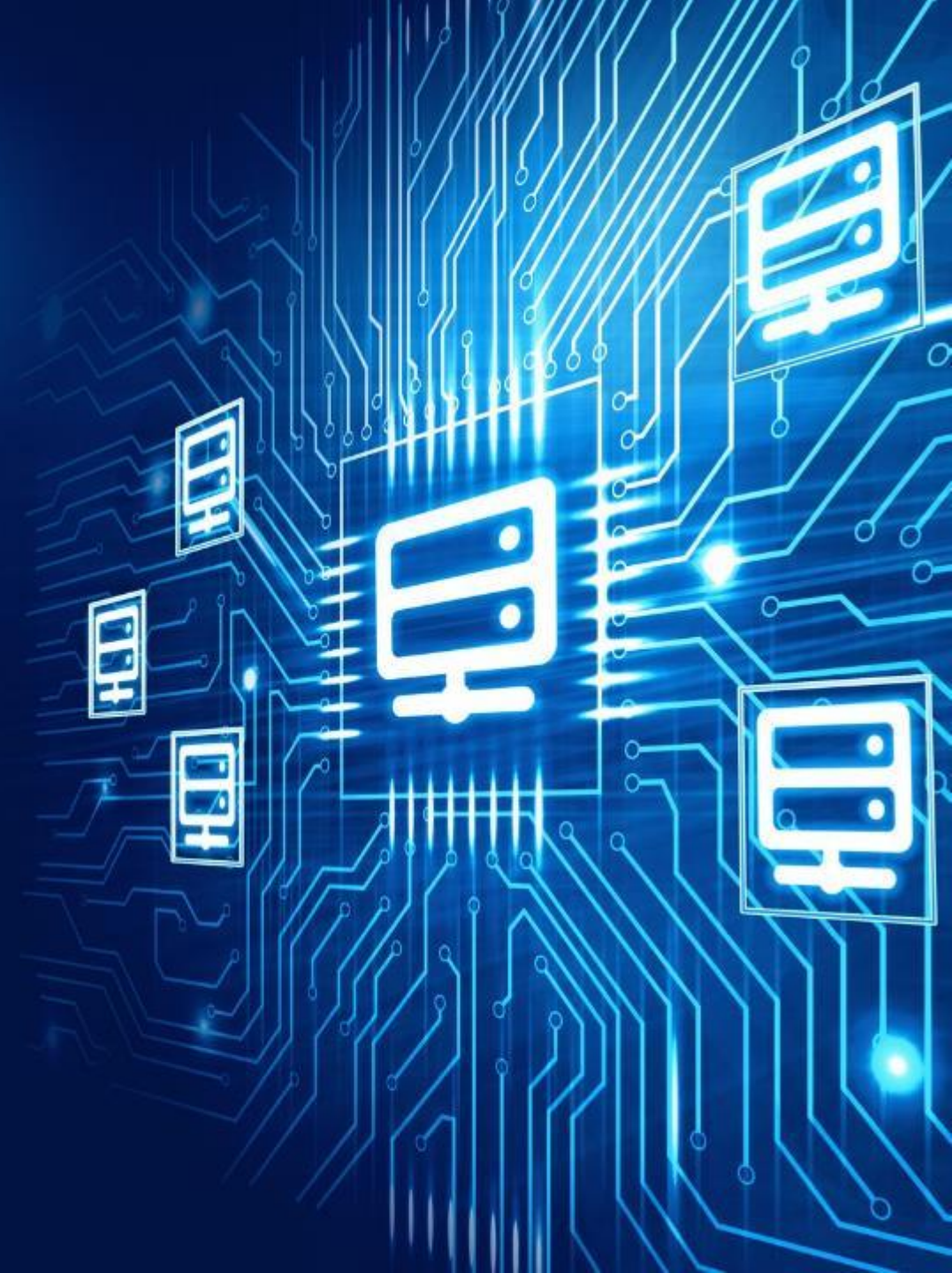







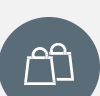

# IP, DATA AND TECHNOLOGY

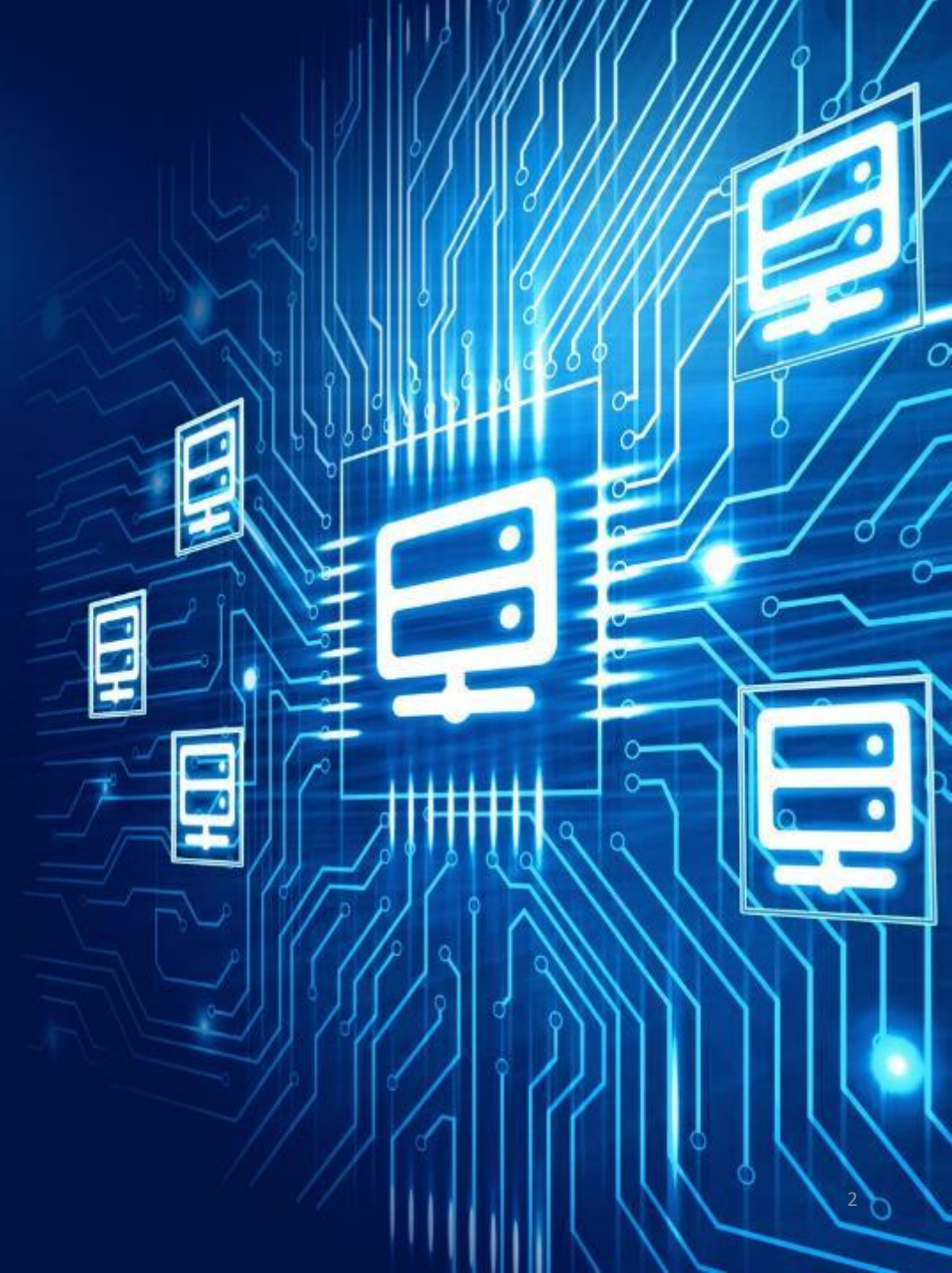
Legal matters:  
2024 retrospective and outlook for 2025

Portugal



# Contents

-  Editorial
-  1. Artificial intelligence
-  2. Intellectual property
-  3. Privacy and data protection
-  4. Telecommunications and technology
-  5. Cybersecurity
-  6. Advertising and consumer law
-  Conclusion



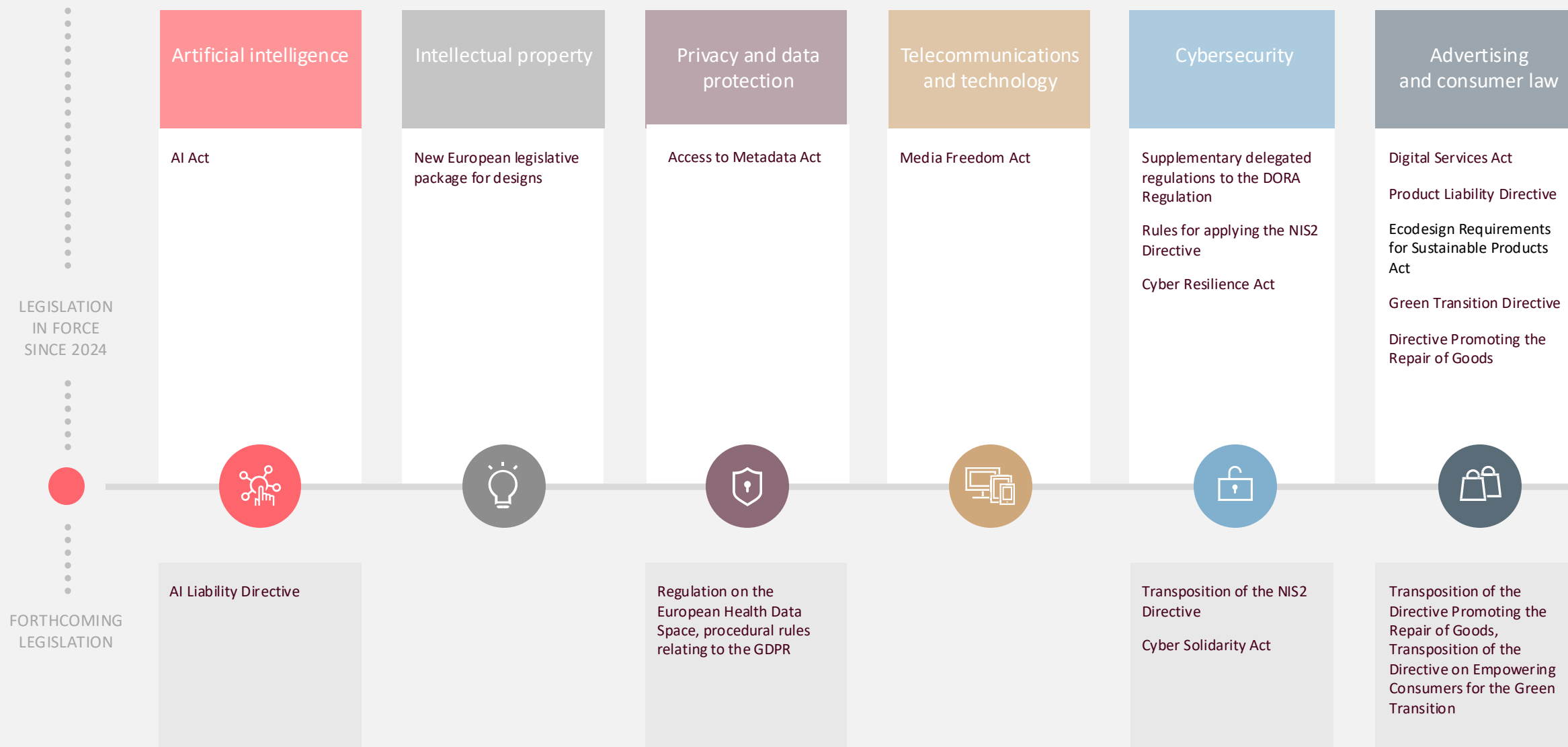
## Editorial

The year 2024 was a transformation and adaptation milestone in major business areas, especially those involving emerging technologies and complex regulations. **Artificial intelligence, cybersecurity, privacy and data protection, intellectual property, advertising and consumer law, and telecommunications** were at the center of important legislative and operational changes.

To ensure **safe, ethical and sustainable development**, the European Union (“EU”) is implementing new legal frameworks and guidelines aimed at balancing technological innovation with the protection of citizens’ fundamental rights.

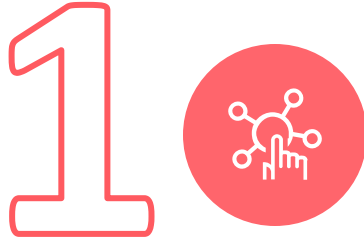
In this non-exhaustive publication, we highlight the main trends and regulatory changes that marked 2024 and anticipate some new developments that 2025 will bring and that promise to shape the future of these areas, focusing on the importance of companies adapting to the legal and technological requirements that lie ahead.

# Legal framework





# Artificial intelligence



With the entry into force of **Regulation (EU) 2024/1689**, of 13 June 2024 (“AI Act”) and the establishment of the **European Artificial Intelligence Office**, Europe has strengthened its position as a global leader in regulating AI systems. Also, the **Artificial Intelligence Treaty** and the **specific Recommendations of the European Data Protection Supervisor** (“EDPS”) and of the OECD for data protection in AI systems have become fundamental guides for public and private sector companies.

As we move ahead in 2025, the forecasts point to a year of regulatory transition and growing adoption of AI in strategic sectors. The **partial application of the AI Act** will mark the first steps in the practical implementation of the new rules and, at the same time, we are also waiting for developments concerning the AI Liability Directive (proposal published in September 2022).

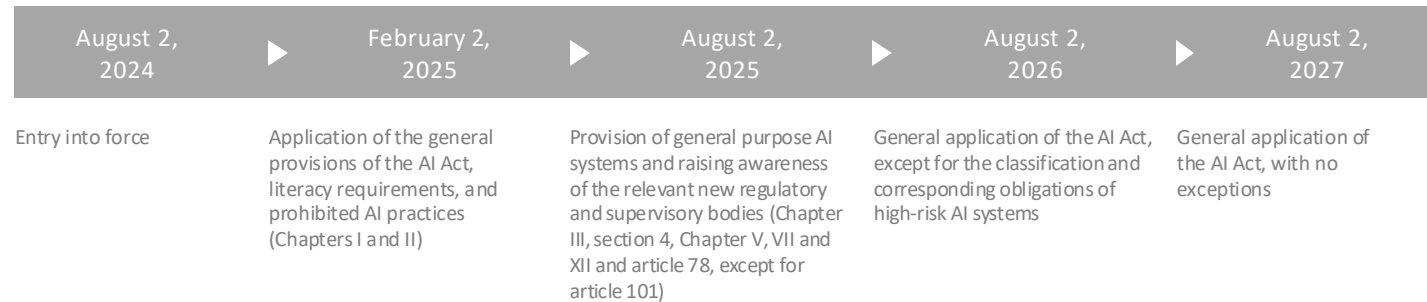
# Artificial intelligence | Legislation

## Artificial Intelligence Regulation or AI Act

The pioneering EU [AI Act](#) is crucial for businesses, as it establishes a common risk-based framework and imposes a broad set of obligations on all those involved in the AI value chain, from providers to deployers.

It also introduces substantial penalties for cases of non-compliance, as highlighted below. Consequently, organizations must identify and mitigate the risks associated with their AI models through specific measures.

See our Guide: [AI Act: Practical Guide](#)



## Non-compliance

- › €35 million or 7% of annual turnover (whichever is higher) for prohibited AI practices
- › €15 million or 3% for breaching other obligations
- › €7.5 million or 1% for providing incorrect information
- › For small and medium-sized enterprises (“SMEs”), including startups, the fines may not exceed the lower of these amounts and percentages.

## ACTION POINTS

- › Assess the impact of the AI Act
- › Map the AI systems used/developed
- › Classify the AI systems and assess the inherent risks
- › Establish an action plan with possible mitigation measures to be implemented
- › Create an internal management system to govern the use of AI in an organization
- › Raise awareness and provide training for AI system users (promoting AI literacy)

# Artificial intelligence | Guidelines

## Spanish Data Protection Agency (“AEPD”) guidelines - Generative AI systems

Provide guidelines for the EU institutions, bodies, offices and agencies (“EUIs”) to ensure compliance with data protection obligations when using generative AI systems.

Highlight the importance of principles such as **data minimization, accuracy and transparency**, and the need for data protection impact assessments (“DPIAs”) for high-risk AI systems.

Emphasize the responsibility of EUIs to develop and use AI **ethically and legally**, avoiding bias and ensuring data security. Generative AI systems present challenges for protecting personal data and transparency for individuals. EUIs must adopt a **robust data governance policy** and involve data protection officers (“DPOs”) at every phase of the AI systems’ lifecycle to ensure regulatory compliance.

See our Post: [EDPS guidelines on the use of generative AI](#)

## ACTION POINTS

- › Ensure that the data protection officer is involved in the use of AI systems processing personal data
- › Ensure compliance in developing and implementing a generative AI system with data protection obligations
- › Identify and understand the life cycle and functioning of AI systems, in particular, to ensure the identification of the origin/source of personal data, and the legal basis for processing
- › Understand the results generated by AI systems (how the input and output mechanisms work) and analyze the decision-making processes implemented in the system
- › Apply data protection principles
- › Ensure compliance with data protection procedures, in particular: (i) conducting a data protection impact assessment, where applicable, (ii) updating the register of processing activities, (iii) ensuring the review and conclusion of data processing agreements

# Artificial intelligence | Guidelines

## EDPB: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

The Irish supervisory authority asked the European Data Protection Board (“EDPB”) for an opinion on the **application of the GDPR in the development of AI models**, addressing anonymization, legitimate interest, and unlawful processing of personal data.

In its opinion, the EDPB:

- › stressed the need for case-by-case assessments for anonymization;
- › said that a three-step test should be conducted to justify legitimate interest and consideration of data subjects’ expectations;
- › presented three unlawful processing scenarios, each requiring a specific GDPR compliance assessment; and
- › emphasizes the importance of mitigation measures and data protection compliance.

## ACTION POINTS

- › Document the anonymization process in detail and keep records that prove the anonymity of the data used in AI systems
- › Conduct legitimate interest assessments (“LIAs”) and DPIAs to analyze the impact of processing on data subjects
- › Consider data subjects’ reasonable expectations when developing and implementing AI models
- › Establish procedures to deal with unlawful data processing scenarios, including data retention in AI systems, processing by another controller, and anonymization before further processing



# Artificial intelligence | Guidelines

## OECD Recommendation - Artificial intelligence

The OECD has updated its [Recommendation](#) on Artificial Intelligence to guide member countries in creating policies that promote responsible AI development. It highlights the following:

- › the importance of transparency, explainability, protection of human rights, and promotion of inclusive and sustainable AI
- › human-centered approach, ensuring robustness and security of AI systems, and high-quality data governance
- › accountability of providers and those responsible for implementing AI systems
- › international cooperation to tackle global challenges by sharing best practices and collaborating on research and development.

View our Post: [OECD updates AI principles](#)

## ACTION POINTS

- › Develop and implement transparent and explainable AI systems
- › Conduct impact assessments of ethical and fundamental rights to identify and mitigate possible AI system risks
- › Adopt practices that promote inclusion and sustainability in the use of AI
- › Ensure that AI systems are robust and secure against attacks and security breaches
- › Create clear accountability mechanisms for AI system developers and operators
- › Use high-quality data and protect them from misuse
- › Promote international cooperation by sharing good practices and collaborating on research and development

# Artificial intelligence | 2025 forecast

## 01

### Partial application of the AI Act

The year 2025 marks the beginning of the application of the [AI Act](#).

From February 2, companies must guarantee the following:

- **AI training and literacy:** The persons involved in operating and using AI systems must have a sufficient level of AI literacy.
- **Prohibited AI practices:** Discontinuation of the use of AI systems, in particular prohibited AI practices.
- Inventory system.

In August, the focus will be on **general-purpose AI models**. To this end, from August 2, providers of these models will have to ensure the following:

- **Compliance:** Compliance with various obligations relating to technical documentation, transparency and making information available, which must be recorded in internal policies and other publicly accessible documents.
- **General-purpose AI models with systemic risk:** Providers of these AI models will have to notify the Commission and comply with additional obligations, including technical assessment, model testing documentation, incident reporting to competent authorities, and ensuring appropriate cybersecurity levels.

By that date, each Member State must also have designated or established **competent regulatory and supervisory bodies**.

## 02

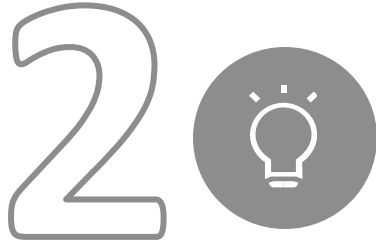
### AI Liability Directive

In 2022, the European Commission presented the proposal for the **AI Liability Directive**, aimed at adapting private law to the digital economy transition requirements and making it easier to bring claims for damage caused by AI systems and the use of AI.

This proposal for a directive still needs to be analyzed by the European Parliament and the Council of the European Union. Following the negotiations and its adoption, EU Member States will have to transpose the AI Liability Directive into their national law within around two years.

It is expected that there will be greater political and legislative pressure to approve this directive in 2025, considering its complementarity with the AI Act.

## Intellectual property



The year 2024 was marked by legislative developments in the field of intellectual property in the EU. These included the implementation of the legislative package comprising **Regulation (EU) 2024/2822** and **Directive (EU) 2024/2823**, aimed at **modernizing and simplifying the industrial design protection system**.

Moreover, the European Commission's Recommendation (EU) 2024/915 of 19 March 2024 established **measures to combat counterfeiting** and enhance the enforcement of intellectual property rights in the EU.

Court decisions on intellectual property include, in particular, the judgments of the Court of Justice of the EU, which **clarified the scope of application and protection of copyright, trademark and patent rights**, tackling issues such as the referential use of trademarks, the burden of proof for certain cases, the protection of applied art works, and the modification of computer programs, among others.

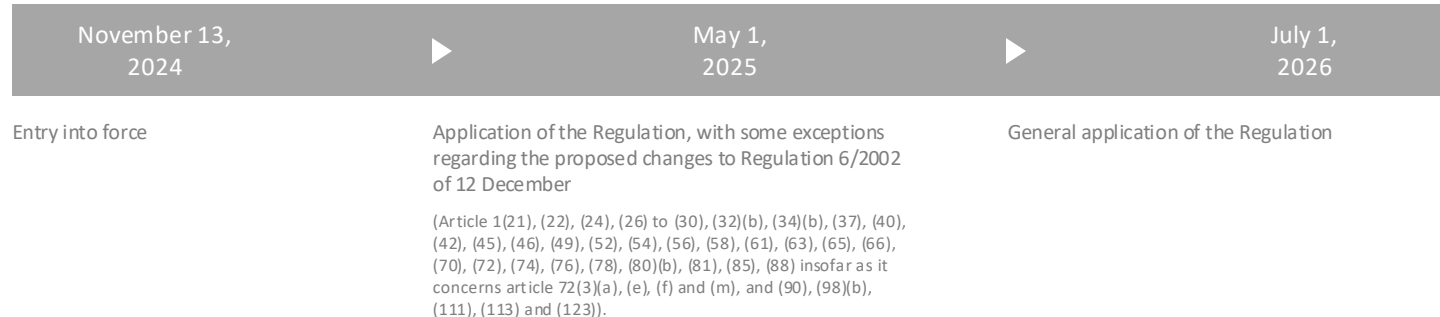
# Intellectual property | Legislation

## New European legislative package for designs

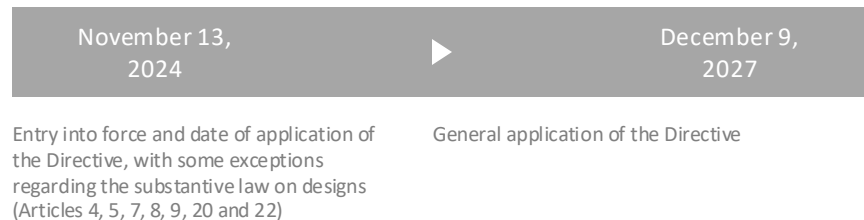
The legislative package comprising [Regulation \(EU\) 2024/2822](#) and [Directive \(EU\) 2024/2823](#) aims to modernize and simplify the **industrial design protection system in the EU**, harmonizing registration rules and introducing quicker and less bureaucratic procedures. The reform facilitates the **registration** process, **reduces costs**, combats **piracy** and **counterfeiting**, and strengthens **holders' rights**. It also extends the **protection of unregistered designs** and adapts the legislation to new technologies, such as digitization and 3D printing, ensuring effective protection in the digital environment.

View our Post: [Reform of European design legislation published](#)

### Regulation (EU) 2024/2822



### Directive (EU) 2024/2823



## ACTION POINTS

- ▶ Companies must ensure that their design registration procedures comply with the **new requirements established by Regulation (EU) 2024/2822 and Directive 2024/2823**.
- ▶ Companies must take proactive measures to protect their designs against counterfeiting. This includes **monitoring the entry of products into the EU market** and using the **customs procedures** established in Regulation (EU) 608/2013 to prevent the entry of products that infringe their design rights.
- ▶ Companies that manufacture or sell components of complex products must clearly inform consumers of the commercial origin and the identity of the manufacturer of the products used for repairs to comply with the **“repair clause”** and avoid legal issues.

# Intellectual property | Guidelines

## Commission Recommendation - Combating counterfeiting and improving respect for IP rights

European Commission [Recommendation \(EU\) 2024/915](#) of 19 March 2024 establishes measures to combat counterfeiting and enhance the enforcement of intellectual property rights in the EU by:

- › highlighting the need for a robust policy against these illegal activities;
- › promoting cooperation between rights holders, intermediary service providers, and competent authorities, and encouraging the use of new technologies and good practices;
- › promoting the modernization of voluntary instruments, the designation of single points of contact, and the use of tools such as the IPR Enforcement Portal (IPEP) and the Safety Gate early warning system;
- › establishing specific measures to prevent the misuse of transportation, logistics, payment, and social networking services;
- › promoting alternative dispute resolution;
- › promoting adaptation to new technologies such as artificial intelligence; and
- › encouraging intellectual property awareness-raising and training, especially for SMEs, through initiatives such as the SME Fund and cyber theft prevention tools, underscoring the importance of a coordinated and collaborative approach to protecting innovation and investment in the EU.

## ACTION POINTS

- › Establish partnerships and collaborate closely with rights holders, intermediary service providers, and competent authorities to combat counterfeiting and piracy, including through the use of voluntary instruments such as memoranda of understanding
- › Designate **single points of contact within the company** to deal with issues of respect for intellectual property rights
- › Adopt and **implement new technologies**, such as artificial intelligence and advanced tracking systems, to **identify and combat counterfeit goods**
- › Use tools such as the **IPR Enforcement Portal (IPEP)** and the **Safety Gate rapid alert system** to facilitate cooperation and the sharing of information about illegal activities

# Intellectual property | Case law

## Trademark infringement

The judgment of the Court of Justice of the European Union of January 11, 2024 in Case [C-361/22](#) interpreted article 6(1)(c) of Directive 2008/95/EC, which allows the **use of trademarks by third parties** to indicate the destination of products or services, provided it is in accordance with honest practices.

The dispute in the main proceedings saw Inditex and Buongiorno Myalert at odds over the use of the “ZARA” trademark in an advertising campaign, with the court concluding that this **use is only permitted when necessary to indicate the destination of a product or service offered by the third party**.

## Exhaustion of rights conferred by an EU trademark

Judgment [C-367/21](#) of the Court of Justice of the European Union of January 18, 2024 addresses the exhaustion of trademark rights in the case between Hewlett Packard and Senetic. The court decided that the burden of **proof regarding the exhaustion of trademark rights cannot fall solely on the plaintiff**, especially when the products do not clearly identify the destination market and are distributed by selective networks.

In these cases, the trademark owner must prove that the products were initially placed on the market outside the EEA to avoid compartmentalization of the national markets and ensure the free movement of products, balancing the protection of intellectual property rights with internal market freedoms.

## Copyright infringement

Case [C-159/23](#) concerns a reference for a preliminary ruling in which the CJEU was asked whether the modification of the content of variables stored in the internal memory of a computer by another program, without altering the source code or object code of the protected program, constitutes a copyright infringement under Directive 2009/24/EC. The Court of Justice of the European Union concluded that **the protection granted by the directive only applies to the literal expression of the computer program, such as the source code and object code, and not to the underlying ideas, principles or functionalities**.

Therefore, the modification of the content of variables by another program that does not allow the reproduction or subsequent realization of the protected program is not covered by the directive's protection.



# Intellectual property | Case law

## Copyright Infringement

In Case [C-227/23](#) the CJEU was asked to interpret the **applicability of copyright on works of art specifically applied in the context of the Berne Convention and Directive 2001/29/EC**. The court concluded that Member States cannot apply the Berne Convention's criterion of material reciprocity to works from third countries, and that the copyright harmonization must be determined by EU legislators.

**This decision ensures standard and high protection for all works in the EU internal market, regardless of the author's country of origin or nationality.**

## Deadline for claiming the priority right in design and patent registration

Judgment [C-382/21](#) of the Court of Justice of the EU of February 27, 2024 addressed **applying the six-month priority period of article 41 of Regulation (EC) 6/2002 to international patent applications.**

The dispute in the main proceedings involved The KaiKai Company Jaeger Wichmann GbR, which claimed priority based on an international patent application under the Patent Cooperation Treaty. The **General Court held that there was a legal loophole and applied the 12-month time limit of the Paris Convention.**

However, the Court of Justice disagreed, stating that article 41 clearly and exhaustively limits the right of priority to six months for design applications, and concluded that the General Court's decision exceeded the limits of a conforming interpretation.

# Intellectual property | 2025 forecast

## 01

### Unified Patent Court

The expected referendum in Ireland on ratifying the Unified Patent Court Agreement may take place, which would bring Irish companies under the UPC's jurisdiction.

This change would enable the centralized enforcement of European patents, simplifying litigation for patent holders.

However, it could also raise questions about jurisdictional changes and practical implications for companies operating in Ireland.

## 02

### Protection of AI-related intellectual property

With the continuing advance of artificial intelligence tools, legal debates on the protection of AI-generated works and the patentability of inventions driven by these technologies are likely to intensify. Fundamental issues such as protecting AI-generated creations under intellectual property law and whether the use of third-party intellectual property to train AI models constitutes an infringement will be at the center of the discussions. At the same time, topics such as the role of human inventors, novelty and inventive step criteria, and the potential consideration of AI as an inventor in its own right could lead to legislative changes or the development of new case law.

Both in the EU and worldwide, these changes are expected to bring greater clarity and definition to the legal framework for addressing these issues in 2025, mainly at a case law level and with the applicability of some of the provisions of the AI Regulation from February of this year.

Companies innovating in the field of AI must carefully monitor these developments, ensuring that their creations and inventions are properly protected and comply with the emerging standards.

See [Artificial intelligence section](#).



## Privacy and data protection

In 2024, there was a consolidation of concepts and methods for collecting and processing personal data, especially the guidelines issued by the EDPB on the use of **facial recognition technologies**, the AEPD on the risks of **Wi-Fi tracking**, as well as the rulings of the Court of Justice of the European Union **on the principles enshrined in the GDPR** and the **calculation of applicable fines**.

**Extraordinary fines** were **imposed** throughout Europe in 2024, most notably the €310 million fine imposed on LinkedIn by the Irish Supervisory Authority.

It should also be noted that the Portuguese Supervisory Authority (“CNPD”) investigated and subsequently suspended **biometric data processing** by the Worldcoin Foundation, whose

project aimed to create a digital proof of identity (WorldID).

The year 2025 will certainly be no different for existing data protection dynamics, specifically regarding the decisions of competent administrative and judicial authorities, the organization of business structures, and the attention given by data subjects to these issues.

# Privacy and data protection | Guidelines

## Valid consent in the context of implemented consent or payment models by large online platforms

The Supervisory Authorities of the Netherlands, Norway, and Germany have asked the EDPB for an opinion on the conditions under which **large online platforms** can validly and freely apply "**consent or pay**" models for **behavioral advertising**. The EDPB stresses the following:

- › Consent must comply with the GDPR principles, including those of necessity, proportionality, and fairness. Platforms must ensure the availability of alternatives that are free or involve less processing of personal data.
- › Consent must be freely given, without the imposition of a fee that compromises the data subjects' freedom of choice, especially when the service is essential to social or professional life.
- › Conditional consent must be avoided, and equivalent alternatives that do not require the processing of personal data must be offered.
- › Consent must be specific, informed and explicit, enabling for granularity in the stated purposes. Those responsible must avoid misleading models, assess the frequency of consent renewal, facilitate its withdrawal, and ensure that data subjects fully understand their choices and the associated consequences.

## ACTION POINTS

- › Provide clear and comprehensible information regarding the options available to data subjects in a Consent or Pay model so that they can make a truly free choice
- › Ensure that the consent collected is free, specific, informed, and explicit
- › Ensure that the fee required in the payment model is not so high as to condition the data subject's choice.

# Privacy and data protection | Guidelines

## Guidance on the risks of Wi-Fi tracking

The guidelines prepared by the AEPD, APDCAT, AVDP and CTDPA on the risks associated with Wi-Fi tracking highlight the growing concern for privacy and the protection of personal data, emphasizing the need for transparency and informed consent from data subjects whose data is collected.

- › Companies must clearly inform data subjects about the collection and offer them the choice to consent or refuse, apart from implementing robust security measures to protect the data.
- › Regulatory authorities are encouraged to bolster enforcement and ensure compliance with the GDPR. At the same time, companies must conduct DPIAs and adopt a privacy-by-design approach.

## ACTION POINTS

- › Clearly inform data subjects about the collection of data through Wi-Fi tracking
- › Obtain the data subjects' free, specific, informed, and explicit consent before collecting their data
- › Implement and review advanced security measures to protect the collected data from unauthorized access and security incidents
- › Conduct DPIAs to identify and mitigate risks associated with Wi-Fi tracking
- › Offer data subjects a clear and easy option to reject the collection of their data through Wi-Fi tracking

# Privacy and data protection | Guidelines

## Guidelines 2/2023 on the technical scope of article 5(3) of the ePrivacy Directive

The 2024 [EDPB Guidelines](#) clarify the application of article 5(3) of Directive (EU) 2002/58/EC (“**ePrivacy Directive**”) to various technical solutions, addressing ambiguities related to new tracking tools.

It aims to **protect the private sphere of users**, covering not only personal data but also any information stored on terminal equipment. The protection applies to operations that involve storing or accessing information on the terminal equipment of a subscriber or user, regardless of the origin or nature of the information.

Article 5(3) of the ePrivacy Directive is not restricted to the use of cookies, but also to similar technologies.

The guidelines identify and analyze the main elements associated with the article under analysis: “**information**”, “**terminal equipment of a subscriber or user**”, “**public communications network**”, “**gaining access**”, and “**stored information**”.

## ACTION POINTS

- Ensure that any use of tracking technologies, such as cookies, device fingerprinting, and pixels is preceded by obtaining the data subjects’ explicit and informed consent
- Adopt measures to protect data subjects’ privacy, ensuring that any access to or storage of information on terminal equipment is duly regulated and has their consent



# Privacy and data protection | Case law

## Interpretation of the concept of "personal data"

Case [C-604/22](#) examined the definition of "personal data" and the responsibility of sectoral organizations in processing consent-related data in digital advertising.

The CJEU concluded that the transparency and consent string (TC String) used by IAB Europe in the transparency and consent framework (TCF) **constitutes personal data, as it is capable of identifying individuals.**

IAB Europe was considered a "Joint Controller" of personal data since it influences the purposes and means of processing, even without having direct access to the data in question.

However, the CJEU clarified that its liability does not automatically extend to future processing performed by third parties such as website providers, unless the IAB directly influences that processing.

## Access to personal data in a criminal investigation without judicial authorization

Case [C-548/21](#) of the CJEU addressed the **legality of the seizure and access to cell phone data by police authorities without judicial authorization** in criminal investigations.

The CJEU concluded that this access constitutes a serious interference with the rights to privacy and protection of personal data **and must be limited to investigations into serious criminal offenses and subject to prior review** by a judge or independent body, except in cases of justified urgency.

The national legislation in question, which allows access without judicial authorization, is incompatible with Directive (EU) 2016/680 and the Charter of Fundamental Rights. In particular, the authorities must inform data subjects of the attempted access unless that information compromises the investigation.

Likewise, the regulations must clearly define the infringements that justify this access, respecting the principle of proportionality.

# Privacy and data protection | Supervisory authority decisions

## General data protection principles

Amazon France Logistique, responsible for Amazon's warehouses in France, was investigated by the French Supervisory Authority ("CNIL") following complaints about the **use of scanners to monitor employees' activity in real time**.

The CNIL identified several irregularities, including the breach of the principle of data minimization, excessive and illegal use of productivity indicators, lack of adequate information for temporary employees and visitors about data collection and video surveillance, and security breaches in access to video surveillance software.

The [decision](#) highlighted the need to respect the principle of data minimization, ensure transparency and security in personal data processing, and avoid excessive control of employees.

## Biometric data

The CNPD launched an investigation into the compliance of biometric data processing by the Worldcoin Foundation, which collected images of individuals' irises, eyes, and faces in exchange for the Worldcoin (WLD) cryptocurrency to create a **proof of digital identity** (World ID). The CNPD said that the Worldcoin Foundation collected biometric data from minors without a prior age check, made it impossible to exercise the right to erasure and withdrawal of consent, and also provided insufficient information to data subjects, breaching the rules and principles enshrined in the GDPR.

On March 25, 2024, the **CNPD imposed a 90-day limitation on the collection and processing of biometric data** by the Worldcoin Foundation in Portugal. Subsequently, on July 9, 2024, the CNPD recognized **BayLDA as the lead controller** for this crossborder data processing, declaring itself to be the interested Supervisory Authority.

## ACTION POINTS

- Ensure that employee monitoring practices are proportionate and justified, avoiding excessive control and respecting employees' privacy rights
- Clearly inform all temporary and permanent employees, as well as visitors, about data collection and the use of video surveillance systems
- Collect only the data that is strictly necessary for the management of operations and avoid excessive collection of information about employees

# Privacy and data protection | Supervisory authority decisions

## General data protection principles

The Dutch Supervisory Authority (“PA”) launched an investigation into Uber following more than 170 complaints about **information given to the data subjects and transfers of personal data outside the European Economic Area (EEA)**.

During this investigation, it was ascertained that Uber collected and stored sensitive information about European drivers on servers in the US without having adopted the appropriate transfer methods, including account data, cab licenses, location, photographs, payment details, identity documents and, in some cases, criminal and medical data.

Consequently, the AP imposed **a fine of €290 million**, which is its third fine since 2018 for **personal data breaches and failure to comply with information duties**.

## ACTION POINTS

- Ensure that all transfers of personal data outside the European Economic Area (EEA) are performed using appropriate transfer mechanisms, in accordance with the GDPR
- Provide clear and complete information to data subjects on how their personal data is collected, used, stored and transferred, complying with all the information obligations established by the GDPR

# Privacy and data protection | Legal content

## EU-US privacy Framework FAQ

The EDPB published [FAQs](#) on the **EU-US data privacy framework**, aimed at facilitating the transfer of personal data between the two regions while ensuring an adequate level of data protection.

This privacy framework was developed in response to concerns raised by the CJEU, which led to the invalidation of the previous EU-US Privacy Shield.

The EDPB guidelines highlight the need for **transparency**, adequate **security** measures, respect for **data subjects' rights**, and effective **appeal and supervision** mechanisms.

Additionally, the EDPB provided **recommendations for companies**, such as conducting DPIAs and creating clear privacy policies, aimed at promoting a safe and efficient transfer of data, protecting the data subjects' fundamental rights.

## ACTION POINTS

- Companies must implement international data transfer procedures that are clear and comply with EU international transfer requirements
- Enter into Data Processing Agreements on the processing of personal data with third parties to ensure that the data transfers they conduct comply with the requirements established in the GDPR

# Privacy and data protection | Legal content

## Data regulation FAQ

The European Commission published FAQs on the Data Act, a legislative proposal that aims to regulate access to and use of data in the EU, promoting innovation and competitiveness.

The Data Act establishes a legal framework for the sharing of data between companies, consumers and public authorities, ensuring the protection of data subjects' rights and data security.

The FAQs highlight

- › who can access the data and under what conditions;
- › the obligations of the parties involved;
- › the interoperability of data systems; and
- › responsibility for data management and the necessary security measures.

It also proposes mechanisms to resolve disputes related to data access and use, such as mediation and arbitration, aimed at creating a single data market in the EU.

See our Legal Update: [\*Data Act: finally approved by the European Parliament\*](#)

# Privacy and data protection | 2025 forecast

## 01

### Applicability of the Data Act

The [Data Act](#) will become applicable in 2025. It aims to ensure that data generated by connected devices and digital services can be accessed and used by different parties, promoting innovation and competitiveness in the European market.

## 02

### Regulation on the European Health Data Area

Discussions are expected to progress on the [proposal](#) for a Regulation on the European Health Data Space, the purpose of which is to create a common European area where individuals can control their electronic health data ([COM 2022/197](#)).

## 03

### Procedural rules relating to the GDPR

Progress is expected on the proposal for a regulation aimed at establishing procedural rules for handling complaints and conducting investigations under the GDPR ([COM/2023/348](#)).

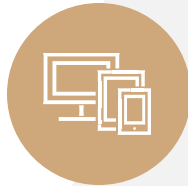
## 04

### Standard contractual clauses for data transfer

The European Commission is expected to publish standard contractual clauses for situations in which a data importer subject to the GDPR is located in a third country.



4



## Telecommunications and technology

The year 2024 was marked by technological innovation. In this section we highlight the **National Digital Strategy**, which targets people, companies, state and infrastructure. It aims to position Portugal as a leader in digital transition by 2030.

In the telecommunications area, we highlight the 2024 decision of the Portuguese Constitutional Court, declaring the unconstitutionality with general mandatory force of the rules contained in Ordinance 1473-B/2008, approved by ANACOM, charging **fees to providers of Tier 2 electronic communications networks and services**. In particular, the Court decided that these rules breached the principle of the rule of law, which must be enacted by Parliament.

# Telecommunications and technology | Legislation

## Regulation on the freedom of the media

[Regulation \(EU\) 2024/1083](#) of the European Parliament and of the Council of 11 April 2024 establishes a **common framework for media services in the EU internal market**, aimed at protecting media freedom and pluralism.

This act harmonizes national rules to ensure a level playing field for media service providers, including the **audiovisual, radio, and press sectors**.

Digitization and internationalization of the media have increased the importance of a coordinated approach to tackling challenges such as disinformation, manipulation of information, and interference from third countries.

## ACTION POINTS

- > Adopt measures to ensure that editorial decisions can be made freely within the company's editorial line
- > Engage in structured dialogue with large-scale online platform providers to resolve content moderation issues and promote access to a diversified media offer
- > Provide accurate and detailed information on the methodologies used to measure audiences, ensuring that they are transparent, impartial and verifiable, and submit them to annual independent audits to ensure their reliability and comparability

May 1,  
2024



November 8,  
2024



February 8,  
2025



May 8,  
2025



August 8,  
2025



May 8,  
2027

Entry into force

Application of the rule on the rights of media services recipients

Application of the rules on service providers' rights and duties, and the chapter on cooperation between authorities

Application of the section on regulatory cooperation and convergence

Application of the entire regulation, with the listed exceptions

Application of the rule on the right to personalize the media offer

# Telecommunications and technology | Legal content

## National DIGITAL STRATEGY

Portugal's [National Digital Strategy](#) aims to position the country as a leader in **digital transition by 2030**, promoting:

- › **digital inclusion;**
- › **sustainability;** and
- › **economic competitiveness.**

Structured around four main aspects—**people, business, state** and **infrastructure**—the strategy includes objectives such as:

- › increasing digital literacy;
- › ensuring the safe use of technology;
- › promoting gender equality in STEM fields;
- › modernizing and digitizing administrative processes;
- › expanding high-speed internet coverage; and
- › strengthening cybersecurity and developing a sovereign cloud infrastructure.

Creating a national digital agency and implementing a national artificial intelligence agenda are key actions to ensure robust digital governance and the ethical and safe adoption of new technologies.

## Media action plan

The media sector faces significant challenges affecting the sustainability of companies and the stability of employees, putting pluralism and freedom of expression at risk.

The government undertakes to develop a comprehensive [plan](#) to tackle structural and cyclical problems arising from technological changes and consumer habits, ensuring the sustainability and independence of the media in Portugal.

Council of Ministers Resolution 105/2024 created the #PortugalMediaLab mission structure to coordinate and monitor the implementation of public policies, promoting transparency, pluralism, diversity, and inclusion in the media, and bolstering public trust in the policy formulation and implementation process.

# Telecommunications and Technology | 2025 forecast

## 01

### National Digital Strategy 2030

Portugal's national digital strategy will position the country as a leader in the digital transition by 2030, promoting digital inclusion, sustainability, and competitiveness.

It is expected that there will be developments regarding the changes and improvements listed, primarily regarding bolstering the digital skills of the population and resources to respond to cybersecurity incidents occurring in the public administration.



## Cybersecurity

Three supplementary delegated regulations to the DORA Regulation were approved, introducing various technical standards related to classifying incidents and managing risks associated with information and communication technologies (“ICT”). Additionally, the European Commission

approved the Cyber Resilience Regulation, aimed at establishing harmonized cybersecurity standards for digital products in the EU. At the same time, various rules have been established for applying the NIS2 Directive.

# Cybersecurity | Legislation

## Delegated Regulation (EU) 2024/1772

Commission [Delegated Regulation \(EU\) 2024/1772](#) of 13 March 2024 supplements Regulation (EU) 2022/2554 (DORA Regulation) by establishing technical standards for the classification of ICT-related incidents and cyber threats in the financial sector. It aims to harmonize and simplify incident reporting requirements for different types of financial entities.

Entry into force

April 2,  
2024



Application of the regulations

## Delegated Regulation (EU) 2024/1773

Commission [Delegated Regulation \(EU\) 2024/1773](#) of 13 March 2024 supplements Regulation (EU) 2022/2554 (DORA Regulation) by establishing technical standards for the use of ICT services provided by third parties in critical financial sector roles.

## ACTION POINTS

- Review and update the current policies and procedures for detecting and responding to cyber threats and information security incidents
- Review the entity's current risk matrix and update it according to the threat landscape in line with the sector of activity, size, and exposure to risk
- Update the procedures for classifying and reporting security incidents
- Develop clear procedures for analysis prior to hiring third-party ICT services, or review and update existing procedures
- Develop security, technical and human capacity analysis forms for the provision of ICT services, focusing on the risk associated with the service and the ability to maintain and continue operations in the event of a security incident
- Include the purchasing, legal, IT, DPO and compliance departments in the prior analysis of the provider, as well as its human resources, when initiating the provision of services to the entity covered by the DORA Act
- Develop/update a register of the entity's ICT providers and their criticality for maintaining the business activities



# Cybersecurity | Legislation

## Delegated Regulation (EU) 2024/1774

Commission [Delegated Regulation \(EU\) 2024/1774](#) of 13 March 2024 supplements Regulation (EU) 2022/2554 and establishes technical standards for managing the risk associated with ICT technologies in the financial sector to ensure the digital operational resilience of financial entities.

Entry into force

April 2,  
2024



Application of the regulation

## ACTION POINTS

- > Review the financial entity's risk-related principles, policies, and procedures in line with the current threat landscape, current and emerging vulnerabilities, and the entity's level of exposure to potential cyber attacks
- > Review the risk classification of the entity's ICT services, products, or assets and identify the interdependencies between them for the provision of the service

# Cybersecurity | Legislation

## Rules for applying the NIS2 Directive

The Commission's [Implementing Regulation](#) of 17 October 2024 establishes rules for the application of Directive (EU) 2022/2555 ("[NIS2 Directive](#)") as regards the technical and methodological requirements of cybersecurity risk management measures established in article 21.2 of the NIS2 Directive and further specification of the cases in which a cybersecurity incident is considered to be significant under article 23.3 of the NIS2 Directive, with regard to DNS service providers, TLD name registries, cloud computing providers, data center service providers, content and distribution network providers, managed service providers, managed security service providers, online marketplace providers, online search engines, social networking services platforms, and trust service providers.

Entry into force

November 2,  
2024



Application of the regulation

## ACTION POINTS

- Review and update, based on this regulation, the entity's security plan, focusing on effective measures for identifying, preventing, and mitigating information security risks
- Implement/review the incident response procedure, in particular analyze and define the criteria for classifying a cybersecurity incident as "significant", based on the specifications of article 23.3 of the NIS2 Directive
- Implement continuous monitoring systems to assess the effectiveness of the applied cybersecurity measures, with a regular audit and update plan

# Cybersecurity | Legislation

## Cyber Resilience Regulation

[Regulation \(EU\) 2024/2847](#) establishes horizontal cybersecurity standards for digital products in the EU, applying to all hardware and software products with digital elements.

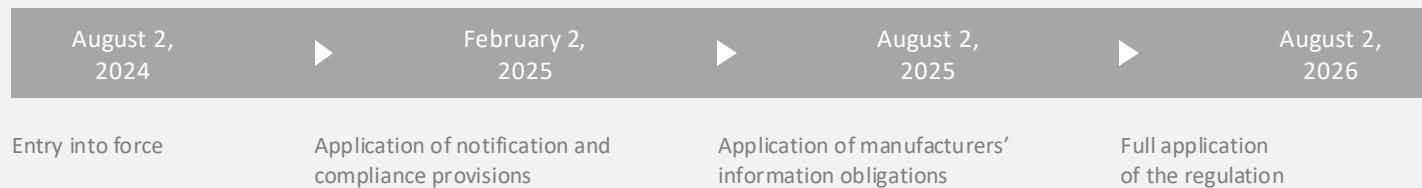
This regulation requires manufacturers, importers, and distributors to adopt safety measures from the product design phase, promoting stringent assessments to identify and mitigate risks, keeping detailed records, and ensuring CE marking.

Moreover, manufacturers must report vulnerabilities and cybersecurity incidents to the relevant authorities, such as ENISA and the CSIRT network, within specific deadlines, and provide continuous security updates.

See our Legal Update: [Cyber Resilience Act](#)

## ACTION POINTS

- Review the information security management systems and update them in line with current reference standards for product security
- For manufacturers: Ensure compliance with technical security and risk management measures for digital products
- For importers and distributors: Develop or adapt a product analysis process in line with the standards and safety measures required by the regulation
- Establish protocols and processes for reporting and sharing information on threats, risks, and vulnerabilities associated with digital products
- Review/develop policies and procedures to continuously update and monitor digital products and ensure the ability to detect, respond to, and eliminate risks when they arise in products
- Establish incident response procedures for the competent supervisory authority, with defined notification criteria, classification, and content



# Cybersecurity | Legislation

## Cyber Resilience Regulation | Non-compliance

Failure to comply with the **basic cybersecurity requirements** established in Annex I and articles 13 and 14:

- › fines of up to €15 million or, if it is a company, up to 2.5% of its total annual worldwide turnover in the previous financial year

Failure to comply with obligations imposed on **manufacturers, importers and distributors**, provisions relating to the declaration of conformity and affixing CE marking, technical documentation, conformity checks, and access to data and documentation:

- › fines of up to €10 million or, if it is a company, up to 2% of its total annual worldwide turnover in the previous financial year

Providing **incorrect or misleading information** to the notified bodies and market surveillance authorities:

- › fines of up to €5 million or, if a company, up to 1% of its total worldwide turnover in the previous financial year

# Cybersecurity | EU-US joint statement

## EU-US Joint Statement on CyberSafe Products Action Plan

The **EU-US Action Plan** on Cybersecurity and **IoT** for consumers aims to strengthen transatlantic cooperation on cybersecurity, especially in the context of the Internet-of-Things (IoT) and consumer products.

This plan recognizes the growing interconnectedness of IoT devices and the need to ensure that these devices are secure and resilient against cyber attacks. Collaboration between the EU and the US is seen as key to establishing common standards and practices that can be adopted worldwide, promoting a safer digital environment for consumers and businesses.

## ACTION POINTS

- Develop and implement specific security standards for IoT devices in collaboration with manufacturers and regulators, including requirements such as authentication, encryption, and automatic updates, ensuring the security of devices throughout their life cycle
- Develop practical guides for manufacturers, suppliers, and consumers
- Establish transatlantic cooperation mechanisms to share real-time information on threats, vulnerabilities, and cyber attacks, enabling a rapid and coordinated response to security incidents
- Invest in research and development between the EU and the US to promote advanced cybersecurity technologies applicable to IoT devices and digital infrastructure, strengthening technological competitiveness

# Cybersecurity | 2025 forecast

## 01

### Digital operational resilience of the financial sector (DORA)

Target entities must be in full compliance with this regulation from January 17, 2025.

Companies should have, among other measures, rigorous systems and processes in place to identify, protect, detect, respond to, and recover from cybersecurity incidents, and to ensure the continuity of critical services even in situations of significant disruption, while maintaining transparent communication with customers and stakeholders about their operational resilience.

The DORA Regulation is expected to promote a more secure and resilient financial environment, reducing the risks associated with technological failures and cyber attacks, both for financial entities and their ICT providers.

## 02

### Regulation on cyber solidarity

Collaboration is expected to be promoted between companies and national authorities by sharing information and resources to improve incident response. Creating a pan-European infrastructure of security operations centers ("SOCs") and implementing a cybersecurity emergency mechanism will be relevant to guarantee a coordinated and effective response to threats, ensuring the continuity of critical services and the protection of sensitive data.

## 03

### Transposition of the NIS2 Directive

The transposition of the NIS2 Directive will require target entities to implement stringent network and information security measures, including effective risk management adapted to the sector of activity and level of exposure.

Throughout 2025, the CNCS will provide tools to support risk analysis and other mandatory security measures. The national cybersecurity reference framework is also expected to be updated, enabling greater support in implementing the security measures required by NIS2. Collaboration with national authorities and transparent reporting on security incidents will be crucial for compliance with NIS2.

## Advertising and consumer law

# 6



The year 2024 will be remembered as a significant milestone in the field of advertising and consumer law, especially regarding its development and regulation in the light of the **digital single market**. In a context of technological advances and changing consumer habits, the EU has taken the lead in creating a **legal and ethical framework for the responsible use of** these practices, underscoring its commitment to safe and sustainable innovation, as well as responsible advertising.

With the implementation of the **new Product Liability Directive**, together with the **Digital Services Act**, the EU is consolidating its position as a global leader in the regulation of consumer practices, keeping up with innovation at the various stages of its development. We are also moving toward an environmentally conscious legislative framework, in line with the environmental strategy adopted by the EU in recent years, with the **review of the repairs**

**regime** and the creation of **new duties of information and prevention of unfair commercial practices** aimed at bringing more transparency to advertising claims, making it easier for the consumer to make an informed purchasing decision.

As we move into 2025, the forecasts indicate a year of regulatory transition and increasing adoption of **innovative business practices** in strategic sectors. It is essential that transposition into Portuguese law is thorough and balanced, with clear and objective rules that enable these standards to be applied effectively. The new legislation must seek to **balance product safety, sustainability, and companies' ability to adapt**, considering consumer rights and technological progress, to create a fair and dynamic market.



# Consumer Law | Legislation

## Regulations for the design of sustainable products

The [Ecodesign Regulation for Sustainable Products](#) integrates essential measures to achieve the goals set by the 2020 Circular Economy Action Plan. In general, the regulation aims to substantially increase the circularity, energy efficiency, and various other aspects of environmental sustainability of the products sold on the European market.

See our Legal Update: [EU publishes ecodesign regulation](#)

Entry into force

July 18,  
2024



Application of the  
regulation

## Ecological Transition of Products Directive

This [directive](#) amends some of the main consumer law directives, creating new unfair commercial practices and new information requirements aimed at increasing transparency in consumer communications. The measures imposed by this directive impose restrictions on the advertising of products and services, labeling, and liability claims when the consumer decides to incorporate parts or accessories from third parties.

See our Post: [Amendments to consumer directives to prevent greenwashing](#)

Entry into force

March 26,  
2024



March 27,  
2026

Limit for transposition

## ACTION POINTS

- > Adopt design practices that increase the durability, repairability, and recyclability of the products
  - > Develop systems to trace the origin of the materials and components used and provide consumers with clear and accessible information on the sustainability of the products
  - > Invest in technologies that reduce energy consumption during production and implement measures to reduce carbon emissions throughout the product's life cycle.
- 
- > Change the terms and conditions to comply with the new information requirements
  - > Review advertising communications to avoid unfair commercial practices
  - > Review the claims made in product labeling

# Consumer Law | Legislation

## Directive Promoting the Repair of Goods

[Directive \(EU\) 2024/1799](#) changes the repair obligations of manufacturers and sellers for defective goods sold to consumers.

View our Post: [EU imposes new repair obligations on manufacturers and sellers](#)

Entry into force

July 30,  
2024



July 31,  
2026

Limit for transposition

## Product Liability Directive - Adapting to technological advances

[Directive \(EU\) 2024/2853](#) of the European Parliament and of the Council of 23 October 2024 replaces Directive 85/374/EEC, updating the liability regime for defective products to include technological advances such as artificial intelligence, new circular economy business models, and global supply chains. The directive broadens the concept of “product” to include software and digital products, strengthens the liability of manufacturers and economic operators such as importers and distributors, and establishes a strict liability regime. It also emphasizes transparency and traceability in the supply chain, requiring detailed records to facilitate the identification and recall of defective products, promoting more responsible and safer business practices.

See our Post: [New directive on liability for defective products](#)

Entry into force

December 8,  
2024



December 9,  
2026

Limit for transposition

## ACTION POINTS

- > Change the terms and conditions to ensure compliance with the new rules
  - > Review the procedures for responding to complaints/exercising consumer rights
  - > Prepare the European Union information form on repairs
- 
- > Companies must implement continuous software monitoring and updating procedures to identify and correct vulnerabilities in their products
  - > Companies must document and keep detailed records documenting product compliance with EU and national safety requirements
  - > Companies must develop incident response plans detailing the procedures to be followed in the event of security breaches or product defects

# Consumer Law | Legislation

## General Product Safety Regulation

[Regulation \(EU\) 2023/988](#) of the European Parliament and of the Council on general product safety establishes essential rules on the safety of consumer products made available on the market and aims to respond to recent technological advances, the growing globalization of markets and supply chains, and the increase in distance and online sales.

Entry into force

May 30,  
2023



December 13.  
2024

Date of application

## ACTION POINTS

- Ensure that the products made available comply with the general safety requirement
- Use the Safety Gate and Safety Business Gateway platforms to provide information related to the safety of the products
- Comply with and ensure that the economic operators they enter into contract with comply with consumer information obligations

# Consumer Law | 2025 forecast

## 01

### Transposition of the Consumer Empowerment Directive for the Ecological Transition of Products

The transposition of the **Consumer Empowerment Directive for the Ecological Transition of Products** into Portuguese law, scheduled in principle for 2025, will bring significant changes to commercial practices and consumer protection.

Companies will have to adjust their **marketing and advertising strategies** to avoid misleading claims about the environmental and social characteristics of products, and unsubstantiated claims will be prohibited.

Companies will have to provide evidence for any environmental claim and clear information on the **durability, repairability, and upgrades** of the products they place on the market, as well as greater transparency regarding warranties and after-sales services (including communication of environmentally friendly delivery options).

These changes will require internal adaptations and investments in certifications, as well as awareness-raising and training for the employees involved in these processes.

## 02

### Transposition of the Directive Promoting the Repair of Goods

The transposition of the Directive **Promoting the Repair of Goods** into Portuguese law, expected in 2025, will bring significant changes to the repair obligations of manufacturers and sellers.

The Directive imposes on sellers **the duty to inform** consumers of their right to choose between **repair and replacement** and to extend the warranty period by a further 12 months if the consumer chooses repair.

Manufacturers must repair certain goods and publish indicative repair prices on their websites, apart from providing spare parts and tools at affordable prices.

The legal concept of the repairer is created to facilitate access to qualified and efficient repair services to promote sustainability and circular responsibility for the products placed on the market.

# Conclusions

## Artificial intelligence

The entry into force of the AI Act and the creation of the European Artificial Intelligence Office have strengthened Europe's position as a global leader in regulating AI systems. Companies must be aware of the new obligations and the substantial penalties for non-compliance, besides ensuring compliance with EDPS and OECD recommendations.



## Intellectual property

The modernization of the industrial design protection system and measures to combat counterfeiting stand out as important advances. Companies must adapt to the new registration rules and adopt advanced technologies to protect their IP rights.



## Privacy and data protection

The consolidation of the concepts and methods of collecting and processing personal data, along with the EDPB guidelines and court judgments, underscore the growing importance of compliance with the GDPR. Companies must ensure transparency and security in processing personal data, especially in international transfers.



## Telecommunications and technology

Portugal's national digital strategy and the Constitutional Court's decision on ANACOM's fees are important milestones. Companies must be prepared for regulatory changes and make the most of technological innovation opportunities.



## Cybersecurity

The DORA Act and the Cyber Resilience Act establish harmonized cybersecurity rules for digital products. Companies must review and update their security policies and incident response procedures to ensure operational resilience.



## Advertising and consumer law

The Product Liability Directive and the Digital Services Act reinforce the EU's position in regulating consumer practices. Companies must adopt transparent and sustainable commercial practices, ensuring product safety and consumer protection.



The forecasts for 2025 point to a regulatory transition and increasing adoption of innovative practices in strategic sectors.

It is essential that companies adapt to the new legal and technological requirements, ensuring compliance and competitiveness in the European market.

## What we offer

We advise on all areas of business law and help our clients with the most demanding matters, in any territory, providing the experience and knowledge of specialized teams.

**29**

legal specialties

**+2000**

professionals

**26**

offices in 12 countries

**29**

nationalities and 16 languages

**+300**

professors and 9 full professors

**26%**

women in management positions

**FT** INNOVATIVE LAWYERS EUROPE 2024 WINNER

Europe's most innovative firm in "Talent management", 2024

Most innovative firm in continental Europe, 2023

Maximum presence in the Iberian Peninsula  
Two offices in Portugal and thirteen in Spain

**THE LAWYER**

Highly commended in Iberia, 2024

Firm of the year in Europe and Iberia, 2022

**RepScore® 2024**

Second position in the OnStrategy reputation index, 2023-24

**Focus on Latin America**  
Offices in Chile, Colombia, Mexico, and Peru  
More than 20 years' experience in the Latin American market

Offices in Brussels, Casablanca, London, Luanda\*, New York, Beijing and Shanghai  
**Four international desks**  
**European network** with leading firms in Germany, France, and Italy  
\*In collaboration with local law firms.



- > Sectoral vision adapted to each type of business.
- > Maximum specialization combined with cutting-edge technology.
- > Long-term relationships with our clients that go beyond legal matters.



We comply with environmental, social, and good governance (ESG) criteria in providing our services and in our internal management.

[Here](#) we detail the main parameters by which we measure our ESG performance. See also our latest [Business Report](#).





## Practical guides

This year, our teams have published several practical guides on legal developments and market trends.

You can access all the guides using the following icons:

[AI Act \(EU\)](#)



[Hot Topics in Employment 2024](#)



[Guide to the Urban Development Simplex](#)



[Plan of action for competition authority inspections](#)



[2025 State Budget Law Proposal](#)







## Key contact persons



**Joana Mota Agostinho**

Partner | Data Protection | Digital Technologies and Media (TMT)

[View CV](#)

[joana.agostinho@cuatrecasas.com](mailto:joana.agostinho@cuatrecasas.com)



**Sónia Queiroz Vaz**

Partner | Intellectual, Industrial Property and Secrets | Data Protection

[View CV](#)

[sonia.queiroz.vaz@cuatrecasas.com](mailto:sonia.queiroz.vaz@cuatrecasas.com)

A informação contida nesta apresentação foi obtida de fontes gerais, é meramente expositiva, e tem de ser interpretada juntamente com as explicações que a acompanham. Esta apresentação não pretende, em nenhum caso, constituir uma assessoria jurídica.

La información contenida en esta presentación se ha obtenido de fuentes generales, es meramente expositiva, y se debe interpretar junto con las explicaciones que la acompaña. Esta presentación no pretende constituir en ningún caso un asesoramiento jurídico.

The information provided in this presentation has been obtained from general sources. It is for guidance purposes only and should be interpreted in relation to the explanations given. This presentation does not constitute legal advice under any circumstances.

