



EU AI ACT

# A Pioneering Legal Framework On Artificial Intelligence

Practical guide

July 2024

# CONTENTS

## Editorial

### **I. COMPREHENSIVE LEGAL FRAMEWORK TO REGULATE AI USE**

1. Regulation goals
2. Coordination of AI Act with other EU legal frameworks
3. Definition of AI system
4. Actors subject to AI Act | Penalties
5. Risk-based approach
6. Prohibited practices
7. High-risk AI systems
  - 7.1. High-risk AI systems requirements
  - 7.2. Main obligations for providers of high-risk AI systems
  - 7.3. Main obligations for users of high-risk AI systems
8. Transparency obligations for certain AI systems
9. General-purpose AI models

### **II. AI ACT | ROADMAP**

10. Roadmap

### **III. IMPACT ON PRACTICES**

11. Competition law: How to comply with competition law when using AI
12. Labor and employment law: Does the new AI Act affect employers?
  - 12.1 What obligations in the workplace does the AI Act impose on companies?
  - 12.2 How can HR areas prepare for the AI Act?
13. Data protection and the AI Act
14. How to comply with copyright law when using AI
  - 14.1 Input problem
  - 14.2 Text and data mining exception
  - 14.3 What specific obligations does the AI Act impose on companies regarding copyright?

Today, the amount of data generated by both humans and machines vastly exceeds humans' ability to process, interpret and make complex decisions based on this data. Artificial intelligence ("AI") is the foundation of all computer learning and the future of all complex decision-making, enhancing the speed, precision and effectiveness of human efforts.

However, **advanced AI capabilities bring significant risks**. These systems threaten to amplify social injustice, erode social and market stability, enable large-scale crime, help automate warfare, facilitate customized mass manipulation, and enhance pervasive surveillance.

Such risks can have a **direct impact in day-to-day business operations**.

For example, competitors simultaneously using the same algorithm could end up colluding on various **competition parameters**. Moreover, self-learning pricing algorithms can independently result in competitor alignment, potentially without their involvement, agreement or even knowledge. As demonstrated by European Union ("EU") caselaw, AI systems can grant or increase the capacity of dominant companies to unlawfully exclude competitors from the market.

AI also plays a **growing role in human resources** (“HR”) departments, transforming how businesses manage employee recruitment, hiring, management, and monitoring. AI solutions are already capable of helping customize employee experiences, such as benefits and training; streamline HR processes across the employment lifecycle; enhance efficiency and significantly reduce administrative load; and provide invaluable workforce insights, thereby enabling data-driven decision making and management. However, these advances may come with potential risks concerning discrimination, data protection, and other fundamental rights that companies must address.

In the **healthcare sector**, AI-driven decisions may result in inaccurate diagnoses or treatments, posing serious risks to patients. Also, the sensitive nature of healthcare data presents escalated privacy risks, even when the data is anonymized before processing.

## AI Act: A practical guide for businesses

The EU’s pioneering AI Act is crucial for businesses, as it establishes a common **risk-based framework** and imposes a **comprehensive set of obligations** on all actors in the AI value chain, from providers to deployers. It also introduces substantial **penalties** for non-compliance. Consequently, organizations must identify and mitigate the risks associated with their AI models through specific measures.

The guide provides an overview of the AI Act, clarifies its scope, and provides practical advice for navigating its complexities. In addition to outlining practical steps for compliance, it also highlights how to leverage the opportunities presented by this innovative piece of legislation.



---

I.

## COMPREHENSIVE LEGAL FRAMEWORK TO REGULATE AI USE



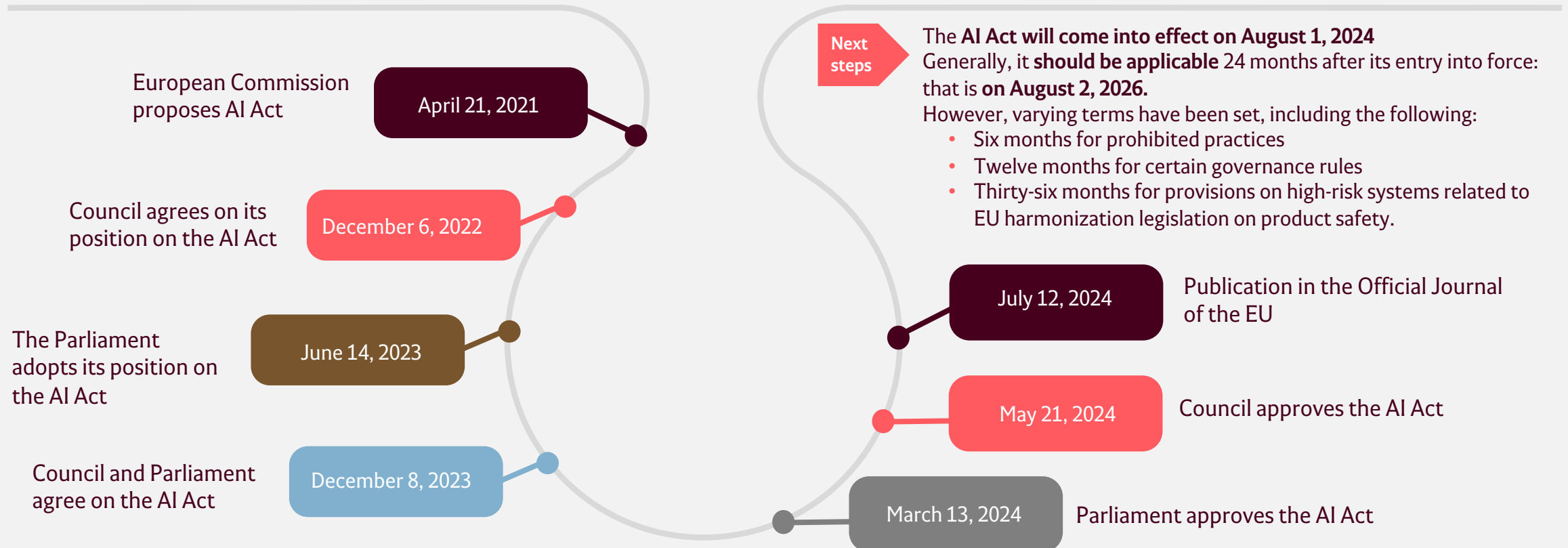
# 1. REGULATION GOALS

The AI Act ([Regulation \(EU\) 2024/1689](#)) regulates the:

- placing on the market, putting into service, and use of AI systems; and
- placing on the market of general-purpose AI models.

It aims to increase trust in AI and ensure that this technology is used in a way that respects the fundamental rights, values and safety of EU citizens.

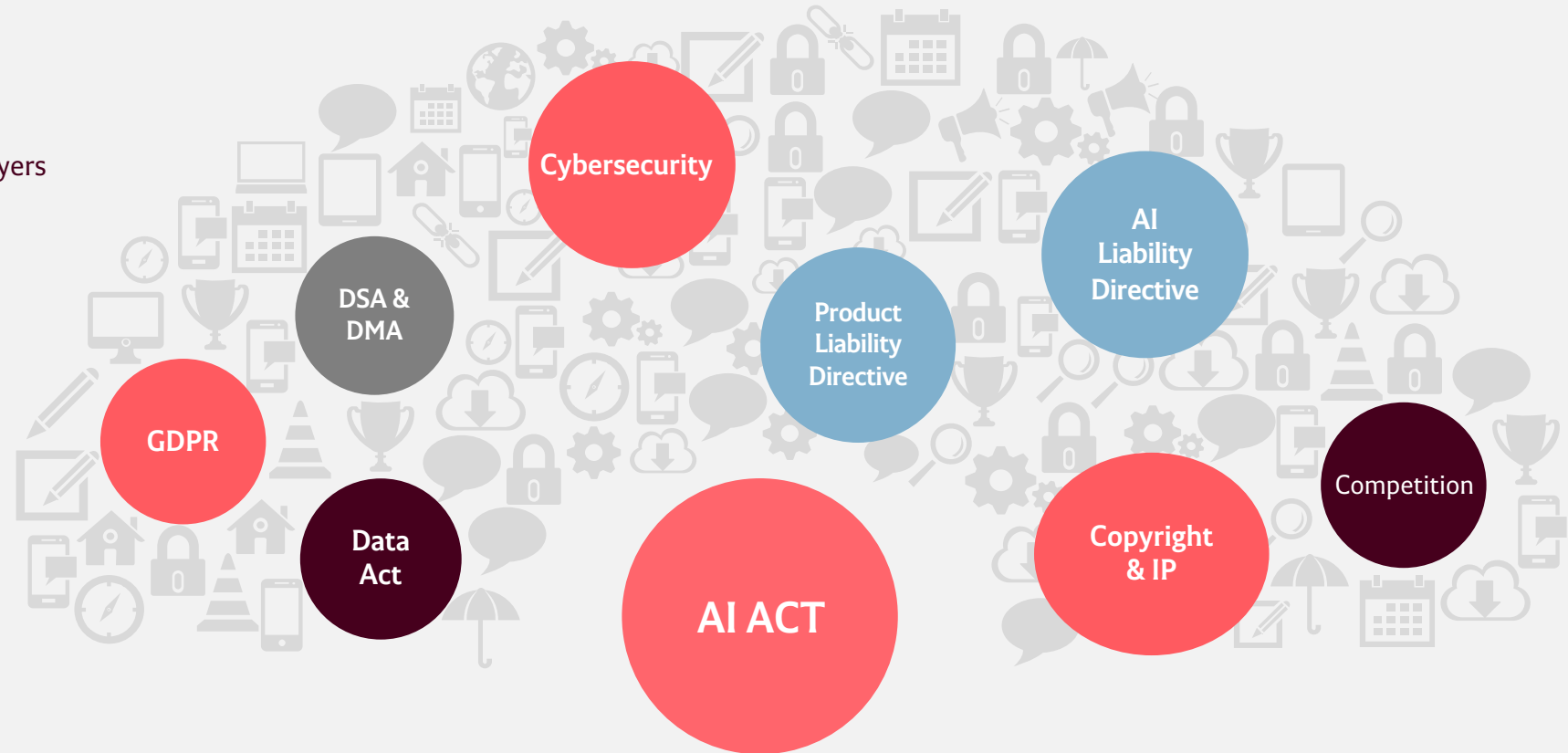
The AI Act ensures the free crossborder movement of AI-based goods and services, preventing Member States from imposing restrictions on the development, marketing and use of AI systems unless explicitly authorized by this act.



## 2. COORDINATION OF AI ACT WITH OTHER EU LEGAL FRAMEWORKS

### Non-prejudicial to existing EU law:

- Data protection (General Data Protection Regulation – “GDPR”): Does not alter GDPR obligations for AI system providers and deployers processing personal data.
- Cybersecurity
- Competition
- Consumer protection
- Fundamental rights
- Employment and employee protection
- Product safety



Ensuring compliance with the AI Act requires a thorough analysis of its interplay with the existing and proposed EU legal frameworks.

### Complementary legislative initiatives:

- Proposal for a **Directive on non-contractual civil liability for AI**, setting rules for burden of proof in damage claims.
- Proposal for a **Directive on liability for defective products**, updating the 1985 directive to cover AI system defects and data loss, allowing for the possibility of seeking compensation from AI-system providers or from any manufacturers that integrate an AI system into another product.

### 3. DEFINITION OF AI SYSTEM

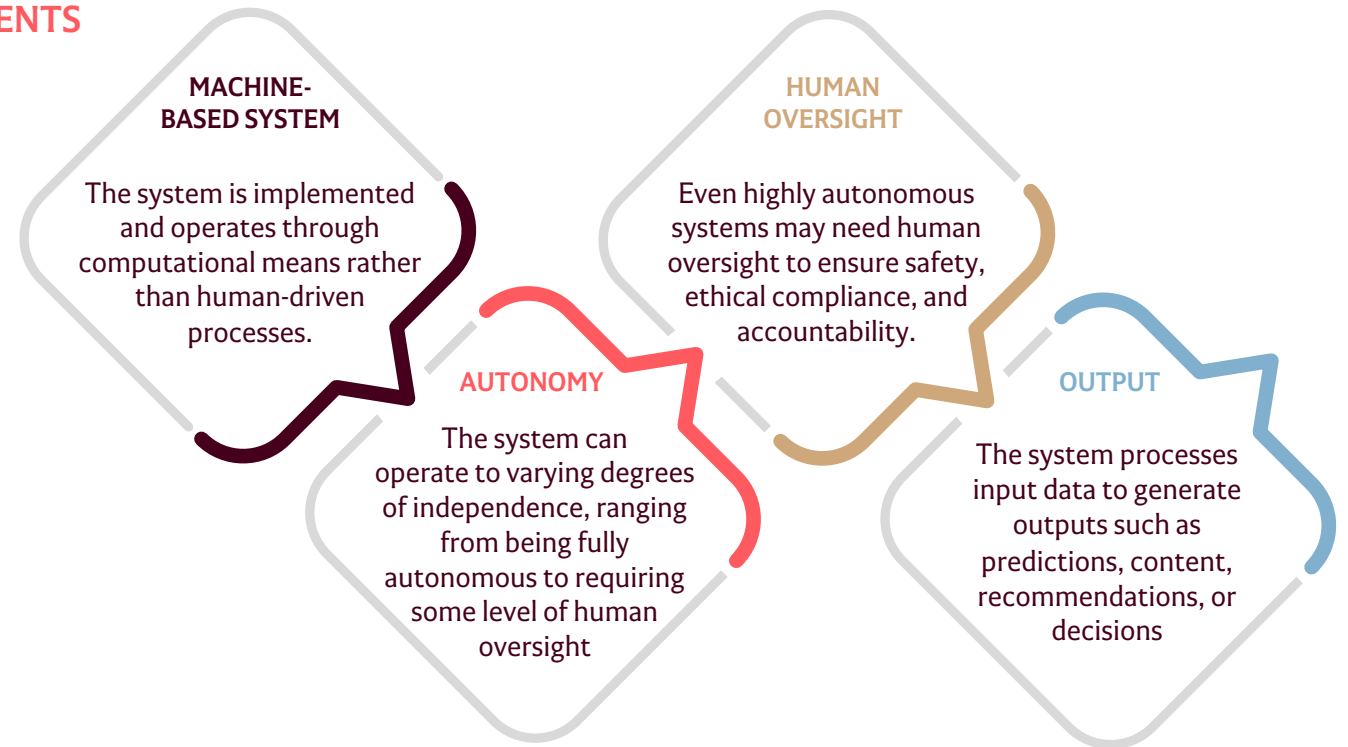
The AI Act defines “AI system” as:

“...a **machine-based system** that is designed to operate with **varying levels of autonomy** and that may exhibit **adaptiveness** after deployment, and that, for **explicit or implicit objectives**, **infers**, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”



It excludes software systems with capabilities lower than those specified above.

#### KEY ELEMENTS



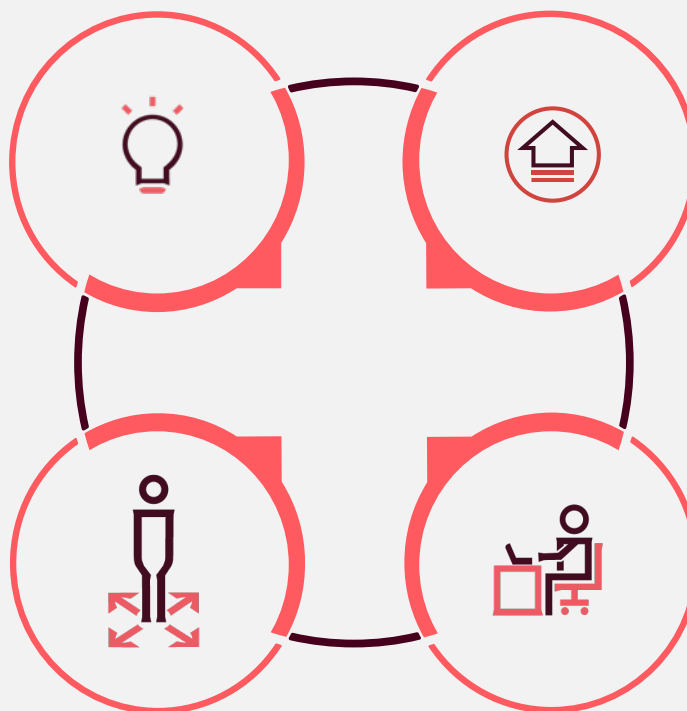


## 4. ACTORS SUBJECT TO AI ACT | PENALTIES

In addition to being the world's first AI law applicable for the EU market, the AI Act will provide a **single rulebook for providers, importers, distributors, deployers of AI systems**, and **individuals affected** by AI systems within the European AI market.

### Provider

A natural or legal person, or public authority that develops an AI system or a general-purpose AI model (or has one developed) and places it on the market or puts the AI system into service under its own name or trademark



### Distributor

A natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market

### Importer

A natural or legal person located or established in the EU that places on the market an AI system of a provider established outside the EU

### Deployer

A natural or legal person, or public authority using an AI system under its authority except where the AI system is used during a personal/non-professional activity

### MAIN EXCLUSIONS

- Systems used exclusively for military, defense or national security purposes, and those used solely for scientific research and development activity
- Any research, testing or development activity relating to AI systems or AI models before their being placed on the market or put into service
- Individuals using AI systems solely for personal/non-professional activity

### Penalties



**€35 million or 7% of global annual turnover** (whichever is higher) for violations of prohibited AI practices.

**€15 million or 3%** for violating other obligations

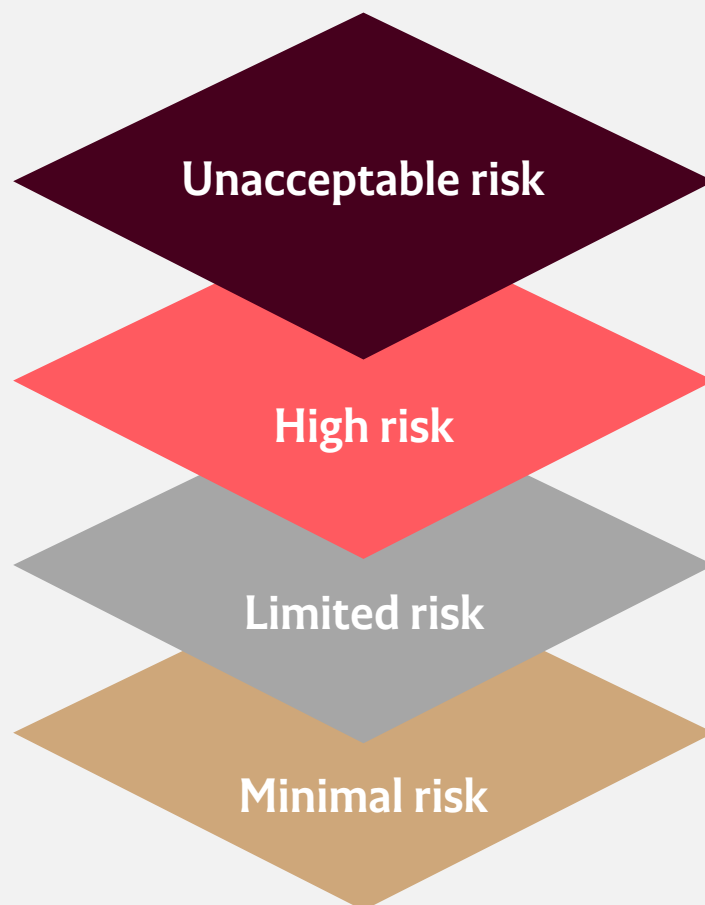
**€7.5 million or 1%** for providing incorrect information

For small and medium-sized enterprises ("SMEs"), including startups, fines will be up to the lower of the above maximum amounts and percentages.

## 5. RISK-BASED APPROACH

**The higher the risk, the stricter the obligations.**

The AI Act follows a risk-based approach whereby legal intervention is tailored to the specific risk level.



### **UNACCEPTABLE RISK**

The AI Act imposes a total ban on several AI practices that pose unacceptable risks—see [Section 6](#).

### **HIGH RISK**

The AI Act classifies as high-risk certain systems that pose a significant risk of harm to health, safety or fundamental rights. See [Section 7](#).

### **LIMITED RISK**

For certain AI systems—regardless of whether they qualify as high-risk—specific transparency requirements are imposed; for example, where there is a clear risk of manipulation (e.g., via the use of chatbots).

Users should be aware that they are interacting with a machine. See [Section 8](#).

### **MINIMAL RISK**

All other AI systems can be developed and used subject to the existing legislation without additional legal obligations.

Providers of these systems may voluntarily choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

## 6. PROHIBITED AI PRACTICES

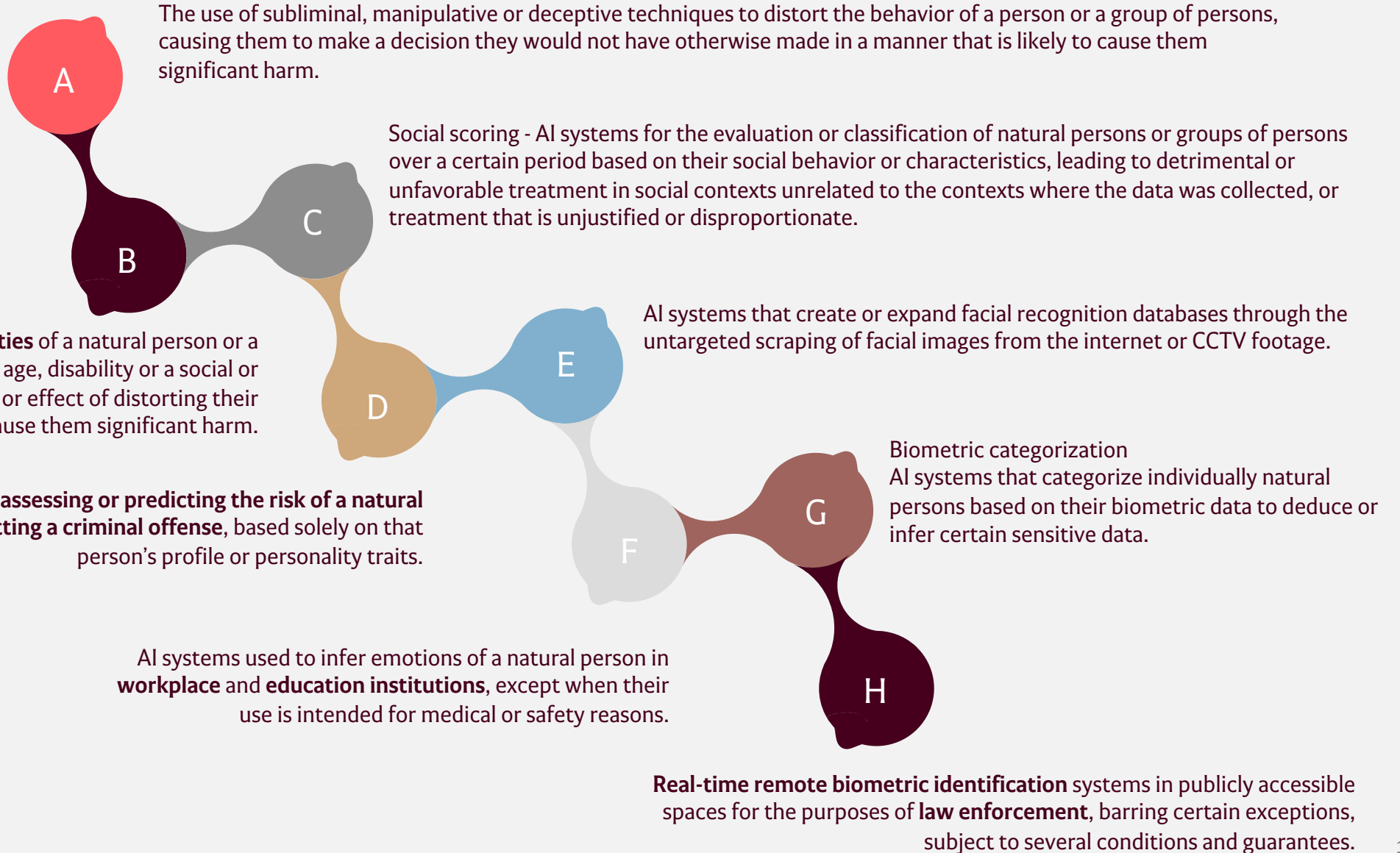


### Unacceptable risk

The **exploitation of the vulnerabilities** of a natural person or a specific group of persons due to their age, disability or a social or economic situation, with the aim or effect of distorting their behavior in a manner that is likely to cause them significant harm.

AI systems for **assessing or predicting the risk of a natural person committing a criminal offense**, based solely on that person's profile or personality traits.

AI systems used to infer emotions of a natural person in **workplace and education institutions**, except when their use is intended for medical or safety reasons.



## 7. HIGH-RISK AI SYSTEMS

The AI Act classifies as **high risk** certain systems that pose a significant **risk of harm to health, safety or fundamental rights**. It differentiates between two groups:.

1

Systems linked to EU harmonization legislation on **product safety**, as listed in [annex I](#) to the AI Act, will be classified as high-risk if the following two conditions are met:

- The AI system is a product included in this harmonization legislation or is a safety component of these products.
- Under this harmonization legislation, the product or component is required to undergo a third-party conformity assessment.

Rules for high-risk AI systems linked to EU harmonization legislation on product safety will apply **36 months** and 20 days after the AI Act is published.

2

Systems listed in [annex III](#) to the AI Act: These systems are typically considered high risk due to the field in which they are used and their specific applications

### Highlights of specific uses

**Biometrics:** This includes systems used for remote biometric verification and biometric categorization based on the inference of sensitive or protected characteristics.

**Critical infrastructure management** (e.g., water, gas, electricity, and transportation).

**Law enforcement**  
Crime prevention and investigation systems, including predictive and profiling systems.

**Education and vocational training:** Systems used to determine admission to educational and vocational training institutions, evaluate learning outcomes, assess the level of education an individual will be able to access, and monitor and detect prohibited student behavior during tests.

**Migration, asylum and border control management.**

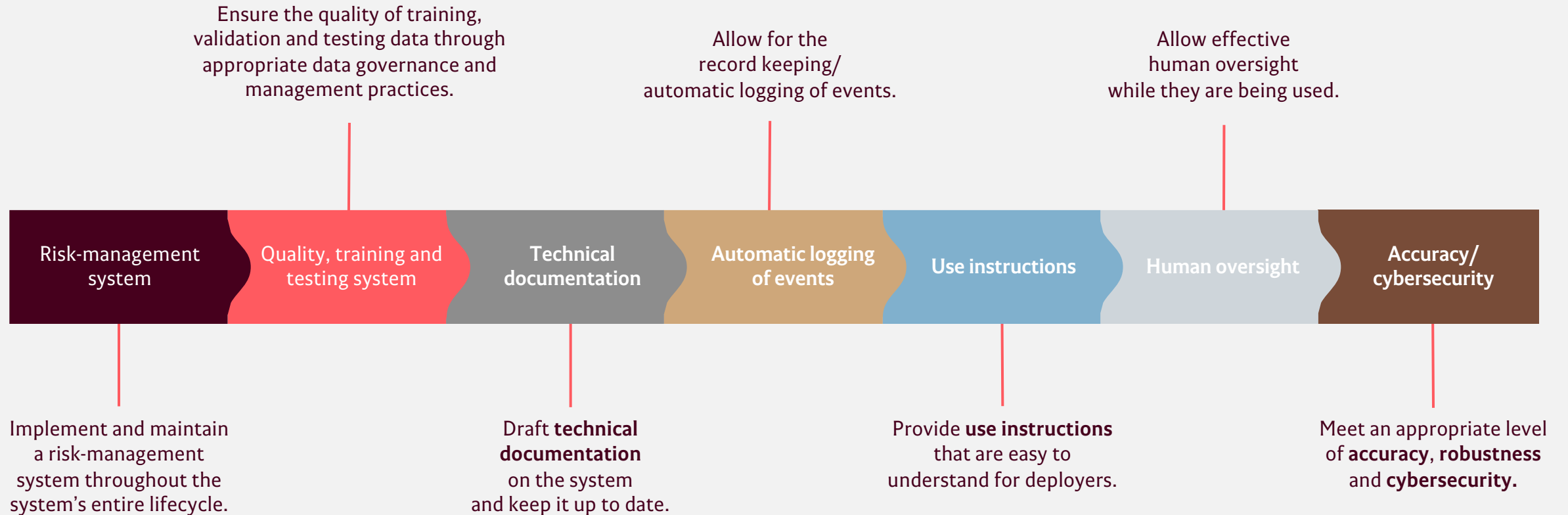
**Employment, employee management and access to self-employment.**  
See [section 12](#)

**Essential private services and essential public services and benefits** (e.g., insurance, banking, credit, and benefits).

**Administration of justice and democratic processes.**

## 7. HIGH-RISK AI SYSTEMS

### 7.1. High-risk AI system requirements





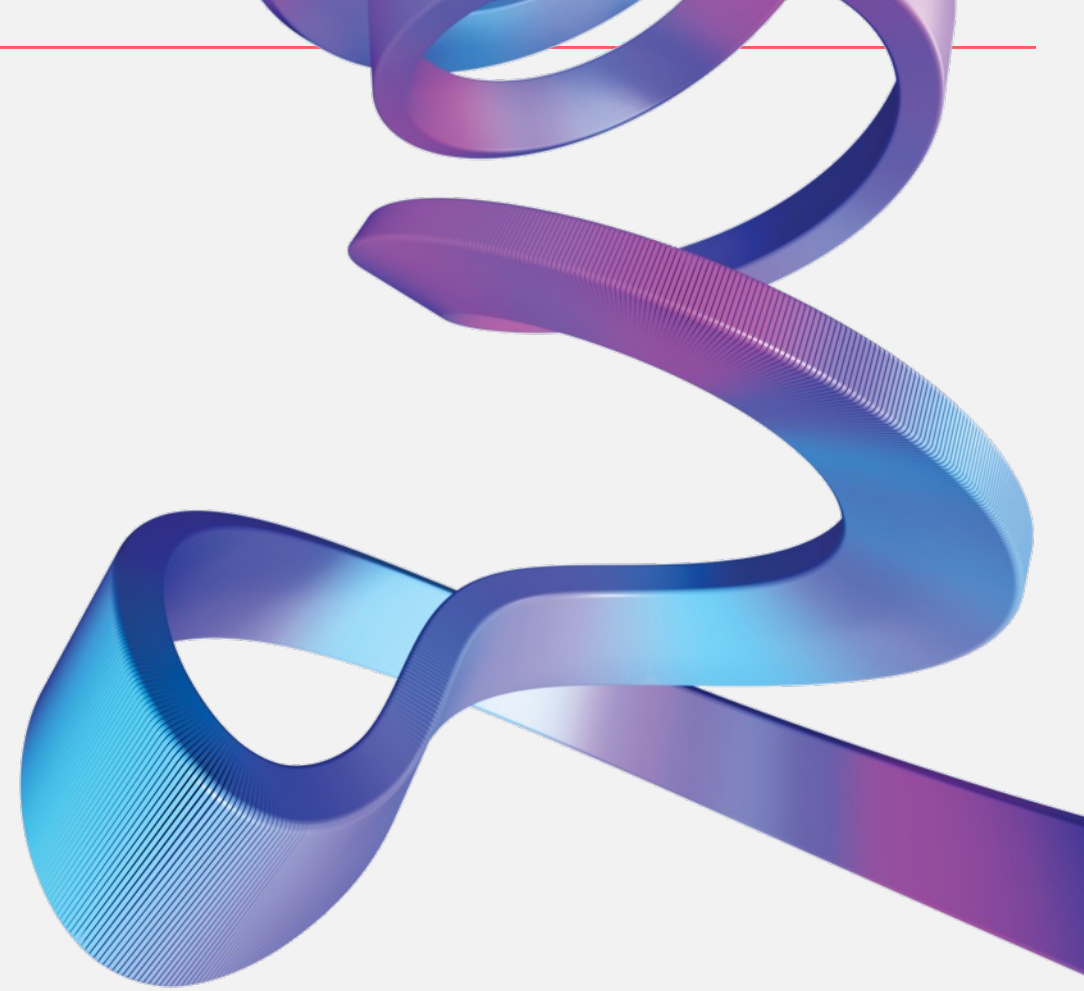
## 7. HIGH-RISK AI SYSTEMS

### 7.2. Main obligations for providers of high-risk AI systems

- Ensure their systems meet the above requirements (see [Section 7.1](#)) and demonstrate their conformity upon a competent authority's reasoned request.
- Establish a sound quality-management system.
- Keep the documentation on the system and make it available to the authorities, as well as any logs under their control.
- Ensure the system undergoes the conformity assessment, draw up an EU declaration of conformity, and affix a CE marking to the system.
- Register the system in the EU database of high-risk systems.
- Take the necessary corrective actions, including withdrawing the system or disabling it if it is not in conformity

A party will be considered a provider—meaning it must adhere to the applicable obligations—in cases where:

- it applies its name or trademark to a high-risk AI system already on the market; or
- substantially modifies it.



## 7. HIGH-RISK AI SYSTEMS

### 7.3. Main obligations for deployers of high-risk AI systems

A natural or legal person, or public authority using an AI system under its authority, except where it is used for personal/non-professional activities, must:

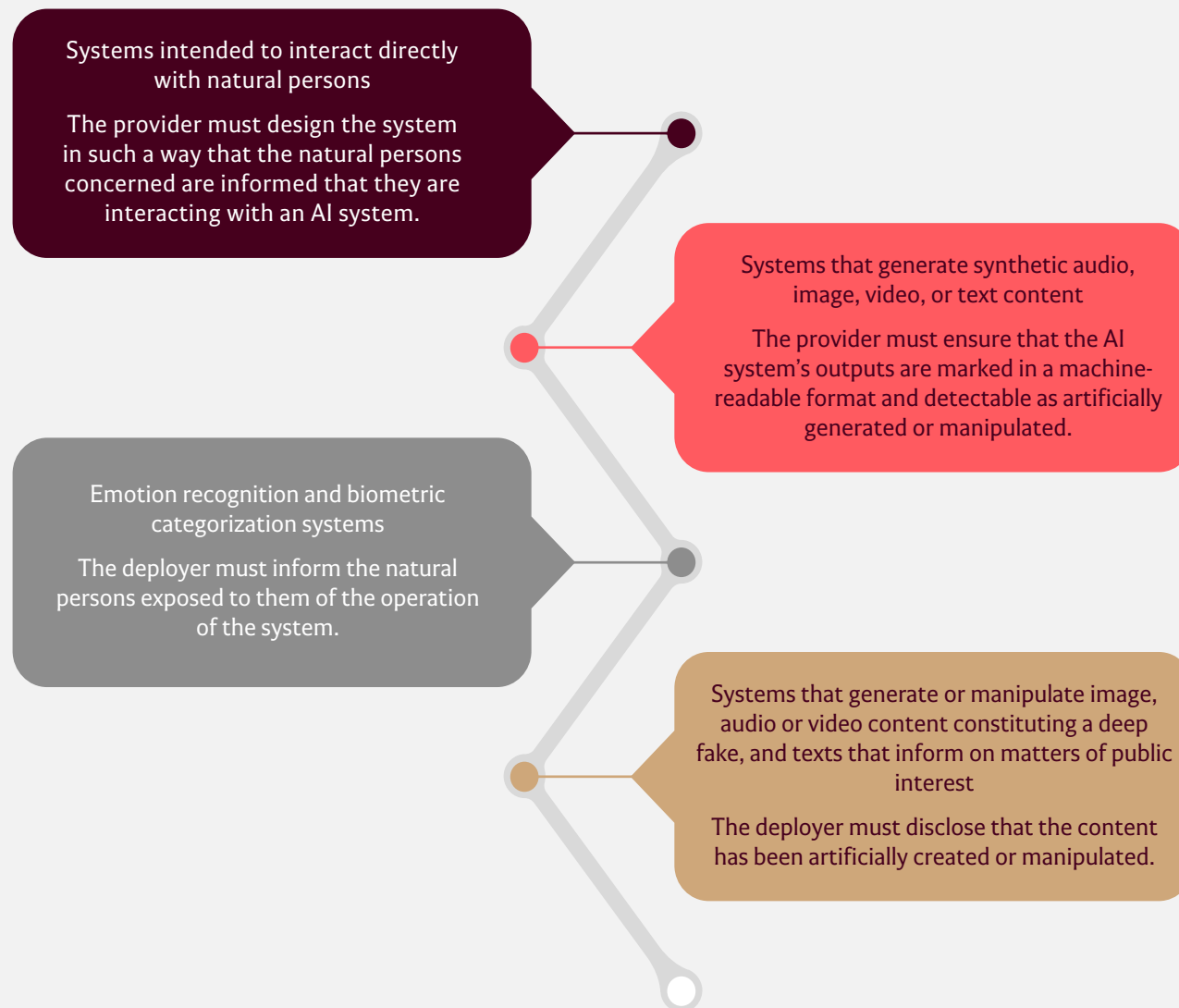
- implement appropriate technical and organizational measures to ensure system use is in line with usage instructions;
- ensure human oversight tasks are performed by adequately competent individuals;
- ensure input data is relevant and representative of the system's intended purpose, to the extent the deployer exercises control over the data;
- monitor the system's operation and report any risks and incidents to the provider, importer, distributor, and market surveillance authorities;
- retain any logs generated under their control;
- inform their employees and legal representatives before implementing a high-risk AI system in the workplace;
- inform any individuals who may be affected by the use of systems who make decisions or assist with decision-making processes;
- cooperate with the competent authorities; and
- ensure employees and other individuals assigned on their behalf to handle the operation and use of AI systems have an adequate level of AI literacy.

In certain cases, deployers must carry out a Fundamental Rights Impact Assessment.



## 8. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS

Transparency obligations for certain AI systems, regardless of whether they qualify as high-risk:



## 9. GENERAL-PURPOSE AI MODELS

General-purpose AI models are integrated into AI systems but are not systems per se.

The AI Act defines general-purpose AI models as those that:

- have a considerable degree of generality;
- can perform a wide range of tasks; and
- can be integrated into several AI systems or applications.

The providers of these models are subject to certain obligations, such as:

- documenting the training process and its evaluation results;
- informing AI system providers who plan to integrate the general-purpose AI model into their systems about their characteristics and legal requirements;
- establishing a policy to comply with EU law on copyright and related rights, particularly as regards text and data mining; and
- disclosing publicly a detailed summary of the content used for training the general-purpose AI model.

Due to their high-impact capabilities, certain general-purpose AI models are considered to pose a systemic risk. To mitigate these risks, providers are subject to more stringent requirements.



---

II.

## AI ACT | ROADMAP





## 10. AI ACT | ROADMAP

An AI system must be “**human centric,**” **accountable, transparent, explainable** and **privacy-enhanced**.

Taking an organized approach will ground the organization in a robust and enduring AI program during an AI system’s lifecycle:



**Planning** | Business problem/goal, data, scope, and governance structure



**Design** | Data quality, format, cleansing, labelling, anonymization, and system architecture



**Development** | Features, model training and testing, and evaluation



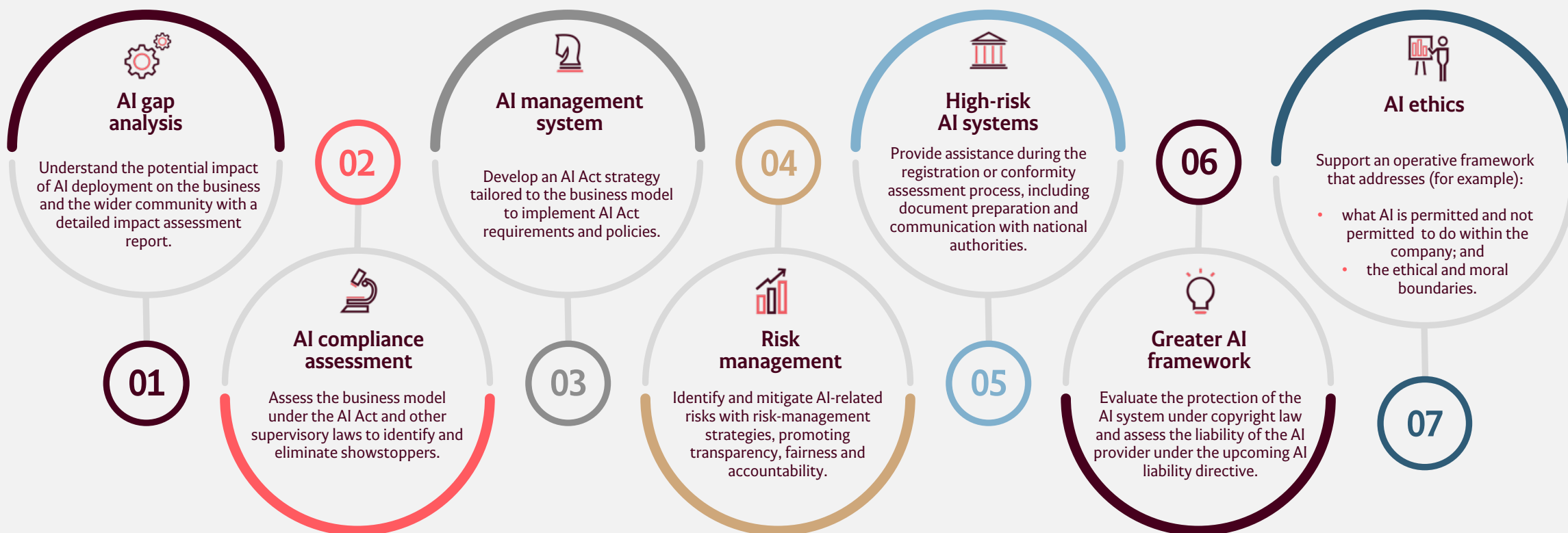
**Implementation** | Continuous monitoring and updates to the model

1. Classification of AI Systems
2. Mapping of applicable requirements
3. Risk assessment (social/ethical, security and operational, privacy, and business)
4. Action plan/identification of mitigation measures
5. Data governance

## 10. AI ACT | ROADMAP

Early compliance requires a deeper understanding of the AI Act's requirements, potential challenges, and best practices.

Companies should embrace the opportunities presented by AI systems while ensuring ethical practices and compliance with the AI Act:

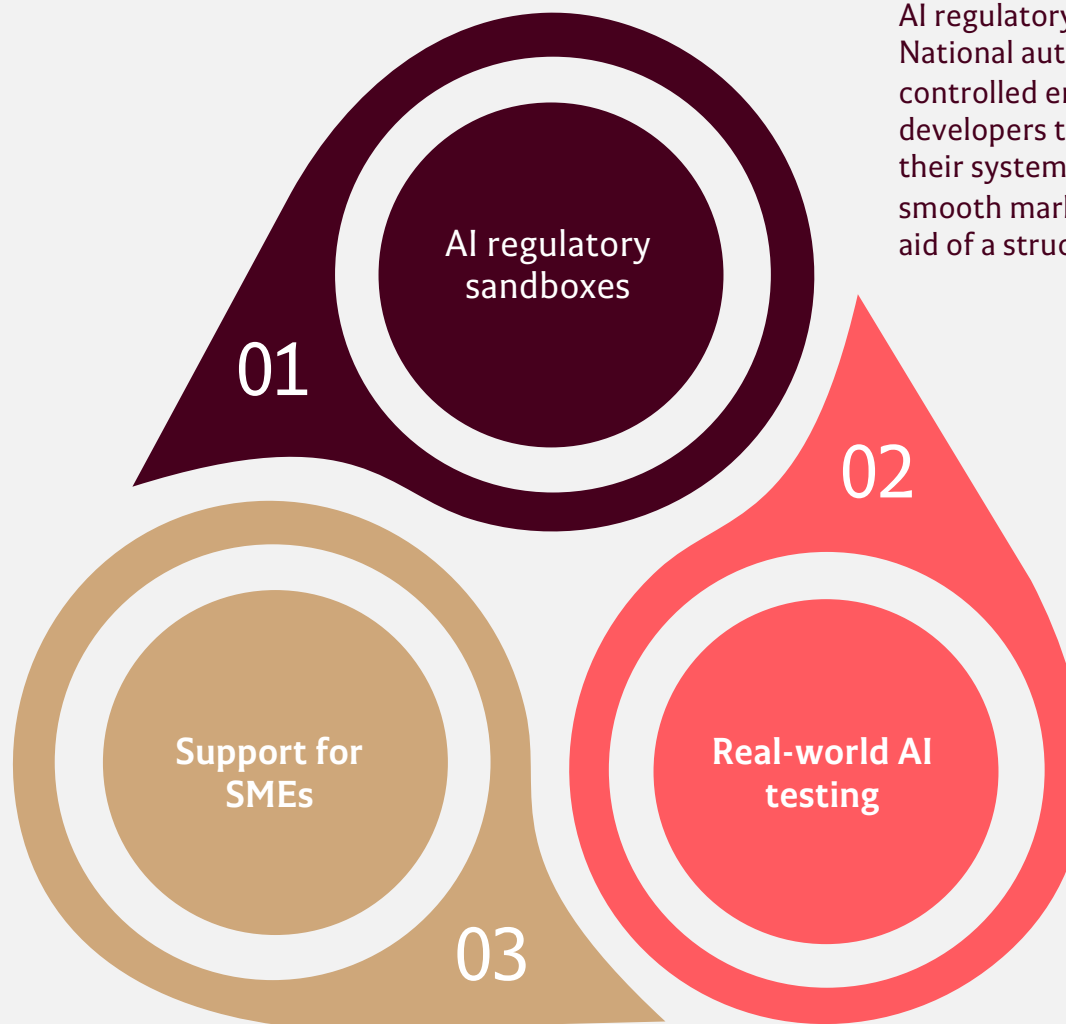


## 10. AI ACT | ROADMAP

### Opportunities

#### Support for SMEs

The AI Act provides SMEs with preferential treatment in testing environments, direct communication channels, and reduced fees, facilitating easier market entry and innovation in AI technology.



**AI regulatory sandboxes:**  
National authorities will create controlled environments for AI developers to innovate and refine their systems, facilitating a smooth market transition with the aid of a structured sandbox plan.

#### Real-world AI testing

AI systems can be tested in real-life scenarios under strict conditions set by national authorities, with a focus on safeguarding fundamental rights and ensuring data protection, especially for vulnerable groups.

### III. IMPACT ON PRACTICES

- Competition Law
- Labor and employment law
- Data protection law
- Copyright law



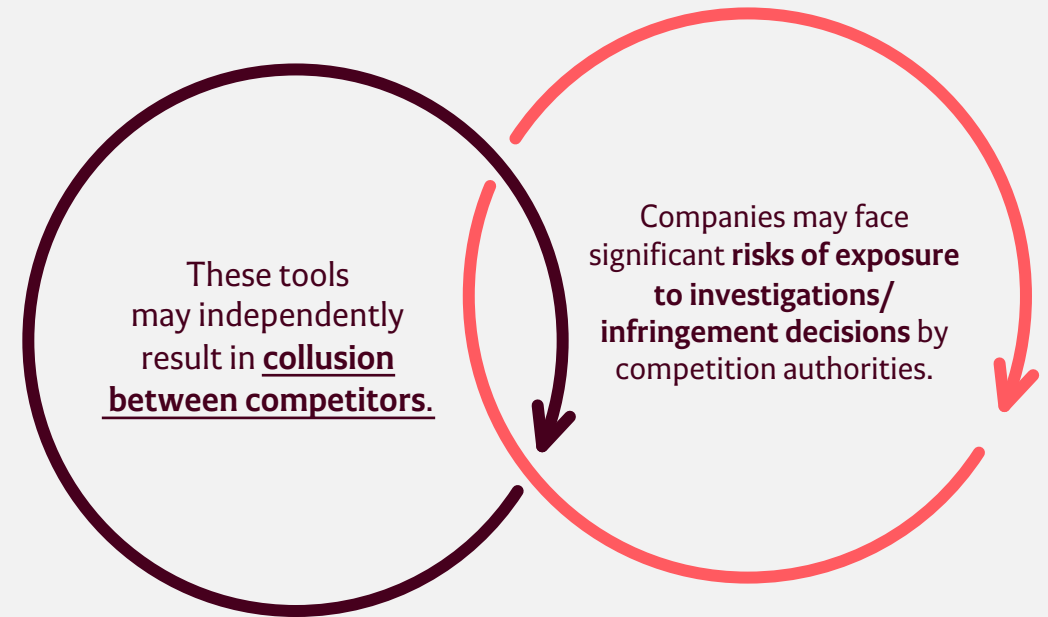
# 11. COMPETITION LAW: HOW TO COMPLY WITH COMPETITION LAW WHEN USING AI

## Potential anticompetitive implications of AI-powered benchmarking, marketing or pricing tools

- The provision of identical algorithms/systems to competitors may result in the alignment of their market behavior, particularly in terms of prices, output and clients.
- Self-learning algorithms may adapt to market conditions and, through their interactions, align pricing or other commercial/strategic decisions with competitors without the involvement, agreement or even knowledge of the user or deployer of such systems.

**Abuse of dominance:** AI systems should not be used by dominant companies to exclude competitors.

- This can happen—for example—through self-preferencing algorithms or the use of predatory pricing, rebates, and tying or bundling schemes, which can be further amplified by AI customer/profile targeting tools.



## Compliance by design

Representations and warranties	Due diligence	Market impact
Implement appropriate contractual safeguards to ensure the AI system provided is designed to prevent the company from engaging in collusive behavior.	Ensure any benchmarking or strategic/commercial decision-making AI system used is not provided or deployed simultaneously—or without any information barriers—with direct competitors.	Assess the potential exclusionary effects of any AI-powered targeting or self-preferencing systems, as well as the possible anticompetitive effects of increased market transparency through AI benchmarking tools.



## 12. LABOR AND EMPLOYMENT LAW: DOES THE NEW AI ACT AFFECT EMPLOYERS?

As employers, companies will be subject to the AI Act if:

- they use an AI system to manage staff-related issues—See [Section 3: Definition of AI system](#);
- the AI system uses employees' **data or makes labor-related decisions**, performs analyses or profiles individuals, monitors work performance, or interacts with employees;
- they are established **in the EU** or, if established outside the EU, use AI-generated data in the EU; and
- they are not exempt from the AI Act—see [Section 4: Actors subject to the AI Act](#).

### When is it considered a high-risk system?

When AI is used on employees to:

- **recruit personnel**, advertise jobs, analyze and filter applications, and evaluate candidates;
- **make decisions** regarding the working conditions, the promotion or termination of the employment relationship, or the assignment of tasks based on an individual's behavior or characteristics; and
- monitor and evaluate employees' **performance and behavior**.

### When is it not considered a high-risk system?

**When it does not pose a significant risk** of causing harm to employees' health, safety, or fundamental rights and does not significantly influence decision-making, **except** in cases involving the **profiling of individuals**.

The European Commission will develop **specific guidelines** with a comprehensive list of practical examples of high-risk and non-high-risk uses of AI systems.

### Prohibitions




The use of AI systems in the workplace is prohibited if it aims to **detect emotions** or **use biometric data to categorize** employees with the aim of obtaining sensitive data. See [Section 6: Prohibited AI practices](#)

# 12. LABOR AND EMPLOYMENT LAW: DOES THE NEW AI ACT AFFECT EMPLOYERS?

## 12.1 What obligations in the workplace does the AI Act impose on companies?

In addition to other obligations imposed on those in charge of deploying a high-risk AI system (see [section 7.3](#)), we highlight the following duties in the workplace:

**Informing employees and their representatives:** The information must be provided in compliance with the rules and practices established in national and EU laws.

EMPLOYERS' DUTY TO INFORM	 AI Act	 Spanish Workers' Statute	 Portuguese Labor Code
When does information have to be provided?	When a high-risk AI system is implemented or used in the workplace.	When algorithms or AI systems are used that affect decision-making relating to employment access, job retention and working conditions.	When algorithms or AI systems are used that affect decision-making relating to employment access, job retention and working conditions, including profiling and the monitoring of professional activity.
What should be reported?	The exposure to a high-risk AI system in compliance with national legal standards and practices for providing information to employees and their representatives.	<ul style="list-style-type: none"><li>• Its existence</li><li>• Parameters: Final model/algorithm's input variables</li><li>• Rules or instructions: Algorithm's internal logic</li></ul>	<ul style="list-style-type: none"><li>• Its existence</li><li>• Parameters</li><li>• Criteria</li><li>• Rules</li><li>• Instructions</li></ul>
Who should be informed?	All affected employees individually and their representatives.	Employees' legal representatives.	All affected employees individually, the works council and the trade union representatives.

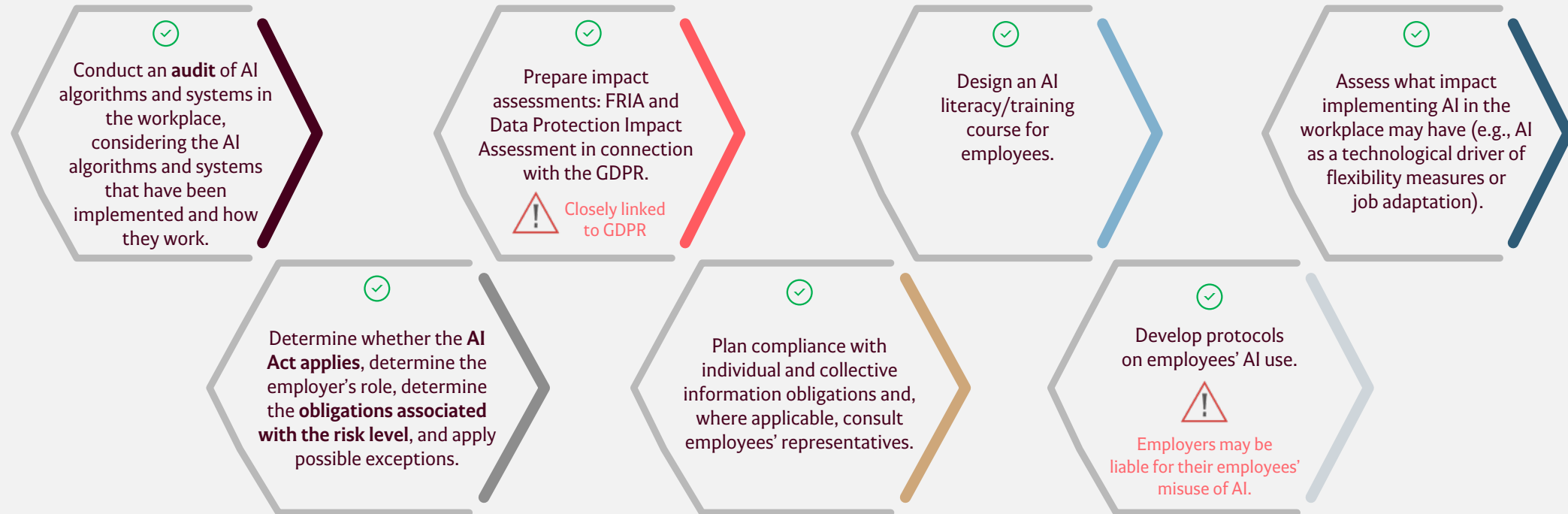
**AI literacy:** Employers must take measures to ensure their employees and other individuals responsible for operating and using AI systems on their behalf have sufficient AI literacy. This should encompass factors such as technical knowledge, experience, education, and training, alongside the intended uses and users of AI systems.

**Fundamental Rights Impact Assessment:** Before implementing an AI system, employers must carry out a Fundamental Rights Impact Assessment ("FRIA") in certain cases.

## 12. LABOR AND EMPLOYMENT LAW: DOES THE NEW AI ACT AFFECT EMPLOYERS?

### 12.2 How can HR areas prepare for the AI Act?

#### Action plan



#### What are the consequences of noncompliance with the AI Act?

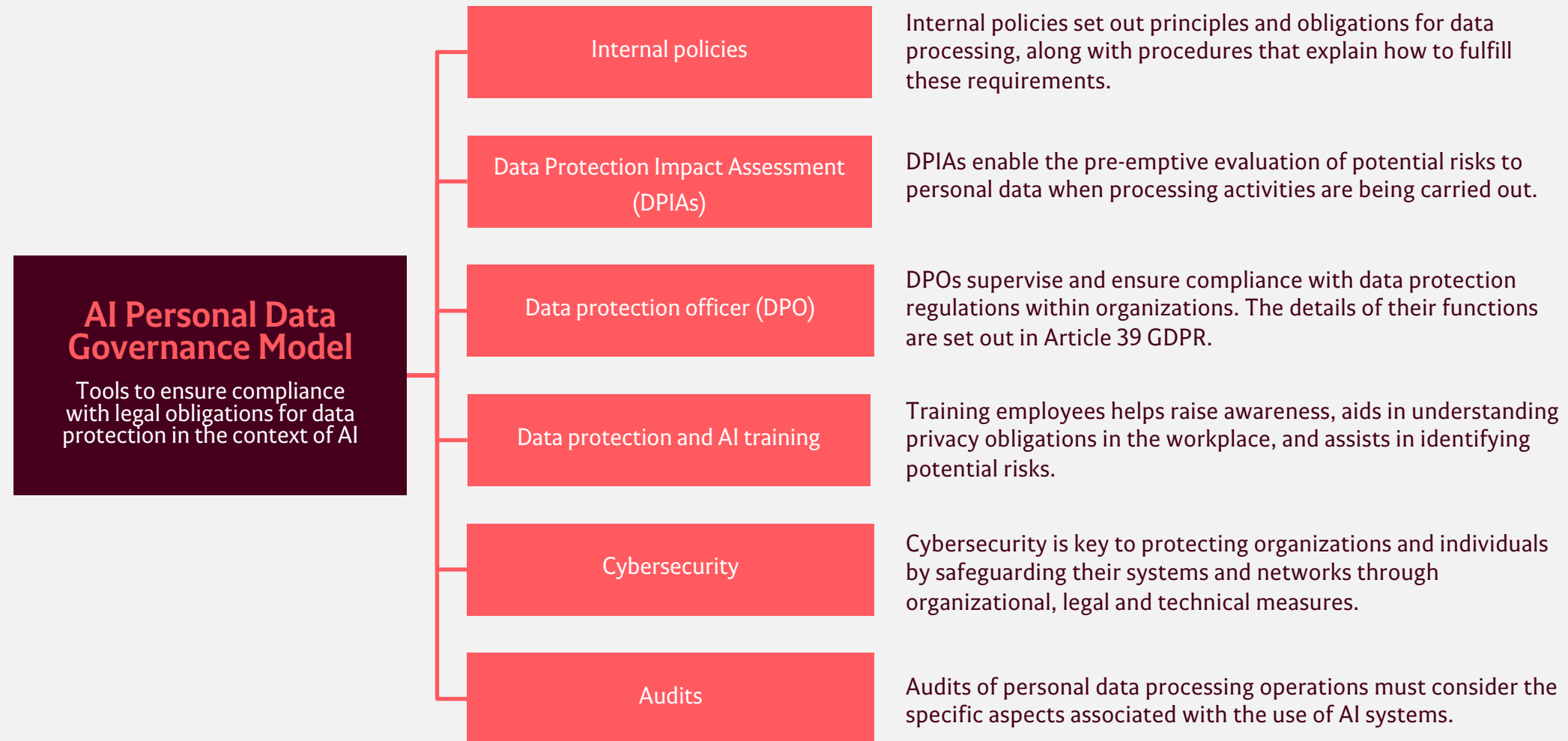
- Potential financial penalties as specified in the AI Act and national labor law-see [Section 4: Penalties](#).
- Compensation for violations of the affected individuals' fundamental rights (e.g., privacy, data protection, algorithmic discrimination, and trade union freedom).
- Claims may come from employees' representatives, trade unions, individual employees, the labor authority, or the supervisory authority overseeing the AI Act.

# 13. DATA PROTECTION AND THE AI ACT

- The AI Act is without prejudice to EU data protection legislation, particularly the GDPR. Compliance with the AI Act alone is insufficient when dealing with personal data.
- In each stage of an AI system’s lifecycle, there is a high likelihood that personal data will be processed, not only during the training stage but also in the deployment stage. Therefore, determining whether this processing complies with the GDPR is essential.
- Even if it were considered that no personal data have been processed, perhaps due to deletion or anonymization, this conclusion must still be documented. Demonstrating the effectiveness of these measures and evaluating any risk of re-identification is also necessary.

<p><b>ROLES AND RESPONSIBILITIES</b></p> <p>Different parties may have varying roles and responsibilities in data processing at distinct stages of an AI system’s lifecycle.</p> <p>For example, a developer may be considered as a data controller during the development stage but later as a data processor during the exploitation stage. There may also be scenarios where two or more parties are considered joint controllers.</p>	<p><b>AUTOMATED DECISIONS</b></p> <p>Under Article 22 GDPR, data subjects have the right not to be subject to decisions that have legal or equivalent effects, based solely on automated processing or profiling. When automated decisions are made based on a contract or the data subject’s explicit consent, the data controller must safeguard the data subject’s rights. These rights include the ability to seek human intervention from the controller, express personal views, and contest the decision.</p> <p>Relatedly, the AI Act requires that high-risk AI systems be subject to effective supervision by natural persons while they are in use.</p>
<p><b>LEGITIMATION OF PROCESSING</b></p> <p>Article 6 of the GDPR sets out six legal bases for the processing of personal data. Data processing at each stage of the AI system’s lifecycle may be justified on various legal grounds, such as the performance of a contract, the existence of a legitimate interest, or the consent of the data subjects, depending on the case.</p>	<p><b>DATA PROTECTION IMPACT ASSESSMENT</b></p> <p>The GDPR requires that a Data Protection Impact Assessment be carried out when the data processing is likely to pose a high risk to the data subject’s rights. Similarly, the AI Act also requires a Fundamental Rights Impact Assessment-however, this requirement is limited to certain scenarios.</p>

## 13. DATA PROTECTION AND THE AI ACT





## 14. HOW TO COMPLY WITH COPYRIGHT LAW WHEN USING AI

### 14.1 Input problem

1

AI systems need to be “taught” or “fed” with data and input so that they can use technical computational analyses to “learn.” They identify correlations, discern patterns, discover connections, make predictions, make decisions, and produce new results or output based on the information fed to them.

2

Copyright-protected work can serve as input for AI systems because they contain granular elements of information or data. However, unlike other ingredients that may be fed into AI systems, the existence of copyright can pose a barrier to applying AI to these protected contents.

3

Actions such as storing or uploading information into a computer system, scanning texts and images, transcribing audio, converting from one format to another, or retrieving information displayed on screen are all subject to reproduction rights under copyright law.

4

Reproducing protected works is only lawful if a license is obtained from the copyright holder or if it falls under an exception or limitation to the rights (legal license).

## 14. HOW TO COMPLY WITH COPYRIGHT LAW WHEN USING AI

### 14.1 Input problem

Without a license, what possible lines of defense could AI system providers and those who train them with copyrighted works have at their disposal?

A

The materials used are no longer protected because they have entered the public domain.

B

The input process is not subject to reproduction rights because it only takes atomized parts of each work and not expressive fragments subject to protection.

C

There is a legal exception or limitation that allows for their use, even if the reproduction right applies.

## 14. HOW TO COMPLY WITH COPYRIGHT LAW WHEN USING AI

### 14.2 Text and data mining exception

The text and data mining (“TDM”) exception is an exception under EU law that allows for the reproduction of works without an author’s consent for the purpose of applying automated analytical techniques. These techniques analyze texts and data in digital format to generate specific results, such as patterns, trends and correlations.

#### EXCEPTION THAT FAVORS MACHINE LEARNING

As these techniques need to reproduce copyrighted works (e.g., to pre-load the information into a computer system), the TDM exception will come into play.

#### VARIANT “A”: STRONG EXCEPTION

A strong exception is in place for research organizations, universities and cultural heritage institutions that have a public interest or non-profit mission. They cannot be prevented from carrying out TDM, even by way of license conditions.

#### VARIANT “B”: WEAK EXCEPTION

For other beneficiaries and purposes, TDM can only be done if the copyright holder has not objected through a properly made reservation of rights (opt out), such as through machine-readable means in the case of content made available to the public online.

## 14. HOW TO COMPLY WITH COPYRIGHT LAW WHEN USING AI

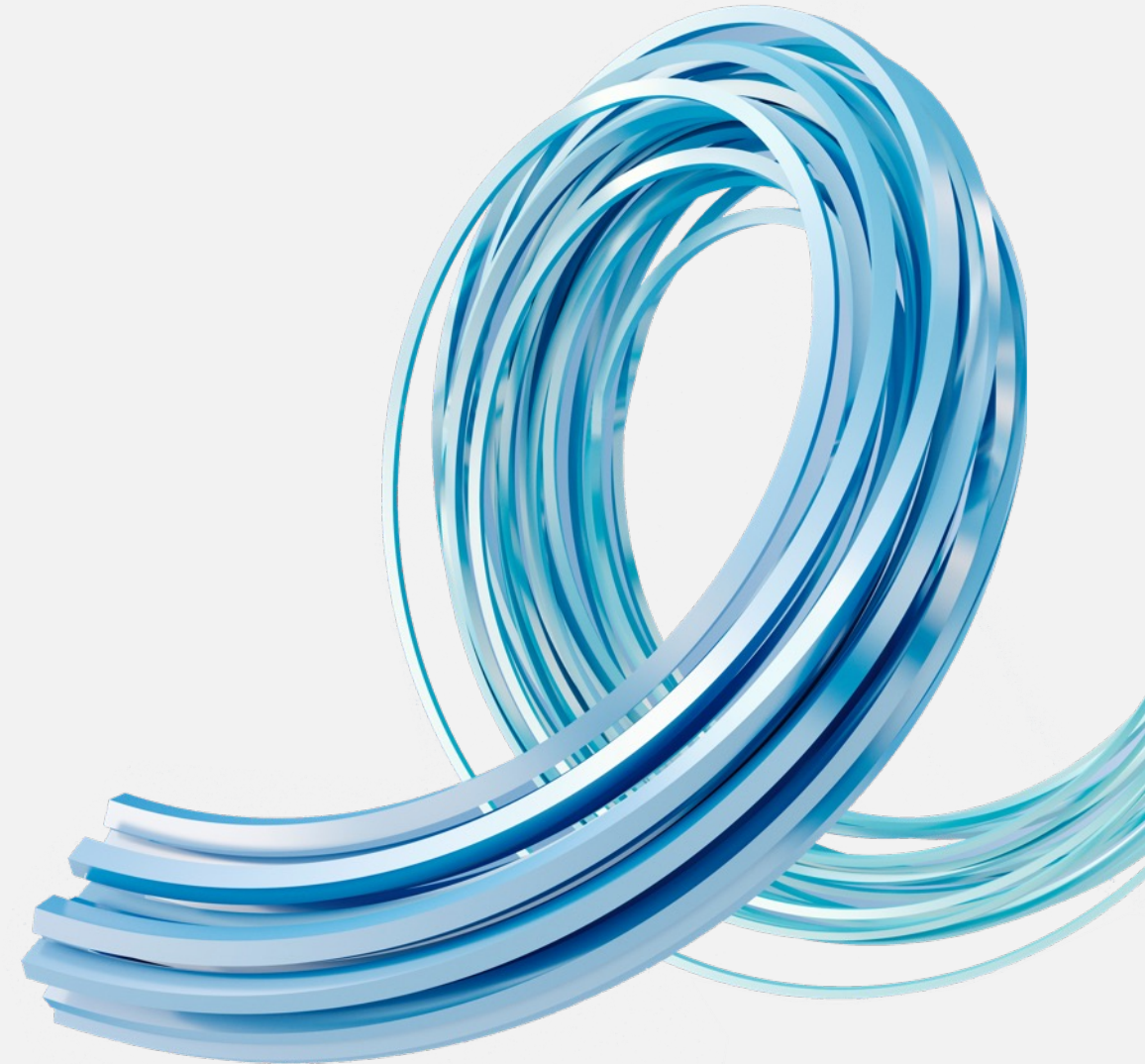
### 14.3 What specific obligations does the AI Act impose on companies regarding copyright?

In addition to the other obligations imposed on providers of general-purpose AI models (see [Section 9](#)), in relation to the data and texts used to train these models, including those protected by copyright, the AI Act stipulates that providers must prepare and make available to the public a sufficiently detailed summary of the content they used, in accordance with the template that will be provided by the European AI Office.

This summary must:

- consider the need to protect trade secrets and confidential business information; and
- be generally comprehensive in its scope to facilitate copyright holders to exercise and enforce their rights under Union law, for example by listing the main data collections or sets that went into training the model, such as large private or public databases or data archives, and by providing a narrative explanation about other data sources used

The AI Act also requires that providers of general-purpose AI models put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights regarding the TDM exception.





## What we offer

Through our highly specialized legal teams with extensive knowledge and experience, we advise on all areas of business law. We help our clients with the most demanding matters wherever they are based.

**29**

Legal specializations

**+1900**

Professionals

**26**

Offices in 12 countries

**29**

Nationalities & 16 languages

**+300**

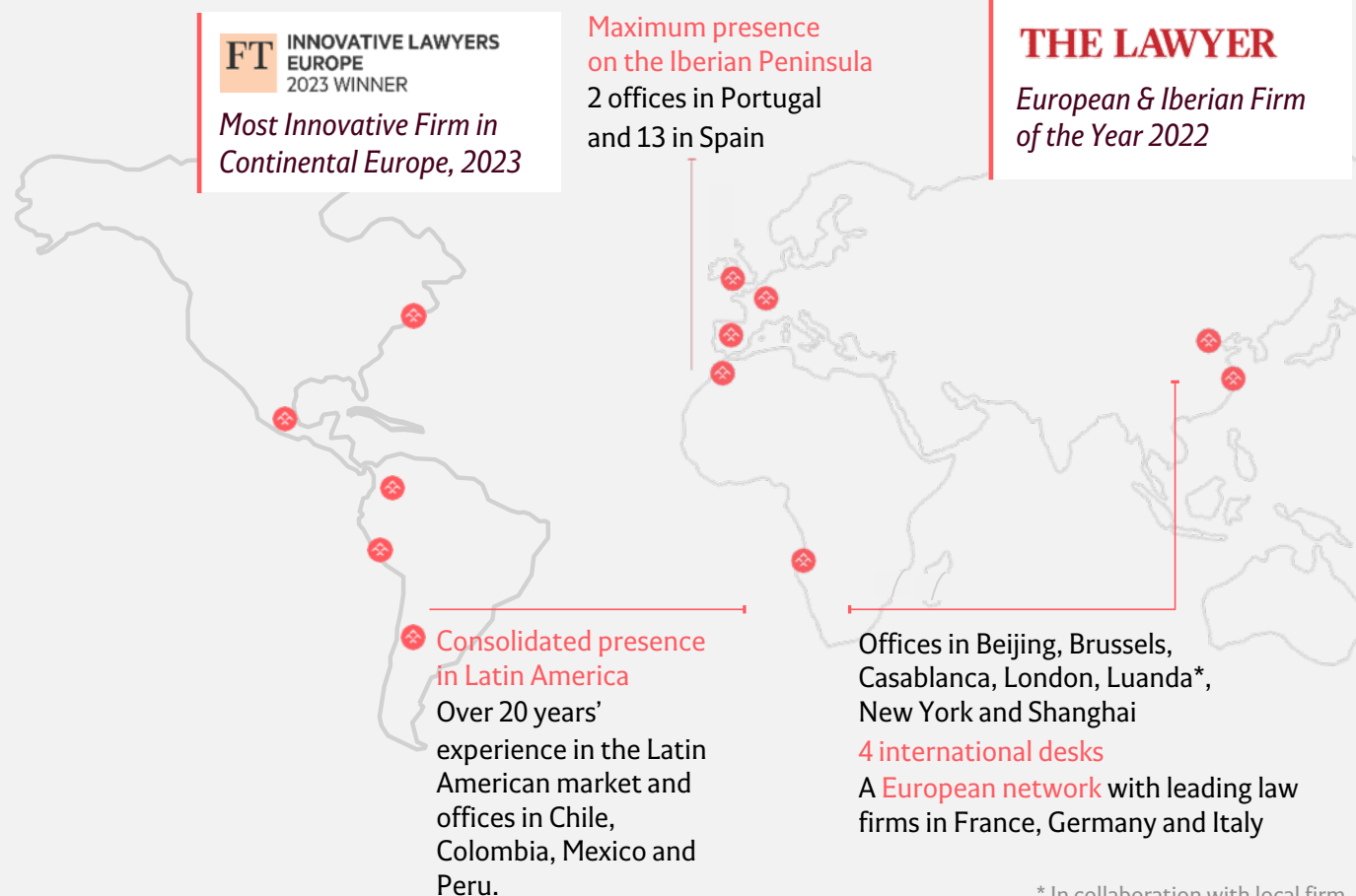
Lecturers & 10 professors

**26%**

Women in top positions



- Business-oriented knowledge with a sectorial approach.
- Maximal specialization combined with the latest technology.
- Knowledge and innovation team, with over 40 academics and specialists for innovative solutions.



At Cuatrecasas, we incorporate environmental, social and governance ("ESG") criteria in our service provision and in our internal management.

[Here](#) we describe the main parameters we use to measure our ESG performance

You can also access our latest [Corporate Sustainability Report](#).







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 acompañan. 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.

[cuatrecasas.com](https://www.cuatrecasas.com)