Chambers AND PARTNERS

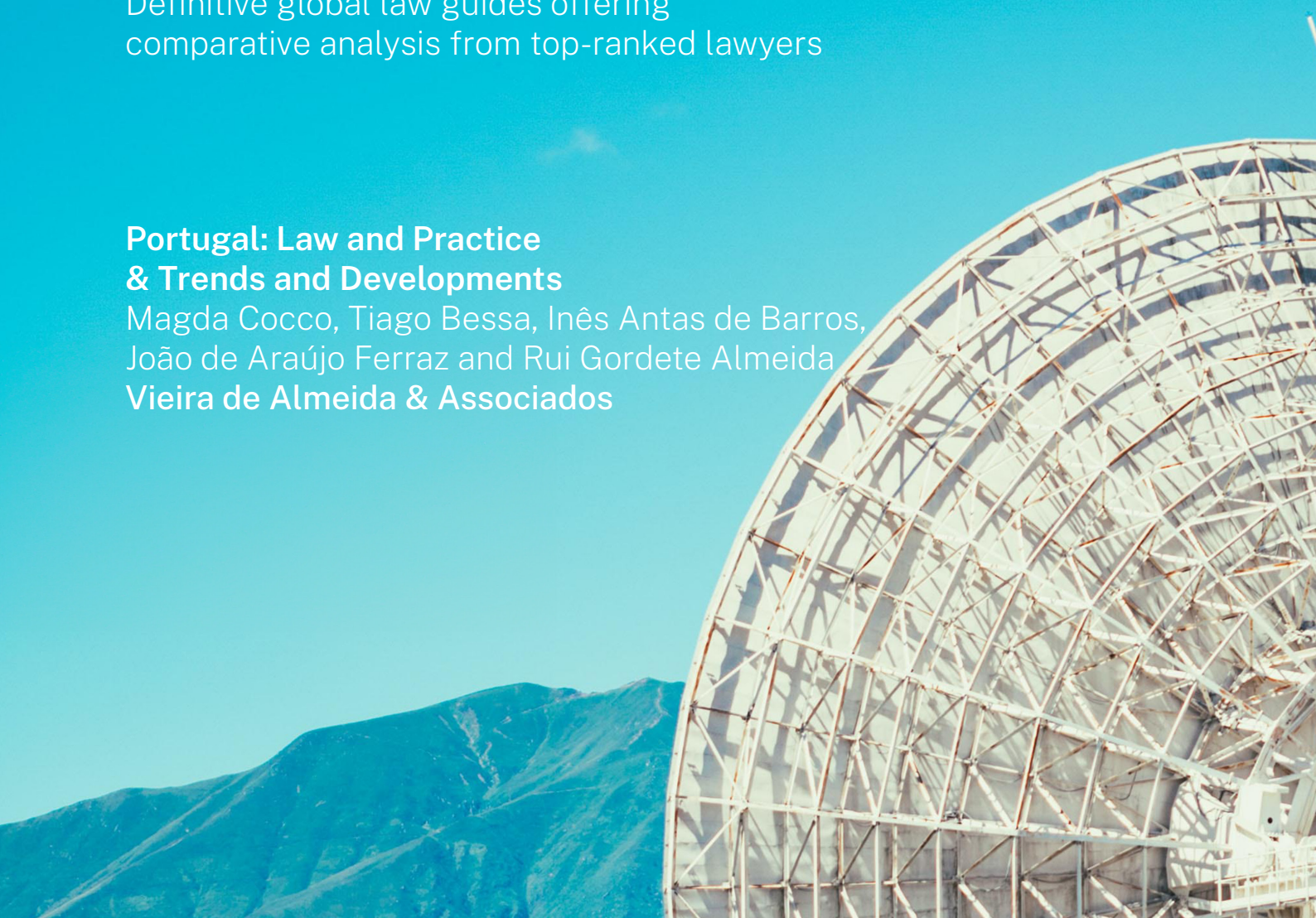
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Portugal: Law and Practice & Trends and Developments

Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida
Vieira de Almeida & Associados



Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui G
Vieira de Almeida & Associados

Law and Practice

Contributed by:
Magda Cocco, Tiago Bessa, Inês Antas de Barros,
João de Araújo Ferraz and Rui Gordete Almeida
Vieira de Almeida & Associados

Contents

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida,
Vieira de Almeida & Associados

Vieira de Almeida & Associados is a leading international law firm with more than 50 years of history, recognised for its impressive track record and innovative approach in corporate legal services. The excellence of its highly specialised legal services, covering several industries and practice areas, enables VdA to overcome the increasingly complex challenges faced by its clients. Recognition of the excellence of its work is shared by the entire team, as well as by clients and stakeholders, and is acknowledged by leading professional associations, legal publications, and academic entities. VdA has been consistently recognised for its outstanding and innovative services, having received the most prestigious international accolades and awards of the legal industry. Through the VdA Legal Partners network, clients have access to eight jurisdictions (Angola, Brazil, Cabo Verde, Mozambique, Portugal, Sao Tome & Principe, Spain, and Timor-Leste), with a broad sectoral coverage in all Portuguese-speaking countries.

Authors

Magda Cocco is group executive partner at VdA and head of digital frontiers, with a recognised practice spanning the full digital regulatory ecosystem across Europe and Africa. Known for her innovative, value-driven advice on complex transactions, policy strategy, and legislation drafting, she was appointed independent expert drafting the EU AI Office's General-Purpose AI Code of Practice. Magda serves on the Portuguese Quantum Institute board, and is a member of the WEF AI Governance Alliance, IBA Electronic Communications Committee Officer, EU D4D Hub Advisory Group, and APDC's Strategic Advisory Board. Ranked Band 1 in Chambers Europe (TMT – Portugal) for over 16 years and Band 2 in Chambers Global (TMT – Africa-wide).

Tiago Bessa is head of the ICT practice and partner of IP Transactions at VdA, working on matters across electronic and postal communications, media, entertainment, gaming and technologies. He has deep expertise in digital, copyright, internet and consumer law, contributing to innovative technological projects in Europe and Africa. Tiago has supported governments and regulatory entities in regulatory policy development and legislative drafting, advising organisations such as the International Telecommunications Union, the World Bank and the European Investment Bank. He also represents VdA in WhatNext.Law, an R&D centre dedicated to leveraging the impactful opportunities created by the ongoing digital transition worldwide.

Inês Antas de Barros is a partner in the information, communication & technology practice at VdA, with extensive experience in innovative technological projects in the electronic communications industry across Europe and Africa. She has worked in multidisciplinary ICT teams, assisting governments and regulatory entities in defining regulatory policies and legislative drafting, while also advising international organizations such as the International Telecommunications Union and the World Bank. Her practice focuses on privacy and information security, contributing to projects across multiple sectors involving data protection, cybersecurity challenges and related legal issues. She provides strategic guidance to clients around the world navigating today's complex digital regulatory landscapes.

João de Araújo Ferraz is a senior associate in the ICT practice at VdA, where he provides specialist advice to companies and public entities from different sectors on various legal issues in the digital economy, namely cybersecurity and emerging technologies. He regularly works on various operations, with particular focus on electronic communications issues. He also provides advice on public consultations, contract negotiations, drafting legal memoranda, litigation and drafting proposals for various legal and regulatory instruments. He has worked with several Portuguese-speaking African countries, particularly Angola, Cabo Verde, and São Tomé and Príncipe, as well as Timor-Leste.

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida,
Vieira de Almeida & Associados

Rui Gordete Almeida is a senior associate in the ICT practice at VdA. He has been actively involved in a wide range of projects in the ICT field, notably telecommunications, consumer protection, data protection, artificial intelligence, digital identity, cybersecurity and emerging technologies. His work includes responses to public consultations, contract negotiations, preparation of legal memoranda and opinions, litigation, drafting of proposals for various pieces of legislation or regulations. He has worked with several Portuguese-speaking African countries as well as Timor-Leste. Rui is a member of the International Bar Association (IBA).

Vieira de Almeida & Associados

28 Rua Dom Luís I
1200-151 Lisboa
Portugal

Tel: (+351) 213113400
Fax: (+351) 213548939
Email: vieiradealmeida@vda.pt
Web: www.vda.pt

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida,
Vieira de Almeida & Associados

1. Digital Economy

1.1 Legal Framework

As an EU Member State, Portugal's digital economy framework is largely shaped by harmonised EU legislation aimed at promoting market fairness, consumer protection and digital trust. Key instruments include:

- Online intermediary services and content moderation legal framework: Regulation (EU) 2022/2065 Digital Services Act (DSA) and the national implementing law (the recently approved draft law 25/XVII/1).
- E-Commerce legal framework: Decree-Law no. 7/2004.
- Digital content and digital services consumer contracts: Decree-Law no. 84/2021, which transposes Directive (EU) 2019/770.
- Cybersecurity legislation: Law no. 46/2018 and Decree-Law no. 65/2021, both transposing the NIS 1 Directive, and, more recently, Decree-Law no. 125/2025, transposing Directive (EU) no. 2022/2555 (NIS2 Directive), which enters into force on 3 April 2026, and Decree-Law no. 22/2025, transposing Directive (EU) no. 2022/2557 (CER Directive).
- Data protection rules: Law no. 58/2019, Regulation (EU) no. 2016/679 (GDPR), Regulation (EU) no. 2023/2854 (Data Act) and Regulation (EU) no. 2022/868 (Data Governance Act).
- Electronic identification and trust services: Decree-Law no. 12/2021 and Regulation (EU) no. 2024/1183 (eIDAS 2 Regulation).
- Electronic communications law: Law no. 16/2022 (ECL), which transposed Directive (EU) no. 2018/1972 (European Electronic Communications Code).

Portugal has also reinforced its digital policy agenda through an updated National Digital Strategy, which prioritises public-sector digitalisation, business transformation, cybersecurity, digital inclusion and the green–digital transition.

Recent EU Developments

The EU has proposed a Digital Networks Act, aiming to update the current electronic communications regulatory framework embodied in the European Electronic Communications Code. The proposal aims to create a more integrated single market for high-quality digital networks that underpin the broader digital economy, including fibre, 5G/6G and advanced connectivity services.

1.2 Key Challenges

Portugal's digital economy is shaped by the continuous expansion of EU digital regulation and the rapid integration of advanced technology. Data governance remains a complex area, particularly in international data transfers, where GDPR safeguards must be balanced against the need to facilitate global digital trade. Addressing persistent digital divides also remains a policy objective, with targeted measures needed to improve digital access and skills among underserved regions, ageing populations and smaller businesses.

AI Governance

An additional central challenge concerns the implementation of AI governance obligations, as regulators and market participants work to support innovation while enforcing new requirements on oversight, risk classification and accountability.

Cyber Resilience

Cyber resilience has become a strategic priority. The growing reliance on digital infrastructure increases systemic exposure to cyber incidents, prompting policymakers to strengthen supervisory frameworks and encourage sustained investment in security, compliance and incident response capabilities.

1.3 Digital Economy Taxation

The taxation of digital goods and services in Portugal is largely shaped by the EU VAT system, with domestic rules closely following EU directives and recent reforms addressing digital business models. VAT is applied on a destination basis, meaning that tax liability is determined by the location of the customer rather than the supplier.

Key Compliance Challenges

From an operational perspective, compliance can be demanding, particularly for digital platforms and cross-border providers. Key challenges include:

- determining customer location;

- applying the appropriate VAT rate across jurisdictions; and
- meeting complex reporting requirements.

Although simplification tools such as the One-Stop Shop system have eased some administrative burdens, ongoing compliance remains resource-intensive, and areas of interpretative uncertainty continue to create exposure.

1.4 Taxation of Digital Advertising

Digital advertising income in Portugal is taxed under the EU VAT framework, with the applicable treatment depending on factors such as the supplier's tax residence, the B2B or B2C nature of the service and the customer's location. In cross-border contexts, destination-based VAT rules and reverse-charge mechanisms are commonly applied.

TMT companies typically rely on automated tax and invoicing systems aligned with Portuguese requirements, including SAF-T reporting, and maintain accurate records on customer identification and VAT status for compliance.

1.5 Consumer Protection

Portugal, as an EU member state, applies a consumer protection regime grounded in EU law and supplemented by national legislation. Key instruments include:

- general consumer protection rules (Law no. 24/96);
- e-commerce legislation (Decree-Law no. 7/2004);
- distance selling legislation (Decree-Law no. 57/2008 and Decree-Law no. 24/2014);
- data protection legislation implementing the GDPR (Law no. 58/2019);
- specific requirements for digital content and services (Decree-Law no. 84/2021); and
- platform obligations under Regulation (EU) no. 2022/2065, the "Digital Services Act" (DSA).

Compliance Obligations

Within this framework, companies need to ensure transparency in contractual terms, pricing and digital content features, apply fair contractual conditions, safeguard personal data and ensure secure digital transactions, while maintaining effective customer support.

Dispute Resolution

Consumer disputes are resolved through a combination of alternative dispute resolution mechanisms and court proceedings, with arbitration, mediation and *julgados de paz* commonly used for lower-value claims. In practice, structured internal complaint-handling systems and alternative dispute resolution mechanisms are increasingly relied upon to manage disputes efficiently and reduce litigation and reputational risk.

1.6 The Role of Blockchain in the Digital Economy

Overview

Blockchain forms part of Portugal's digital ecosystem, primarily within defined and specialised use cases in the TMT sector. Beyond crypto-assets, deployment tends to be selective, with applications emerging in areas such as digital identity, smart contracts and limited platform governance functions.

Regulatory Classification and Compliance

The main legal challenges stem from regulatory classification and compliance. Despite the introduction of a comprehensive EU framework under Regulation (EU) no. 2023/1114, (the MiCA Regulation), and the expansion of AML obligations to crypto-asset service providers, legal uncertainty may still arise around the legal characterisation of tokens, licensing requirements and the application of securities law to specific use cases.

Additional compliance challenges stem from the pseudonymous nature of blockchain transactions in the context of AML/CFT rules and the tension between ledger immutability and GDPR principles, particularly data minimisation and erasure rights.

AML Obligations

In the AML domain, crypto-asset service providers that fall within the definition of the MiCA Regulation, regardless of whether they are otherwise subject to the remaining provisions of Law no. 83/2017 (AML Law) have become subject to the MiCA Regulation's enforcement measures as provided for in the AML Law. They are therefore subject to a set of obligations

aimed at mitigating risks associated with transfers of funds and crypto-assets, including:

- customer due diligence;
- examination, detection and reporting of suspicious transactions and irregularities to the authorities; and
- ensuring compliance with restrictive measures.

Registration with the *Banco de Portugal* (the Portuguese Central Bank and banking regulator) is mandatory, as it is the competent authority in Portugal responsible for verifying compliance with MiCA and the AML Law. Crypto-asset service providers are subject to the sanctions regime under the AML Law in the event of non-compliance. Depending on their features, token issuances may also qualify as securities and fall under the supervision of the *Comissão de Mercado de Valores Mobíliarios* (CMVM), the Portuguese Securities Market Commission, responsible for regulating and supervising the securities market and all agents operating within it.

Overall, Portugal's approach aims to support innovation while managing financial, technological and governance risks in line with evolving EU standards.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

General Framework

In Portugal, cloud and edge computing services that process personal data are subject to the GDPR, complemented by Law no. 58/2019, which ensures its application in Portugal. The GDPR also applies to non-EU based cloud and edge providers when they process personal data of subjects located in the EU. In such cases, transfer impact assessments must be carried out and appropriate safeguards must be implemented, particularly where foreign laws may require access to the data. The Data Act also introduces cloud switching and interoperability obligations. Unjustified data-localisation requirements for non-personal data are also prohibited under Regulation (EU) 2018/1807. The regulation also applies to cloud and data-centre services.

Controller–Processor Obligations

In most cases, cloud service providers act as processors under the GDPR. This means that controllers must enter into contracts with these providers, governing matters such as processing instructions, security measures, data return or deletion when the contract ends. Regulators also stress the importance of data portability and having clear exit strategies when changing providers.

EU Policy Developments

EU policy developments are expected to further strengthen security and governance requirements. These include planned initiatives such as the European Commission's Cloud and AI Development Act, which aims to promote a secure and competitive European cloud and AI ecosystem.

Sector-Specific Requirements

Sectors that handle large amounts of sensitive or critical data, such as banking and finance, insurance, healthcare and telecommunications, are subject to stricter supervisory and sector-specific rules. These often require higher security, resilience, and audit standards in cloud outsourcing agreements, as well as close control of international data transfers.

Under the NIS2 Directive, public authorities, critical infrastructure operators, essential service providers and digital service providers must implement appropriate technical and organisational security measures and report significant incidents. These requirements also affect cloud and edge computing deployments.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

The EU AI Framework

Portugal applies the EU's horizontal AI regime, with Regulation (EU) 2024/1689 (EU AI Act) as the primary, directly applicable instrument. The EU policy environment continues to evolve, including:

- The AI Continent Action Plan – focused on strengthening European AI capabilities and uptake.

- The Apply AI Strategy – driving AI deployment in key sectors.
- The general-purpose AI (GPAI) Code of Practice – intended to support compliance for providers of GPAI models.
- The Digital Omnibus initiative – aimed at streamlining and aligning parts of the EU digital rulebook, in particular by delaying the AI Act's obligations by up to 16 months to December 2027.
- The Data Union Strategy – to unlock data access and boost AI innovation.
- The draft implementing act establishing AI regulatory sandboxes – to support controlled testing of compliant AI systems.
- The Memorandum of Understanding on AI gigafactories, – to accelerate large-scale AI infrastructure in Europe.
- The First Draft Code of Practice on Transparency of AI-Generated Content – to promote disclosure and traceability of synthetic content.

Complementary Legal Frameworks

Beyond the EU AI Act, AI-related activities must also comply with the GDPR, consumer and product safety rules, cybersecurity requirements as well as civil and criminal law.

National Measures

In addition to *Autoridade Nacional de Comunicações* (ANACOM) serving as the national AI authority (which also acts as the Portuguese telecoms and postal regulator), Portugal has adopted the National AI Agenda (*Agenda Nacional de Inteligência Artificial*, ANIA) through Council of Ministers Resolution no. 2/2026. This agenda aims to promote responsible AI adoption and strengthen institutional capacity.

Complementing ANIA, the National Digital Strategy Action Plan 2026–2027 advances cloud sovereignty, data spaces, interoperability and cybersecurity, and creates public-sector enablement mechanisms to scale responsible AI adoption in government and the economy.

Deepfakes and AI in Transport

Portugal still has no laws specifically targeting deepfakes or AI in transport. However, existing laws may still apply. Deepfakes may give rise to liability under existing civil liability rules (including claims for damages), cybercrime and fraud offences under Law no. 109/2009 (the Cybercrime Law), and the GDPR, since a person's image and voice qualify as personal data.

Pilots and testing of self-driving features rely on EU law, most notably Regulation (EU) no. 2019/2144 (the Vehicle General Safety Regulation). For drones, the regime is defined by Regulation (EU) no. 2018/1139, on common rules in the field of civil aviation, and the EU Drone Regulations (Regulation (EU) no. 2019/945 and Regulation (EU) no. 2019/947), implemented domestically via Decree-Law no. 87/2021.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Applicable Legal Framework

IoT solutions may be subject to a set of cross-cutting EU and national legal instruments, depending on the specific solution's characteristics.

Electronic Communications

At the forefront, IoT solutions may be subject to the ECL to the extent that these qualify as connectivity services falling under the electronic communications services' definition provided therein. In such cases, sector-specific conditions apply, including the obligation to obtain a general authorisation to provide such services from the national regulatory authority (ANACOM).

In this context, rules on legal interception, personal data and communications privacy apply where IoT and machine-to-machine communications are qualified as electronic communications services and/or networks, notably pursuant to Law no. 41/2004, which transposes Directive 2002/58/EC (ePrivacy Directive). This law sets obligations relating to confidentiality and security of communications and regulates the processing of traffic and location data.

Data Protection

IoT and machine-to-machine solutions that entail the processing of personal data are fully subject to the GDPR (and the implementing Law no. 58/2019),

including data minimisation, purpose limitation, security of processing, breach notification and privacy by design and by default requirements.

The Data Act

IoT solutions may also be subject to the Data Act, which establishes harmonised rules on access to and use of data generated by connected products and related services, granting users access and sharing rights and regulating data sharing with public sector bodies in cases of exceptional need.

Cybersecurity

Cybersecurity obligations may arise where IoT solutions support essential or important entities under the NIS2 Directive. In Portugal, the NIS2 Directive has been transposed by Decree-Law no. 125/2025, covering risk management, incident reporting, supply-chain security and governance. In parallel, Regulation (EU) no. 2024/2847 (the Cyber Resilience Act) introduces horizontal essential cybersecurity requirements for products with digital elements, including vulnerability handling, updates and conformity assessment across the lifecycle.

AI in IoT

The EU AI Act is increasingly relevant to IoT ecosystems where connected devices integrate AI systems or models for monitoring, profiling, prediction, or automated decision-making.

4.2 Compliance and Governance

Companies deploying IoT solutions in Portugal face significant compliance challenges arising from the combined and lifecycle-based application of EU data, product and cybersecurity frameworks, in addition to the electronic communications regulatory framework.

Data Governance

A central challenge is compliance with the Data Act, which introduces obligations connected with data generated by connected products, including:

- pre-sale transparency;
- free and machine-readable user access;
- user-directed data sharing with third parties; and
- mandatory business-to-business data sharing under fair, reasonable, and non-discriminatory conditions where required by law.These obligations are particularly complex in IoT ecosystems involving personal and non-personal data and multiple actors across the value chain.

Cybersecurity Compliance

The Cyber Resilience Act establishes essential cybersecurity requirements for products with digital elements, including vulnerability management, defined security update lifecycles and incident and vulnerability reporting obligations. Manufacturers, importers, and distributors must prepare for conformity assessments and CE marking within applicable transition periods.

Data Protection

The GDPR imposes strict requirements on data minimisation, purpose limitation, security, accountability, breach notification and the performance of Data Protection Impact Assessments for high-risk processing. These obligations are particularly demanding in IoT contexts characterised by continuous, passive personal data collection and extensive inferential capabilities.

Governance Frameworks

To manage these overlapping requirements, companies should adopt integrated governance frameworks aligning Data Act compliance, cybersecurity under the Cyber Resilience Act, and privacy governance under the GDPR, supported by coordinated legal, technical and organisational measures across the product.

4.3 Data Sharing

IoT companies in the EU operate primarily under the GDPR, the EU Data Act, the Data Governance Act and applicable sector-specific regimes.

General Data Protection Regulation

Under the GDPR, any sharing of personal data must comply with the principles of lawfulness, fairness, transparency, purpose limitation and data minimisation, and rely on a valid legal basis (consent, contract, legal obligation, or legitimate interests). Controllers must clearly inform users about what data is shared, with whom, and for what purposes and must implement appropriate security and accountability measures.

Special category data (health, biometric, or genetic data) are subject to strict conditions, enhanced safeguards, and typically require Data Protection Impact Assessments. Criminal offence data and children's data attract additional protections under both EU and Portuguese law. In combined personal and non-personal data sets, the GDPR and the Data Act apply concurrently, requiring logical separation, purpose binding, role-based access controls and protection of trade secrets and confidential business information.

Data Act

The Data Act establishes a user-centric framework for data generated by connected products and related services. Users have the right to access such data and to instruct data holders to share them with third parties of their choice. The regulation also introduces pre-contractual transparency obligations and design duties for manufacturers and service providers.

Where a legal obligation to make data available exists under either EU or national law, business-to-business data sharing must occur on fair, reasonable and non-discriminatory terms, with restrictions on unfair contractual clauses and enhanced protections for Small and Medium Enterprises. For cloud and data processing services, the Data Act introduces a switching and interoperability regime, progressively removing switching charges, with full elimination by 12 January 2027.

Data Governance Act

The Data Governance Act complements this framework by regulating data intermediation services and the re-use of certain categories of protected public-sector data, with the objective of fostering trust in voluntary and cross-sector data sharing.

Sector-Specific Rules

Sector-specific rules (including healthcare, finance, energy, or electronic communications) may impose additional confidentiality, security, or notification obligations. Where IoT or machine-to-machine connectivity qualifies as an electronic communications service, ePrivacy-style secrecy of communications may apply to both content and metadata.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Provision of audiovisual media services (AVMS) in Portugal is subject to a set of requirements and procedures that must be met by television broadcast services, operators and distributors, video-sharing platform services and providers, as well as by on-demand audiovisual services and providers.

Television Broadcasting Services

According to Law no. 27/2007 (the Television Law), television broadcasting may only be pursued by companies with varying fixed minimum share capital and whose main corporate purpose is to carry out such activities. Television broadcasting services, operators and distributors, if subject to Portuguese jurisdiction according to Articles 2 and 28a of Directive no. 2010/13/EU, should be registered with the *Entidade Reguladora para a Comunicação Social* (ERC), the Portuguese Media Regulatory Authority.

Provision of television broadcasting services may be accessed by two means.

- Licensing via public tender launched by the government, if the services use terrestrial radio spectrum for the purpose of organising unconditional access television programme services (in the case of operators) or selecting and aggregating television programme services with conditional access or subscription-based access (in the case of distributors).
- Authorisation via application before the ERC, if the services do not use the terrestrial radio spectrum and are distributed through a licensed distributor, typically via a fixed network (cable or optical fibre).

Licences and authorisations, which are non-transferable, are issued for a period of 15 years and are renewable for equal periods. Every five years, including upon renewals, the ERC conducts periodical assessments in order to ascertain compliance with the legal and regulatory preconditions of the licence or authorisation. The Television Law safeguards freedom of reception and retransmission from other EU Member States.

Video-Sharing Platform Services and On-Demand Audiovisual Services

Video-sharing platform services and on-demand audiovisual services are also within the scope of the Television Law, as amended by Law no. 74/2020, which transposes into national law Directive (EU) no. 2018/1808. However, they are not subject to the same requirements and procedures set forth above for television broadcasting services, thus benefitting from a considerably simpler regime.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

Scope of Application of Electronic Communications Rules

The Electronic Communications Law (Law no. 16/2022) comprises the core regulatory framework for electronic communications networks and services in Portugal. The ECL applies to electronic communications networks and services, associated facilities and services, including:

- fixed and mobile electronic communications services, such as public switched telephone networks (PSTN) and voice over internet protocol (VoIP) telephony, mobile voice and SMS, as well as broadband internet access;
- transmission services used for broadcasting, namely electronic communications services that underpin the transmission and distribution of audiovisual or radio content;
- interpersonal communications services, both number-based and number-independent, including OTT communications services;
- machine-to-machine and IoT connectivity services and networks;
- private and enterprise electronic communications networks and services; and
- satellite and space-based communications services, including low Earth orbit satellite internet services, satellite-enabled broadband services and earth station services.

Requirements Prior to Market Entry

As a rule, the provision of electronic communications networks and services does not depend on the prior granting of an individual licence from ANACOM. Instead, it is subject to the simpler general authorisation regime, which determines that undertakings intending to provide electronic communications networks or services must notify ANACOM before commencing their activity in Portugal. Following the notification, companies can start their activity immediately, while also becoming subject to the set of regulatory obligations associated with the general authorisation regime.

Notwithstanding the above, the use of radio frequencies and numbering resources remains subject to separate regulatory procedures, including the granting of individual rights of use if required.

Security Requirements

The ECL imposes extensive security obligations on providers of electronic communications networks and services, for safeguarding the integrity, availability and confidentiality of networks and services. ANACOM has supervisory and enforcement powers, including the power to define technical and organisational security requirements, issue binding instructions, require security audits, monitor compliance and adopt corrective or sanctioning measures.

ANACOM's Regulation no. 303/2019, on the security and integrity of electronic communications networks and services, deepens these obligations and requires undertakings to:

- designate a Chief Security Officer;
- define, implement and maintain a security policy;
- conduct security audits of their networks and services; and
- submit periodic security reports to ANACOM.

Non-compliance with the security obligations set forth in the ECL and Regulation no. 303/2019 may result in administrative fines and, in cases of repeated infringements or serious negligence, operational restrictions or revocation of the right to operate. While these obligations are, in practice, still being enforced by ANACOM, they are expected to become formally revoked

in the near future, per Decree-Law no. 125/2025. This framework sets out horizontal cybersecurity obligations and applies to providers of public electronic communications networks and services.

6.2 Net Neutrality Regulations

In Portugal, net neutrality is primarily governed by Regulation (EU) no. 2015/2120 on open internet access, which establishes that, as a rule, internet access providers must treat all traffic equally, without discrimination, restrictions or interferences, regardless of content, applications, services, end users or equipment.

In exceptional circumstances, providers are allowed to introduce measures not aligned with this principle to:

- comply with legal obligations or binding decisions;
- preserve the security and integrity of networks and services or terminal equipment; and
- prevent or mitigate temporary or exceptional network congestion.

These rules aim to ensure competition in electronic communications and adjacent markets, strengthening end user protection and market transparency by limiting discriminatory traffic practices. However, they also impose significant constraints on providers by requiring ongoing investments in capacity planning, monitoring and auditable controls to justify any exceptional traffic management measures strictly on technical and legal grounds.

6.3 Emerging Technologies

Overview

Emerging technologies such as 5G, IoT and AI are accelerating the convergence of electronic communications, digital services and data-driven business models, reshaping electronic communications services and networks. 5G provides the core connectivity layer enabling massive IoT deployments and low-latency communications, while AI increasingly supports network planning, management, optimisation and security.

In Portugal, as across the EU, this convergence has increased regulatory focus on network resilience, cybersecurity (with special focus on Decree-Law no. 125/2025 and the EU 5G Toolbox), infrastructure deployment, data and consumer protection, reflecting the growing strategic importance of electronic communications infrastructures.

Infrastructure and Connectivity

The deployment of and access to 5G and IoT-enabled physical infrastructures are governed by Regulation (EU) no. 2024/1309 (the Gigabit Infrastructure Act), which aims to accelerate fibre, backhaul and 5G networks by:

- facilitating access to their supporting infrastructures;
- introducing single information points;
- simplifying permitting procedures; and
- requiring new buildings and major renovations to be “fibre-ready” or “gigabit-ready”.

This framework operates alongside the national regime under Decree-Law no. 123/2009, which transposed Directive 2014/61/UE (the Broadband Cost Reduction Directive), and is expected to be amended soon.

AI in Telecommunications

The AI Act applies to AI systems used in electronic communications, particularly high-risk applications, introducing additional obligations on transparency, risk management and non-discrimination. Although no national implementing legislation has yet been adopted, the National Artificial Intelligence Agenda, approved by Resolution of the Council of Ministers no. 2/2026, anticipates increased computational demands and greater reliance on cloud and edge computing. This will have implications for network coverage and architecture, security and regulatory compliance, whilst increasing interdependence between telecommunications, cloud services and data infrastructures.

Cybersecurity

The NIS2 Directive, transposed into Portuguese law by Decree-Law no. 125/2025, also expands cybersecurity obligations for entities in the telecommunications and digital infrastructure sectors. Providers of electronic communications networks and services are classified as essential or important entities and must implement comprehensive risk management

measures, report significant incidents to competent authorities and ensure supply chain security.

Practical Implications

Companies integrating 5G, IoT, and AI technologies must address a broad set of legal requirements, including spectrum licensing and usage conditions, network security and resilience, cybersecurity compliance, data protection, infrastructure access and territorial planning. Given the complexity and overlap of these regimes, an integrated legal and regulatory compliance approach from the outset is essential, namely to ensure that product and service development is aligned with this.

7. Challenges With Technology Agreements

7.1 Legal Framework Challenges

Technology Agreements: Main Challenges and Specificities

Organisations entering into technology agreements in Portugal face recurring challenges under the influence of European regulatory frameworks. Portugal does not have a single, standalone legal instrument for technology agreements; instead, these are governed by multiple overlapping legal regimes. These challenges encompass four main areas.

- Intellectual property – ensuring clear ownership and licensing terms for IP rights, covering pre-existing IP, deliverables, jointly developed works and employee-created IP (such as computer programs, software and databases), particularly under Decree-Law no. 63/85 as amended (the Copyright and Related Rights Code), Decree-Law no. 252/94 (the legal protection regime for computer programs), Directive no. 2009/24/EC (the Software Directive), and Decree-Law no. 122/2000 (the databases legal protection regime), transposing Directive no. 96/9/EC (the Database Directive).
- Data protection – compliance with the GDPR and Portugal's implementing Law no. 58/2019, imposing strict controller–processor obligations and lawful data transfers. These frameworks require written agreements between controllers and processors and only permit transfers outside the EU where there is adequate protection or safeguards (such as Standard Contractual Clauses per Commission Implementing Decision (EU) no. 2021/914 or Binding Corporate Rules) in place.
- Cybersecurity – including risk management, incident reporting and supply chain security across various sectoral laws, especially the NIS2 Directive, as transposed by Decree-Law no. 125/2025, which imposes mandatory cybersecurity measures and incident notifications for essential and important entities, and the Data Act, which introduces mandatory requirements for data portability and interoperability for data processing services. Contracts should allocate NIS2 Directive roles/duties, establish incident reporting mechanisms, SLA terms and right-to-audit for critical suppliers.
- Standard contractual clauses – Portugal's regime on standard contractual clauses under Decree-Law no. 446/85 addresses abusive clauses and requires clarity and prior communication in contracts. Terms enabling unilateral price changes, broad liability exclusions, or forum selection that materially prejudice the counterparty may be struck if not aligned with the legal requirements.

Regulated Industries and Greater Restrictions

Some regulated sectors in Portugal are subject to additional restrictions. For instance, banking and financial services are governed by Regulation (EU) 2022/2554 (the DORA Regulation), requiring comprehensive ICT risk management, resilience testing (including threat-led penetration testing), incident reporting, oversight of critical ICT third-party providers, including contractual rights to audit, data access and exit strategies.

7.2 Service Agreements and Interconnection Agreements

Key Elements in Electronic Communications Services Agreements

Electronic communications services agreements in Portugal are shaped by key mandatory provisions under Law no. 16/2022, transposing the European Electronic Communications Code. Key elements to include are listed below.

- Scope, disclosures and contract summary – clearly specifying the types and features of services, pro-

viding required pre-contractual information, and a concise, durable contract summary. For bundled or enterprise contracts, tailored summaries help avoid ambiguity.
- Transparency, pricing and billing – publishing tariffs and standard conditions, clearly itemising bundle components and prices and specifying acceptable price variation methods. Agreements should enable free consumption alerts and detailed billing, negotiate limits on price indexation, seek precise change-control triggers, and align with Law no. 16/2022 transparency duties.
- Quality of service and remedies – including measurable service level agreements for key metrics such as latency, jitter, packet loss and data speeds (minimum/typical/maximum). In the case of retail end-user contracts, remedies must allow for cost-free termination in cases of recurring non-conformity, as per Law no. 16/2022, and negotiation of service credits, step-in rights and termination.
- Duration, changes and switching – offering options both with and without binding periods; binding periods are capped at 24 months and must provide consumer benefits. Termination rights apply after automatic renewal (maximum one-month notice) and for contractual changes not exclusively beneficial or legally required. Seamless switching, portability, delay compensation and refunds for prepaid services must be provided.
- Accessibility and security – ensuring service accessibility, disclosing emergency access information, complying with data protection, integrating security-by-design/by-default, notifying customers of threats, and including terms for incident cooperation, liability allocation and audit rights.

Companies should closely monitor future legal developments, as the Digital Networks Act, which will replace the European Electronic Communications Code, proposed on 21 January 2026, may introduce relevant changes to the legal landscape in this regard.

Interconnection Agreements

In Portugal, interconnection agreements are mostly regulated by the ECL. Key considerations for companies entering interconnection agreements include:

- defining scope and modalities of interconnection services, including traffic and IP interconnection;
- aligning with technical standards and specifications for network interfaces;
- setting clear obligations for collaboration, communication, and technical changes and future development;
- addressing dimensioning, installation and operation of interconnection circuits, including redundancy, cost allocation and maintenance;
- establishing network management, fault resolution and service continuity procedures;
- including provisions for data protection, confidentiality and cybersecurity;
- defining service quality levels and remediation measures;
- tackling illicit practices, ensuring lawful use of interconnection circuits and prevention of fraudulent activity; and
- including dispute resolution, ANACOM involvement, service suspension, termination, liability, force majeure and agreement reviews.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Primary Legislation

The primary legislation governing trust services, electronic signatures, and digital identity in Portugal and across the EU is Regulation (EU) no. 910/2014 (the eIDAS Regulation), implemented nationally by Decree-Law no. 12/2021. This regime addresses the validity, effectiveness and probative value of electronic documents, recognition of electronic identification for natural and legal persons, and rules for the State Electronic Certification System (SCEE), based on public key infrastructure. Providers of qualified trust services are strictly liable for damages from non-compliance and must maintain sufficient insurance.

Data Protection

All processing and management of personal data is subject to the GDPR and Law no. 58/2019, ensuring secure processing, data minimisation, valid user consent and breach notification.

Legislative Developments

Legislative developments include Decree-Law no. 125/2025 and the eIDAS 2 Regulation, which updates the eIDAS Regulation framework for new digital identity solutions and expanded trust services. In short, the eIDAS 2 Regulation provides for:

- cross-border recognition of electronic identification for natural and legal persons under notified national schemes and introduction of European digital identity wallets;
- harmonised trust service rules for legal certainty in electronic transactions EU-wide;
- a legal framework for electronic signatures, seals, timestamps, documents, registered delivery services, website authentication certificates, archiving, attribute attestation, signature creation devices, seal creation devices and ledgers.

Trusted Lists

The eIDAS Regulation and the eIDAS 2 Regulation require all Member States to establish, maintain and publish trusted lists, detailing qualified trust service providers and services. Commission Implementing Decision (EU) no. 2015/1505 sets the technical specifications and formats relating to these lists. In Portugal, the National Security Cabinet is the designated supervisory body responsible for the national trusted list.

The updated Portuguese trusted list issued on 27 January 2026 includes six active trust service providers:

- ACIN – iCloud Solutions, Lda.
- Agência para a Reforma Tecnológica do Estado, I.P.
- CEGER – Centro de Gestão da Rede Informática do Governo.
- DigitalSign – Certificadora Digital.
- Instituto dos Registos e do Notariado, I.P.
- MULTICERT – Serviços de Certificação Electrónica, S.A.

Digital Identity Schemes

Portugal's digital identity ecosystem is anchored by the eID Citizen Card and complemented by the Digital Mobile Key, Professional Attributes Certification System (SCAP), and ID.gov.pt wallet, with Autenticação.gov as the main electronic authentication and signature platform. These schemes ensure user control, data access, correction rights, and guarantee privacy and non-discrimination under both the Portuguese Constitution and the EU Charter.

9. Gaming Industry

9.1 Regulations

Overview

In addition to being subject to sector-specific regimes where there are elements of gambling or betting, gaming activity is also subject to general legal regimes. Key regulatory instruments include:

- Consumer Protection – Law no. 24/96 (general consumer rights) and Decree-Law no. 84/2021.
- The Digital Services Act.
- E-commerce and Intermediary Liability – Decree-Law no. 7/2004 and the DSA.
- Intellectual Property – Copyright and Related Rights Code and Decree-Law no. 110/2018 (the Industrial Property Code), software protection under Decree-Law no. 252/94.
- Online Gambling and Betting (RJO) – Decree-Law no. 66/2015.

While Portugal does not have a gaming-specific regulatory framework, Pan-European Game Information (PEGI) self-regulation is a voluntary, pan-European scheme widely used by Member States; it is not an EU "legal code" but an industry-led self-regulatory initiative.

Main Legal Challenges

Increasingly blurred boundary between gaming and gambling – the incorporation of specific features and monetisation models into games, particularly certain forms of loot boxes, continues to attract regulatory scrutiny, raising questions as to their possible alignment with gambling-like activities.

Gaming platforms with social functionalities – platforms that integrate social features face a growing set of regulatory and operational challenges, including content moderation obligations and the implementa-

tion of effective reporting arising from the Digital Services Act.

Intellectual property in digital and virtual environments – significant risks persist, notably in relation to piracy, unauthorised reproduction of assets and characters and the misuse of trademarks within virtual settings.

In-Game Purchases and Loot Boxes

In-game purchases may qualify as digital content or digital services and may therefore be subject to consumer protection rules on conformity, information duties and updates. Consumers are entitled to remedies such as repair, price reduction, or termination/refund in the event of non-conformity, in accordance with Decree-Law no. 84/2021.

Loot boxes present a particular challenge, where they involve payment, randomised outcomes and the attribution of a prize with economic value, they may fall within the concept of games of chance and thus be classified as gambling. In such cases, their offering is subject to licensing and regulatory requirements under Decree-Law no. 66/2015.

Age Ratings and Content Restrictions

In Portugal, video games carry age ratings overseen by IGAC and must be sold in line with that label (Decree-Law no. 23/2014). Online gambling and betting services, as well as content comparable to games of chance, are in principle restricted to individuals aged 18 and over, pursuant to Decree-Law no. 66/2015.

The legal requirements for game developers in terms of content restrictions require compliance with Portuguese criminal and civil law, particularly rules prohibiting illegal or harmful content and ensuring the protection of minors. For games with online or social features, developers may also be subject to the Digital Services Act, which sets obligations on the handling of illegal content and the safeguarding of minors, while consumer and gambling laws may further limit certain content and monetisation practices.

9.2 Regulatory Bodies

In Portugal, multiple authorities oversee gaming compliance:

- *Serviço de Regulação e Inspeção de Jogos* (SRIJ) licenses and supervises gambling under Decree-Law no. 66/2015;
- *Inspeção-Geral das Atividades Culturais* (IGAC) is responsible for age classification and the supervision of the public exhibition and distribution of videograms (as video games);
- *Comissão Nacional de Proteção de Dados* (CNPD) enforces data protection rules on player data, profiling, and online features; and
- *Autoridade de Segurança Alimentar e Económica* (ASAE) polices consumer protection standards, including advertising, pricing transparency and in-game purchase practices.

These authorities have broad enforcement powers, including inspection and audit rights, the ability to order the suspension or modification of unlawful practices, the imposition of administrative fines and ancillary sanctions and, where applicable, the seizure of equipment or referral for criminal proceedings.

Recent Enforcement Actions

The SRIJ has taken enforcement action against unlicensed online gambling platforms operating without the required authorisation in Portugal.

9.3 Intellectual Property

IP Challenges Faced by Game Developers

Game developers face heightened IP exposure from piracy and unauthorised copying with rapid online and streaming distribution, disputes stemming from poorly scoped or mismanaged licences (including music, third-party characters and proprietary engines), and the complexity of enforcing rights across multiple jurisdictions with divergent copyright, trademark and software laws.

Legal Protection of IP in Virtual Environments

Portugal provides robust legal protection for game developers through the Copyright and Related Rights Code, which safeguards creative content and software. Game titles, branding, technologies and visual elements are protected by Decree-Law No. 252/94 on the legal protection of computer programs and the Industrial Property Code. Game developers hold copyright protection over the original digital assets they create, including character models, maps, ani-

mations and in-game environments. Developers may enforce these rights through measures such as court injunctions or claims for damages. Contractual arrangements are essential to ensure that IP ownership is clearly allocated and consolidated across all contributors.

Copyright Key Considerations in Digital and Virtual Assets

Game developers retain copyright over original digital assets and their protection depends on clear licensing arrangements, the use of Digital Rights Management (DRM) measures to prevent unauthorised use and careful consideration of virtual economy assets, whose legal treatment may vary according to their functionality and the applicable jurisdiction.

Trademark Laws for Virtual Goods and Services

Trademark protection covers brand identifiers such as names, logos and other distinctive signs used in games and related services. In Portugal, this may also apply to virtual goods, requiring developers to secure appropriate licences for virtual reproductions of real-world brands and increasingly to seek trademark registration specifically for use in virtual and metaverse contexts in order to safeguard their digital brand presence.

Implications of User-Generated Content

User-generated content such as mods, skins and custom levels raises IP challenges relating to the definition of ownership, the risk of third-party IP infringement and the monetisation of player-created content. To mitigate these risks, developers must rely on clear terms of service and licensing frameworks that allocate rights, regulate use and commercialisation, and enable effective control over infringing or unauthorised content within the game ecosystem.

10. Social Media

10.1 Laws and Regulations for Social Media

Legal and Regulatory Framework

Although Portugal has no specific legal framework for social media, various key legal regimes impact these activities.

On the one hand, social media is subject to legislation on intermediary services, consumer protection, gambling and contractual clauses, specifically:

- the Digital Services Act;
- e-commerce law, Decree-Law no. 7/2004;
- consumer rights in digital transactions, Decree-Law no. 84/2021;
- distance and off-premises contracts law, Decree-Law no. 24/2014;
- law on individual restrictive trade practices, Decree-Law no. 166/2013;
- advertising code, Decree-Law no. 330/90;
- consumer protection law, Law no. 24/96;
- gambling law, Decree-Law no. 422/89; and
- standard contractual clauses regime, Decree-Law no. 446/85.

On the other hand, data protection, privacy and cybersecurity legislation are also key to social media activities, notably:

- GDPR;
- Portuguese GDPR implementation law, Law no. 58/2019;
- Portuguese cybersecurity law, Decree-Law no. 125/2025; and
- Cybercrime Law.

Finally, legislation on intellectual property and artificial intelligence may also play an important part when regulating social media activities, including:

- copyright and neighbouring rights code, Decree-Law no. 63/85;
- database protection law, Decree-Law no. 122/2000;
- computer program protection law, Decree-Law no. 252/94; and
- AI Act.

Considering the increasing impact of social media consumption, particularly the widespread use of influencer marketing, self-regulation has been active in producing best practices frameworks, such as:

- Guia 3 I's,

- Influenciar os Influenciadores que são Influenciados – provides best practices regarding influencer marketing and native advertising, by *Auto-Regulação Publicitária*.
- Marketing de Influência - gives information on rules and best practices for influencer marketing in commercial communication in the digital environment, provided by the General Directorate for Consumers.
- Code of Conduct of the Portuguese Association of Direct and Digital Marketing, by the Portuguese Association of Direct and Digital Marketing.

Key Legal Challenges

There is an increasing awareness regarding the protection of minors, namely in relation to data protection and privacy, age verification, content moderation, monetisation of user data, targeted advertising and profiling, and the potential mental health consequences regarding the use of AI algorithms of an addictive nature within social media software.

Control of disinformation and hate speech are still major concerns for social media platforms, especially in the context of content directed at minors, as well as during political campaigns and electoral periods. Enforcement of the DSA regarding online protection of minors, alongside risk assessment and mitigation of illegal content, is an ongoing challenge.

Following the European Parliament's Report of 26 November 2025 advising EU Member States to limit social media use for minors under 16, these topics are expected to be under national discussion in the near future.

10.2 Regulatory and Compliance Issues

Supervision of the different legal and regulatory aspects of social media activities in Portugal is conducted by:

- the Directorate-General for Consumers (DGC);
- the Food and Economic Safety Authority (ASAE);
- the Gaming Regulation and Inspection Service (SRIJ);
- the Media Regulatory Authority (ERC);
- the Portuguese Data Protection Authority (CNPD);
- the Portuguese Electronic Communications Authority (ANACOM); and
- the National Cybersecurity Centre (CNCS).

These authorities are empowered to:

- conduct inspections and audits to assess legal and regulatory compliance; and
- determine sanctions, including fines, as well as corrective measures, such as content removal, for breach of the applicable laws.

Consumer associations also ensure close monitoring and enforcement of legislation applicable to social media activities, while being empowered to initiate class actions.

The Directorate-General for Consumers (DGC), the Food and Economic Safety Authority (ASAE) and the Gaming Regulation and Inspection Service (SRIJ) have been especially active in investigating and enforcing against illegal activities in the social media ecosystem, with a clear focus on influencer marketing and compliance with consumer protection legislation.

11. Data Privacy and Cybersecurity

11.1 Data Privacy in Telecommunications

Regulatory Framework

In Portugal, electronic communication service providers operate under a layered framework that couples the GDPR and its national implementing law (Law no. 58/2019) with sector-specific rules arising from Law no. 41/2004 (transposing the ePrivacy Directive) and the ECL. General data-protection principles interact continuously with telecommunications-specific confidentiality and security duties.

The Portuguese Data Protection Authority (CNPD) supervises compliance with the GDPR, while the National Regulatory Authority (ANACOM) oversees telecom-specific obligations and related regulation, ensuring that network integrity and user-protection requirements dovetail with data-protection standards. Providers must uphold the confidentiality of communications, respect strict limits on processing traffic and location data, obtain prior consent for non-essential

cookies and marketing, notify breaches and meet contractual and disclosure duties to end-users.

Operational Challenges

Operational challenges mirror EU norms but are amplified by the vast volumes of network data typical for telecom providers. Valid consent must be secured for some uses (such as analytics and marketing) beyond core service provision, while data-minimisation imperatives routinely collide with billing, fraud-prevention, and quality-of-service needs.

The effective execution of user rights (access, erasure, and portability) must function seamlessly across operational and business support systems, as well as multi-vendor ecosystems. This pressure has only increased as CNPD's recent outreach and enforcement on unsolicited marketing and cookies signal heightened scrutiny of consent and transparency controls.

Cross-Border Transfers

Cross-border transfers must comply with the GDPR by deploying approved mechanisms (notably the modernised standard contractual clauses) and performing transfer-impact assessments. CNPD directs controllers to the European Commission's updated clauses while monitoring third-country risks. Telecom operators typically combine rigorous vendor due diligence with strong encryption and data-at-rest segregation – particularly where cloud hosting or global network operation centres are involved – to keep residual risks within tolerable bounds.

Lawful Interception and Data Retention

Lawful access obligations are framed both by criminal procedure and Cybercrime Law and by the evolving data-retention regime, which was recalibrated through the approval of Law no. 18/2024 to narrow retention and reinforce judicial oversight. In practice, providers must engineer interception and retention capabilities that remain strictly bounded by necessity and proportionality and are activated only pursuant to judicially authorised access.

Third-Party Vendors and Cloud Service Providers

Because third-party processors and cloud vendors are integral to Portuguese telecom networks – from virtualisation layers to CRM and billing – GDPR-compliant frameworks must be underpinned by detailed data processing agreements with sub-processor flow-downs and audit rights. The sector-specific security and integrity regime (which will be revised following the approval of Decree-Law no. 125/2025, transposing the NIS2 Directive) imposes incident-reporting duties, security-policy obligations, permanent contact points and disclosures where incidents significantly impact services. These contractual and regulatory levers shape architectural choices for 5G, edge deployments and data-residency patterns.

Impact of Evolving Regulations

With NIS2 now transposed, the governance, risk-management, supply-chain and incident-reporting expectations for "essential" and "important" entities (categories that typically capture major telecom operators) have expanded significantly. This requires commensurate updates to contracting frameworks and to board-level oversight and accountability.

11.2 Cybersecurity in Digital Media and Streaming Services

Primary Challenges

For Portuguese digital media and streaming services, the privacy and security baselines are set by the legislation outlined above. Primary challenges include consent orchestration across devices, reconciling minimisation with personalisation, and providing granular user controls and rights workflows at scale. CNPD's public focus on unsolicited communications and cookies signals enforcement risk for ad-tech implementations and may imply changes in the near future.

Privacy-by-Design and Security-by-Design

Privacy-by-design and security-by-design are operationalised via data protection impact assessment for new tracking or profiling features, default-off settings for non-essential cookies, strict purpose scoping, data mapping of events and identifiers, and pseudonymisation. Security controls should reflect GDPR requirements and sector security duties, including:

- encryption in transit and at rest;
- role-based access;
- secure coding and dependency management;
- vulnerability management; and

- tested incident-response runbooks with the applicable notification triggers.

Where platforms rely on content delivery networks (CDNs), cloud, or analytics, controllers must implement processor screening, SCCs/transfer assessments where relevant, and maintain audit and deletion routines.

Third-Party Data Sharing

Third-party sharing with advertisers, analytics and CDN partners creates role-allocation complexity (controller/processor/joint controller). Contracts must embed GDPR terms, sub-processor flow-downs and clear bans on own-use of data, with technical mitigations such as server-side tagging, IP truncation, event-level hashing and access minimisation. Transparency layers should comply with Law no. 41/2004 and provide easy opt-outs and preference centres.

Impact of Emerging Cybersecurity Regulations

Portugal has recently updated its framework via the approval of Decree-Law no. 125/2025. Many streaming platforms fall within "digital providers" or other covered categories, triggering governance, risk management, supply chain and incident-reporting duties overseen by the National Cybersecurity Centre (CNCS).

Where operators also qualify as providers of electronic communications services or networks (thus being considered essential entities), ANACOM's integrity/security regime adds notification and policy duties, which are also covered under Decree-Law no. 125/2025.

Technology agreements should therefore allocate NIS2-aligned controls, notification timelines, cooperation, audit and liability, and reference CNCS guidance, which will be approved in 2026. Aligning these with GDPR breach-notification and processor obligations helps avoid duplicative workflows and inconsistent timelines.

Trends and Developments

Contributed by:
Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida
Vieira de Almeida & Associados

Vieira de Almeida & Associados (VdA) is a leading international law firm with more than 50 years of history, recognised for its impressive track record and innovative approach in corporate legal services. The excellence of its highly specialised legal services, covering several industries and practice areas, enables VdA to overcome the increasingly complex challenges faced by its clients. Recognition of the excellence of its work is shared by the entire team, as well as by clients and stakeholders, and is acknowledged by leading professional associations, legal publications, and academic entities. VdA has been consistently recognised for its outstanding and innovative services, having received the most prestigious international accolades and awards of the legal industry. Through the VdA Legal Partners network, clients have access to eight jurisdictions (Angola, Brazil, Cabo Verde, Mozambique, Portugal, Sao Tome & Principe, Spain, and Timor-Leste), with a broad sectoral coverage in all Portuguese-speaking countries.

Authors

Magda Cocco is group executive partner at VdA and head of digital frontiers, with a recognised practice spanning the full digital regulatory ecosystem across Europe and Africa. Known for her innovative, value-driven advice on complex transactions, policy strategy, and legislation drafting, she was appointed independent expert drafting the EU AI Office's General-Purpose AI Code of Practice. Magda serves on the Portuguese Quantum Institute board, and is a member of the WEF AI Governance Alliance, IBA Electronic Communications Committee Officer, EU D4D Hub Advisory Group, and APDC's Strategic Advisory Board. Ranked Band 1 in Chambers Europe (TMT – Portugal) for over 16 years and Band 2 in Chambers Global (TMT – Africa-wide).

Tiago Bessa is head of the ICT practice and partner in the IP transactions team at VdA, working on matters across electronic and postal communications, media, entertainment, gaming and technologies. He has deep expertise in digital, copyright, internet and consumer law, contributing to innovative technological projects in Europe and Africa. Tiago has supported governments and regulatory entities in regulatory policy development and legislative drafting, advising organisations such as the International Telecommunications Union, the World Bank and the European Investment Bank. He also represents VdA in WhatNext.Law, an R&D centre dedicated to leveraging the impactful opportunities created by the ongoing digital transition worldwide.

Inês Antas de Barros is a partner in the information, communication & technology practice at VdA, with extensive experience in innovative technological projects in the electronic communications industry across Europe and Africa. She has worked in multidisciplinary ICT teams, assisting governments and regulatory entities in defining regulatory policies and legislative drafting, while also advising international organisations such as the International Telecommunications Union and the World Bank. Her practice focuses on privacy and information security, contributing to projects across multiple sectors involving data protection, cybersecurity challenges and related legal issues. She provides strategic guidance to clients around the world navigating today's complex digital regulatory landscapes.

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida,
Vieira de Almeida & Associados

João de Araújo Ferraz is a senior associate in the ICT practice at VdA, where he provides specialist advice to companies and public entities from different sectors on various legal issues in the digital economy, namely cybersecurity and emerging technologies. He regularly works on various operations, with particular focus on electronic communications issues. He also provides advice on public consultations, contract negotiations, drafting legal memoranda, litigation and drafting proposals for various legal and regulatory instruments. He has worked with several Portuguese-speaking African countries, particularly Angola, Cabo Verde, and São Tomé and Príncipe, as well as Timor-Leste.

Rui Gordete Almeida is a senior associate in the ICT practice at VdA. He has been actively involved in a wide range of projects in the ICT field, notably telecommunications, consumer protection, data protection, artificial intelligence, digital identity, cybersecurity and emerging technologies. His work includes responses to public consultations, contract negotiations, preparation of legal memoranda and opinions, litigation, drafting of proposals for various pieces of legislation or regulations. He has worked with several Portuguese-speaking African countries as well as Timor-Leste. Rui is a member of the International Bar Association (IBA).

Vieira de Almeida & Associados

28 Rua Dom Luís I
1200-151 Lisboa
Portugal

Tel: (+351) 213113400
Fax: (+351) 213548939
Email: vieiradealmeida@vda.pt
Web: www.vda.pt

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida,
Vieira de Almeida & Associados

The Road Towards the AI Act Implementation and the Signs of Simplification on the Horizon

The European Union has positioned itself at the forefront of artificial intelligence (AI) regulation with the adoption of the Regulation (EU) no. 2024/1689 (the AI Act). This will be the world's first comprehensive legal framework governing the development, placing on the market and use of AI systems. The AI Act's risk-based approach, based on the EU's product safety framework, has been widely praised. However, following the publication of the Draghi Report, the policy agenda in Europe and Portugal has shifted towards the need for simplification and the promotion of competitiveness.

The AI Act entered into force on 1 August 2024, with its obligations becoming applicable in phases. The first set of obligations, relating to AI literacy and prohibited AI practices, became applicable on 2 February 2025. These obligations apply broadly to all organisations deploying AI systems. Following this, the obligations applicable to providers of general-purpose AI models (GPAI) will also become enforceable. During this timeframe, both the European Commission and the AI Office have been promoting the development and adoption of a set of new guidelines on the definition of AI systems, prohibited practices, the scope of obligations for general-purpose AI models (GPAI), as well as the first code of practice for GPAI. The first drafts of the AI sandboxes implementing act and the code of practice on marking and labelling AI-generated content are already available, although the guidelines for high-risk AI systems are still pending.

The next major milestone of the AI Act is 2 August 2026, when obligations for AI systems under Annex III will become applicable. However, this deadline may be subject to significant change. In November 2025 the European Commission proposed the Digital Omnibus package, including a Digital Omnibus for AI regulation. The Commission's proposals reflect a recognition that, as the AI Act moves into its implementation phase, adjustments may be necessary to ensure that the regulatory framework remains proportionate and conducive to innovation, whilst maintaining a high level of protection for fundamental rights. As such, it aims to simplify many of the AI Act's obligations and procedures, including delaying the applicability of most obligations. The specific deadline of August 2026 will be postponed until 2 December 2027 under the condition that the European Council and Parliament agree on the text of this proposal.

The applicability of these provisions will raise many challenges across the AI value chain, considering the lack of guidelines, common specifications and EU harmonised standards available. European standardisation bodies are still developing the necessary technical standards. Enforcement is also not yet in place, as the majority of Member States are yet to officially designate the competent authorities and adopt implementing legislation for the AI Act.

AI Agents: Emerging Challenges for the EU Legal Framework

One of the defining technological trends of 2025, and likely to continue in to 2026, is the rapid proliferation of AI agents – autonomous or semi-autonomous AI systems capable of perceiving their environment, making decisions and taking actions with limited or no direct human intervention in pursuit of defined objectives. AI agents are increasingly being deployed across a wide range of sectors, from customer service and e-commerce to financial services, healthcare and legal practice, often operating in complex, multi-agent environments where they interact with other AI systems, digital platforms and human users.

The emergence of AI agents poses significant challenges for the EU legal framework, and in particular for the AI Act. The AI Act's regulatory architecture is built around relatively clear distinctions between providers, deployers and users of AI systems, and presupposes a degree of human oversight and control that may be difficult to maintain in the context of autonomous agents capable of independent decision-making and action. Questions arise as to the allocation of responsibility and liability along the AI value chain and become particularly complex where AI agents act as intermediaries, enter into transactions or produce outputs that have legal or practical consequences for third parties.

These challenges extend beyond the AI Act and intersect with a range of other areas of EU law, including product liability, data protection, contract and consumer law and the regulation of online platforms. The

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida, **Vieira de Almeida & Associados**

question of whether, and how, existing legal concepts, such as legal personality, agency, contractual capacity and fault-based liability can or should apply to AI agents is the subject of growing academic and policy debate.

Portugal and the AI Act: National Developments and Institutional Framework

As of early 2026, no specific national legislation implementing or complementing the AI Act has been adopted.

In this regard, *Autoridade Nacional de Comunicações* (ANACOM), the Portuguese national communications authority, has been designated as the competent authority by the government for the AI Act, pending formal legal enactment. This designation is noteworthy given that ANACOM's traditional remit has centred on electronic communications, postal services and related areas. It reflects the Portuguese government's decision to leverage existing regulatory expertise and institutional capacity in the digital domain for AI governance purposes.

More broadly, the Portuguese government has adopted a national digital strategy (Resolution of the Council of Ministers 214/2025) and a national AI Agenda (Resolution of the Council of Ministers 2/2026) that encompass, among other objectives, the promotion of AI adoption across the economy and public administration, the development of digital skills and AI literacy, as well as the creation of conditions for responsible and trustworthy AI. However, further regulatory and institutional developments will be necessary in the future to ensure that the national framework is fully equipped to support the implementation of the AI Act. These include the establishment of AI regulatory sandboxes, co-ordination among national authorities with sectoral competences, and the provision of guidance to market participants on their obligations under the new legal framework.

Finally, AMALIA, the Portuguese large language model (LLM), developed by a consortium of public universities with the backing of the government, should become widely available, with the objective of its integration in systems in both the public and private sector.

A Reinforced EU Cybersecurity Framework

The European Union's cybersecurity regulatory landscape continues to evolve at pace, with 2026 marking a shift in emphasis from the adoption of new legislative instruments to the simplification and consolidation of existing frameworks.

This trend is clearly reflected in the Omnibus IV package and the Cybersecurity package, presented by the European Commission (May 2025 and January 2026, respectively). The former aims to reduce regulatory burden for small and medium-sized enterprises as well as small mid-cap enterprises, seeking to rationalise reporting obligations, streamline compliance processes and avoid unnecessary duplication across overlapping EU instruments. Of particular relevance to the cybersecurity domain, the Omnibus IV package also includes measures to amend Directive (EU) 2022/2557 (CER Directive), which was transposed to Portugal through Decree-Law no. 22/2025, with a view to ensuring that the resilience obligations imposed on critical entities remain proportionate and coherent with the wider regulatory architecture.

Alongside the simplification agenda, the European Commission has recently presented a new Cybersecurity Package, comprising two key legislative proposals. The first is a proposed regulation – commonly referred to as the Cybersecurity Act 2 – which aims to build upon and update the original Regulation (EU) no. 2019/881 (Cybersecurity Act), reinforcing the mandate and capabilities of ENISA (the European Union Agency for Cybersecurity) and further developing the EU cybersecurity certification framework. The second element of the package is a proposed directive to amend the Directive (EU) 2022/2555 (NIS2 Directive), transposed to Portuguese law through Decree-Law no. 125/2025, which established measures for a high common level of cybersecurity across the EU. The proposed amendments to NIS2 Directive are intended to address implementation challenges identified during the transposition period, enhance cross-border co-ordination and incident response mechanisms, and further clarify obligations for entities falling within the scope of the NIS2 Directive. These proposals will need to follow the ordinary EU legislative procedure, and are unlikely to be finished before the end of the year.

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida, **Vieira de Almeida & Associados**

Portugal and the aftermath of the late transposition of NIS2 and DORA

2025 was a significant year for the national cybersecurity legal framework, with the transposition of three major EU instruments into Portuguese law.

First, Decree-Law 125/2025, transposed the NIS2 Directive into Portuguese law. This Decree-Law establishes a comprehensive national regime for the cybersecurity of networks and information systems, setting out obligations for essential and important entities. The law introduces requirements relating to risk management measures, incident reporting, supply chain security, governance and accountability, and grants the competent national authorities – notably the *Centro Nacional de Cibersegurança* (CNCS) – enhanced supervisory and enforcement powers. The transposition of NIS2 Directive represents a substantial upgrade of Portugal's cybersecurity framework and places new obligations on a significantly broader set of entities compared to the previous regime under the original NIS Directive.

Second, Decree-Law no. 73/2025 was adopted to implement the Regulation (EU) no. 2022/2554 (DORA), which establishes uniform requirements for the security of network and information systems of financial entities, and to transpose Directive (EU) 2022/2556, which amended several EU financial services directives to align them with DORA's requirements. This Decree-Law ensures that the Portuguese legal framework for financial services is aligned with the EU's digital operational resilience standards, imposing obligations on financial entities in areas such as ICT risk management, incident reporting, digital operational resilience testing and the management of ICT third-party risk. Together, these legislative developments signal a marked strengthening of Portugal's regulatory approach to cybersecurity and digital resilience, reflecting the broader EU trend of building a more comprehensive and harmonised framework for the security of critical digital infrastructure and services.

Finally, Decree-Law no. 22/2025, transposed the CER Directive, as mentioned above.

The Possible Future Reform of the Data Protection Law

Regulation (EU) no. 2016/679 (GDPR) remains the cornerstone of EU data protection law and continues to shape the regulatory environment for the processing of personal data across all sectors of the economy, including in the development of AI. The GDPR, once referred to as the "law of everything" due to its all-encompassing scope of application and broad definition of personal data, is set to be reformed during 2026.

As part of its simplification agenda, the European Commission put forward two proposals concerning the GDPR in 2025.

The first was the previously mentioned Omnibus IV package, which includes an exemption from the obligation to maintain records of processing activities under Article 30 of the GDPR for small mid-cap enterprises. This proposal appears to enjoy broad support among stakeholders and authorities, which may facilitate its development and possible approval. Nevertheless, its adoption before the end of 2026 appears unlikely.

The second, the Digital Omnibus proposal, introduces more far-reaching amendments to the GDPR as well as to the broader EU data acquis and will be the centre of the policy debate. The proposal aims to address a range of practical difficulties and interpretive uncertainties that have emerged since the GDPR's entry into application, and to ensure greater coherence between the GDPR and other EU legislation governing the digital economy. The proposal revokes several data directives and regulations, with their provisions to be consolidated into the Regulation (EU) no. 2023/2854 (Data Act), in order to adjust and simplify the rules regarding data sharing and facilitate the development of the European data economy whilst maintaining a high level of protection for data subjects.

The changes to the GDPR include:

- redefining personal data, with the aim of aligning the text with recent case-law, namely C-423/23 P, which limits the concept of pseudonymised data considering the position of third-party recipients;

- establishing that development and operation of AI systems and AI models may be carried out on the basis of legitimate interests under Article 6 (1), with residual processing of special categories of personal data (eg, health or biometric data) if there are strict safeguards implemented but it is nevertheless incidentally processed;
- allowing the processing of biometric data by the data subject where it is necessary for verifying its own identity; and
- changes to simplify the data transparency requirements and the data breach notifications.

The Digital Omnibus is a much more controversial legislative package among stakeholders, including the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), raising concerns over several of its measures. The negotiations between the European Parliament and the Council of the European Union will be at the centre of policy debate in matters of data protection law.

The EDPB and the national data protection authorities have designated transparency and information obligations as the focus of the 2026 Coordinated Enforcement Action. Data controllers and processors can expect actions from their Data Protection Authority (DPA) on this topic, and the Portuguese data protection regulator (CNPD) will also take enforcement action.

The Portuguese government has also committed to proposing and adopting a law implementing the Data Act, as well as revising the law implementing the Regulation (EU) no. 2022/868 (Data Governance Act).

EU Developments: The Gigabit Infrastructure Act, the Digital Networks Act and the Cloud and AI Development Act

The telecommunications sector in Europe continues to undergo a significant regulatory transformation, driven by the EU's ambition to ensure universal access to high-speed connectivity and to adapt the regulatory framework to the evolving technological and market landscape.

A key development in this regard is the entry into force of the Regulation (EU) no. 2024/1309 (Gigabit Infrastructure Act or GIA), which establishes measures to reduce the cost and accelerate the deployment of gigabit electronic communications networks. GIA requires Member States to adopt a range of national measures within specified deadlines across 2025 and early 2026, including the designation of competent bodies responsible for overseeing the application of the Regulation, the establishment of enforcement frameworks and the setting up of dispute resolution bodies. As of early 2026, Portugal has not yet adopted the necessary national measures to comply with these requirements (which would require amendments to Decree-Law 123/2009), this delay will need to be addressed promptly to avoid regulatory gaps and potential infringement proceedings. In its multi-year activity plan, ANACOM has included the amendment of this Decree-Law, and the approval of the GIA will likely accelerate the process.

Alongside the GIA, the European Commission has recently presented a proposal for a Digital Networks Act (DNA), which represents a broader and more ambitious initiative to reform the EU's telecommunications regulatory framework. The proposed DNA aims to modernise the rules governing electronic communications networks and services, with a particular focus on promoting investment in very high-capacity networks, fostering cross-border consolidation and scale in European telecoms markets, ensuring fair contribution to network costs by large traffic generators and adapting the regulatory framework to the convergence of telecoms, cloud and digital infrastructure services. As such, the proposal is centred on reforming the Directive (EU) no. 2018/1972 (European Electronic Communications Code).

Furthermore, the European Commission is preparing a proposal for a Cloud and AI Development Act, which aims to address the challenges hindering the expansion of the EU's data centre capacity, including difficulties in accessing natural resources, slow permitting processes and high capital requirements. It also aims to promote sustainable solutions and technological innovation in data centre operations. The Cloud and AI Development Act is expected to complement existing legislation, such as the Data Act, the AI Act and the DNA, as part of a broader policy effort to strengthen Europe's digital sovereignty and technological com-

petitiveness. The proposal is expected in the course of 2026 and will add a further layer to the increasingly comprehensive EU regulatory architecture for digital infrastructure and services.

EU Consumer Law: Waiting for The Digital Fairness Act

Consumer protection in the digital environment remains a key priority for the European Union. Building upon the existing body of consumer protection legislation – including, the Directive (EU) no. 2011/83/EU (Consumer Rights Directive, which has been transposed in Portugal through Decree-law 24/2014), the Directive (EU) no. 2005/29/EC (Unfair Commercial Practices Directive, transposed in Decree-Law 57/2008), the Directive (EU) no. 93/13/EEC (Unfair Contract Terms Directive, transposed in Decree-Law 446/85) and the more recent Directive (EU) no. 2019/2161 (Omnibus Directive, transposed through Decree-Law 109-G/2021 and Law 10/2023) – the European Commission has announced that it will present a proposal for a Digital Fairness Act by the end of 2026. The Digital Fairness Act is expected to address a range of emerging consumer protection challenges in the digital economy, including issues such as dark patterns, addictive design practices, the use of personalisation techniques that may undermine consumer autonomy and the transparency of algorithmic systems that influence consumer decision-making. The initiative reflects a growing recognition at an EU-wide level that existing consumer protection instruments, whilst robust, may not fully capture the specific harms and asymmetries arising from the design and operation of digital services and platforms. The proposal is expected to complement the Regulation (EU) no. 2022/2065 (DSA) and the Regulation (EU) no. 2022/1925 (DMA), forming part of a comprehensive regulatory ecosystem for the digital economy.

The Year of Transposition of Key EU Consumer Protection Directives

A notable feature of the current consumer law landscape in Portugal is the significant number of EU consumer protection directives that require transposition in 2026, alongside others whose transposition deadlines have already elapsed without the corresponding national legislation having been adopted. The Portuguese legislature is now under considerable pressure to meet these deadlines.

The Directive (EU) no. 2024/1799 (Right to Repair Directive), which introduces obligations aimed at promoting the repair of goods as an alternative to replacement, thereby contributing to sustainability objectives and strengthening consumer rights in relation to the durability and reparability of products, must be transposed by 31 July 2026. In Portugal, it will also impact the legal warranty extensions following repairs of defective products under Decree-Law 84/2021, from six-month extensions (for a maximum of four, ie, two years in total) to at least one (or more) year-long extension(s).

The Directive empowering consumers for the green transition (Directive (EU) no. 2024/825), which amends the Directive (EU) no. 2005/29/EC (Unfair Commercial Practices Directive) and the Consumer Rights Directive to better protect consumers against misleading environmental claims and premature obsolescence practices, must be transposed by 27 September 2026, thereby requiring changes to Decree-Law 24/2014 and Decree-Law 57/2008.

The new Directive (EU) no. 2024/2853 (Product Liability Directive), which modernises the EU's product liability framework to account for digital products, AI-enabled systems and software, establishing updated rules on the burden of proof and extending liability to cover defective products in the digital age, must be transposed by 9 December 2026. This may occur through amendments to the Decree-Law 383/89, or its revocation and replacement altogether.

In addition to the directives with upcoming transposition deadlines, a number of EU consumer protection directives have transposition deadlines that have already elapsed in 2025 without the corresponding national measures having been adopted (nor any draft law proposed):

- Directive (EU) no. 2023/2673 on financial services contracts concluded at a distance; and
- Directive (EU) no. 2023/2225, the new Consumer Credit Directive.

Contributed by: Magda Cocco, Tiago Bessa, Inês Antas de Barros, João de Araújo Ferraz and Rui Gordete Almeida, **Vieira de Almeida & Associados**

The failure to transpose these directives within the prescribed deadlines creates legal uncertainty for market participants and consumers alike, and puts Portugal at risk of infringement proceedings. Addressing both the overdue and upcoming transposition obligations will be a legislative priority in the months ahead, and is essential to ensuring that the Portuguese legal framework keeps up to date with the evolving EU consumer protection acquis.

Regulation of Online Services and Platforms: DSA Enforcement

The European Commission has been actively exercising its direct supervisory and enforcement powers under the DSA over very large online platforms (VLOPs) and very large online search engines (VLOSEs), which are subject to enhanced obligations relating to systemic risk assessment and mitigation. The Commission has opened formal proceedings and taken enforcement action against a number of designated platforms, reflecting its determination to ensure that the DSA's most stringent requirements are effectively applied from the outset.

Among the most prominent actions, the Commission has pursued proceedings against X (formerly Twitter) for deceptive design of its "blue checkmark", the lack of transparency of its advertising repository and the failure to provide access to public data for researchers. Additionally, it has also taken action against Temu and Shein due to concerns over the sale of illegal and unsafe products, the transparency of their systems and the measures taken to protect consumers.

A further development is the potential designation of ChatGPT, the AI-powered conversational service developed by OpenAI, as a very large online search engine. Such a designation, if confirmed, would be of considerable significance, as it would bring a generative AI service within the scope of the DSA's most demanding obligations, namely the assessment and mitigation of systemic risks to fundamental rights and data access.

Portugal: Implementation of the Digital Services Act

The DSA has been directly applicable across the European Union since 17 February 2024, establishing a comprehensive framework for the regulation of intermediary services, including online platforms and search engines. However, as an EU Regulation, the DSA requires Member States to adopt national measures designating competent authorities, establishing enforcement mechanisms and defining the applicable sanctioning regime. In Portugal, the draft law implementing the DSA is expected to be approved and published in the course of 2026. The proposed legislation designates ANACOM as the sole competent authority and Digital Services Coordinator for the purposes of the DSA in Portugal. This designation is consistent with the broader trend of consolidating digital regulatory competences within ANACOM, as already observed in respect of the AI Act. The draft law establishes a national framework for the enforcement of the DSA, including supervisory powers, procedural rules and a sanctioning regime applicable to providers of intermediary services that fail to comply with their obligations under the Regulation. The approval of this legislation will be a significant step towards ensuring the effective application of the DSA in Portugal and providing legal certainty to market participants.

Age Verification and the Protection of Minors Online Arrive in Portugal

The growing international trend towards the adoption of age verification laws to protect minors online has also reached Portugal. The Portuguese legislature is considering a legislative proposal that would require a wide array of online services to implement measures to verify the age of their users. The scope of the proposed legislation is notably broad, encompassing social media platforms, video content sharing platforms, online gambling services and, more generally, any online service susceptible to being accessed or used by a minor. Under the proposed framework, most online services would be required to implement technical and organisational measures to verify the identity of their users and to ascertain whether they are minors, with a view to restricting or conditioning access to certain content or functionalities accordingly. A distinctive feature of the Portuguese proposal is its recommendation for the use of *Chave Móvel Digital* (Digital Mobile Key) as the preferred mechanism for age verification. The *Chave Móvel Digital* is a national digital authentication tool that connects with the civil identification public database, enabling secure and reliable verification of identity and age.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Luke.Wilson@Chambers.com