confirmed as the Digital Services Coordinator in Portugal and now takes on the central role in monitoring and supervising the regime, being responsible, among other functions, for receiving complaints, requesting information, carrying out investigative measures and adopting measures intended to ensure compliance with the DSA, without prejudice to the specific powers assigned to ERC (*Entidade Reguladora para a Comunicação Social- Portuguese Regulatory Authority for the Media*) and CNPD (*Comissão Nacional de Proteção de Dados- Portuguese Data Protection Authority*) in certain matters.



This new framework is equally relevant to users, who now have a clearly identified national authority to which they may turn when they consider that a provider has failed to comply with the DSA rules, particularly in situations relating to **illegal content, the removal or restriction of content, the suspension or closure of accounts or the operation of the complaint mechanisms made available by the platform itself**, with ANACOM being able, where the provider is established in another Member State, to forward the complaint to the competent authority in that country.

This recent legislation also provides for the creation of a communication platform managed by ANACOM, through which certain communications may be exchanged between authorities and providers, including requests for information and orders intended to require action in relation to illegal content, and **the companies concerned should therefore ensure that their points of contact are kept up to date** and are effectively monitored, so that any communication received can be immediately identified, forwarded to the responsible department and dealt with within the applicable time limit.

This platform should not, however, be confused with the mechanisms that providers themselves must make available to users, among which, in the case of hosting services, the notification and action mechanism, or notice and action,

“FOR COMPANIES, THESE OBLIGATIONS TRANSLATE INTO A VERY CONCRETE NEED FOR INTERNAL ORGANISATION, SINCE IT IS NOT SUFFICIENT MERELY TO MAKE A CONTACT ADDRESS OR FORM FORMALLY AVAILABLE, AND PROCEDURES MUST EXIST THAT MAKE IT POSSIBLE TO KNOW WHO RECEIVES EACH COMMUNICATION, WHO ANALYSES IT, WHAT DECISION MUST BE TAKEN, WITHIN WHAT TIME LIMIT AND HOW THE HANDLING OF THE SITUATION WILL BE DOCUMENTED.”

is particularly important, as it allows the existence of content considered to be illegal to be notified to the platform so that the platform can assess the situation and decide whether to remove, restrict or retain the content in question.

Where an online platform is concerned, an internal complaint-handling system may also be required in order to **allow the user to challenge certain decisions already taken by the platform**, namely the removal of content, the suspension of the service or the closure of an account, and it is therefore essential to distinguish between the two mechanisms: while the first makes it possible to flag the existence of potentially illegal content, the second makes it possible to challenge the decision subsequently adopted by the provider.

For companies, these obligations translate into a very concrete need for internal organisation, since it is not sufficient merely to make a contact address or form formally available, and procedures must exist that make it possible to know who receives each communication, who analyses it, what decision must be taken, within what time limit and how the handling of the situation will be documented.

The review should therefore cover points of contact, terms and conditions, content

moderation policies and notification and complaint mechanisms and, where applicable, other specific matters provided for in the DSA, such as the identification of traders using marketplaces, advertising transparency, the protection of minors or the use of interfaces capable of unduly influencing users' choices.

The need to ensure effective compliance with these obligations is reinforced by the sanctions regime now established, which identifies the conduct capable of constituting an administrative offence and lays down the fines applicable according to the infringement committed, with the relevant maximum limit, in the case of legal persons, potentially corresponding to 1% or 6% of the annual worldwide turnover achieved in the financial year immediately preceding the decision imposing the penalty.

In conclusion and in practical terms, the main change brought about by the enforcement law therefore consists in enabling compliance with the DSA to be supervised and enforced in Portugal, and providers should therefore begin by confirming whether the regime applies to them, identifying the obligations corresponding to the service they actually provide and verifying whether the mechanisms required by the Regulation not only formally exist, but operate effectively, in an organised manner and in a way that can be demonstrated to users and authorities.