



## Navigating the EU AI Act: Unacceptable AI Practices and Compliance Strategies

January 2025



# Contents



|   |   |
|---|---|
| 01  | Unacceptable AI Practices: Prohibited on 2 February 2025        |
| 02  | Unacceptable AI Practices: The Core of EU's Risk-Based Approach |
| 03  | Liability: Impacts and Effects                                  |
| 04  | Specific Examples of Unacceptable AI Practices                  |
| 05  | Identification of Unacceptable Approaches                       |
| 06  | Alternative Compliant Approaches                                |
| 07  | Immediate Steps for Identifying Unacceptable AI Practices       |
| 08  | Strategic Approach: Governance, Awareness, and Monitoring       |
| 09  | Conclusion: Preparing for Compliance                            |
|  | How Can Deloitte Help?  |
|  | Get In Touch  |



# Unacceptable AI Practices: Prohibited on 2 February 2025

The use of unacceptable AI practices is **prohibited** by the European Union's Artificial Intelligence Act (AI Act) from **2 February 2025**.

**Penalties** regime applies from **2 August 2025**.



In the **intermediate period**, prohibited practices can already be considered **unlawful**.

Unlawfulness may make operators **vulnerable to civil action lawsuits** on other legal grounds (e.g., discrimination, consumer, employee, childrens' rights, etc.).

While the full application of the AI Act is not immediate, organizations should begin preparing for compliance as soon as possible, especially given the complexity of AI systems and the potential need for significant changes to existing practices to identify and prevent unacceptable use.

## 2025 - 2 February

- Prohibition of unacceptable practices
- AI Literacy requirement

## 2025 - 2 August

- AI Act sanctions

## 2026 - 2 August

- General application of requirements for high-risk systems

The AI Act introduces substantial penalties for violations, particularly those related to prohibited practices:

| Maximum fines   | Scaled penalties  | Market removal  | Liability for violation   | Reputational damage  |
|---|---|---|---|--|
| Up to €35 million or 7% of global annual turnover (whichever is higher) for violations related to prohibited practices. | Lesser fines for other types of violations, with the severity depending on the nature of the infringement and the size of the organization. | Potential removal of non-compliant AI systems from the EU market. | ...of other rights or requirements.<br>Use of prohibited practices constitutes an illegal action which can result in various types of harm to individuals or consequences based on other legal grounds. | Beyond financial penalties, non-compliance can lead to significant reputational harm and loss of public trust. |



# Unacceptable AI Practices: The Core of EU's Risk-Based Approach



The AI Act categorizes AI systems based on their **potential risks**.

Unacceptable risk practices are outright prohibited as they are **particularly harmful and abusive** and contradict Union values and fundamental rights.

For operators of AI solutions, **understanding the specifics** of these prohibitions, their **implications** and **strategies for ensuring compliance** is essential.

## EMOTIONS AT WORKPLACE AND EDUCATION

**Prohibition:** Using AI to infer emotions in workplaces or schools, except for medical or safety purposes.

**Example:** AI detecting employee emotions to influence productivity ratings or student engagement without their knowledge.

## IMAGE SCRAPPING

**Prohibition:** Creating or expanding facial recognition databases by scraping images from the internet or CCTV without consent.

**Example:** Collecting images from social media or public cameras without user permission for surveillance.

## PREDICTIVE POLICING

**Prohibition:** AI predicting criminal behavior solely based on personality traits or profiling, without objective facts.

**Example:** AI system predicting someone will commit a crime based on their personality test results.

## SUBLIMINAL TECHNIQUES

**Prohibition:** AI systems using techniques that manipulate or deceive beyond conscious awareness to distort behavior and impair informed decision-making, causing significant harm.

**Example:** Ads using subliminal messages or exploiting emotional state to push impulsive purchases or change habits without user awareness.

**UNACCEPTABLE**  
Prohibited

## SOCIAL SCORING

**Prohibition:** AI systems classifying people based on their behavior or characteristics, leading to unfair treatment in unrelated contexts.

**Example:** Denying someone a loan due to negative social media behavior or past unrelated actions.

## EXPLOITING VULNERABILITIES

**Prohibition:** AI systems exploiting vulnerabilities due to age, disability, or economic status to distort behavior and cause harm.

**Example:** Manipulative marketing targeting children or elderly people to purchase unnecessary products.

## REAL TIME BIOMETRIC IDENTIFICATION BY LAW ENFORCEMENT

**Prohibition:** Using real-time biometric systems (like facial recognition) in public spaces for law enforcement, except for specific situations.

**Example:** Using facial recognition at a public event for surveillance without a genuine imminent threat.

## BIOMETRIC CATEGORISATION

**Prohibition:** Using AI to categorize individuals by biometric data (race, political views, religion, etc.), leading to biased conclusions.

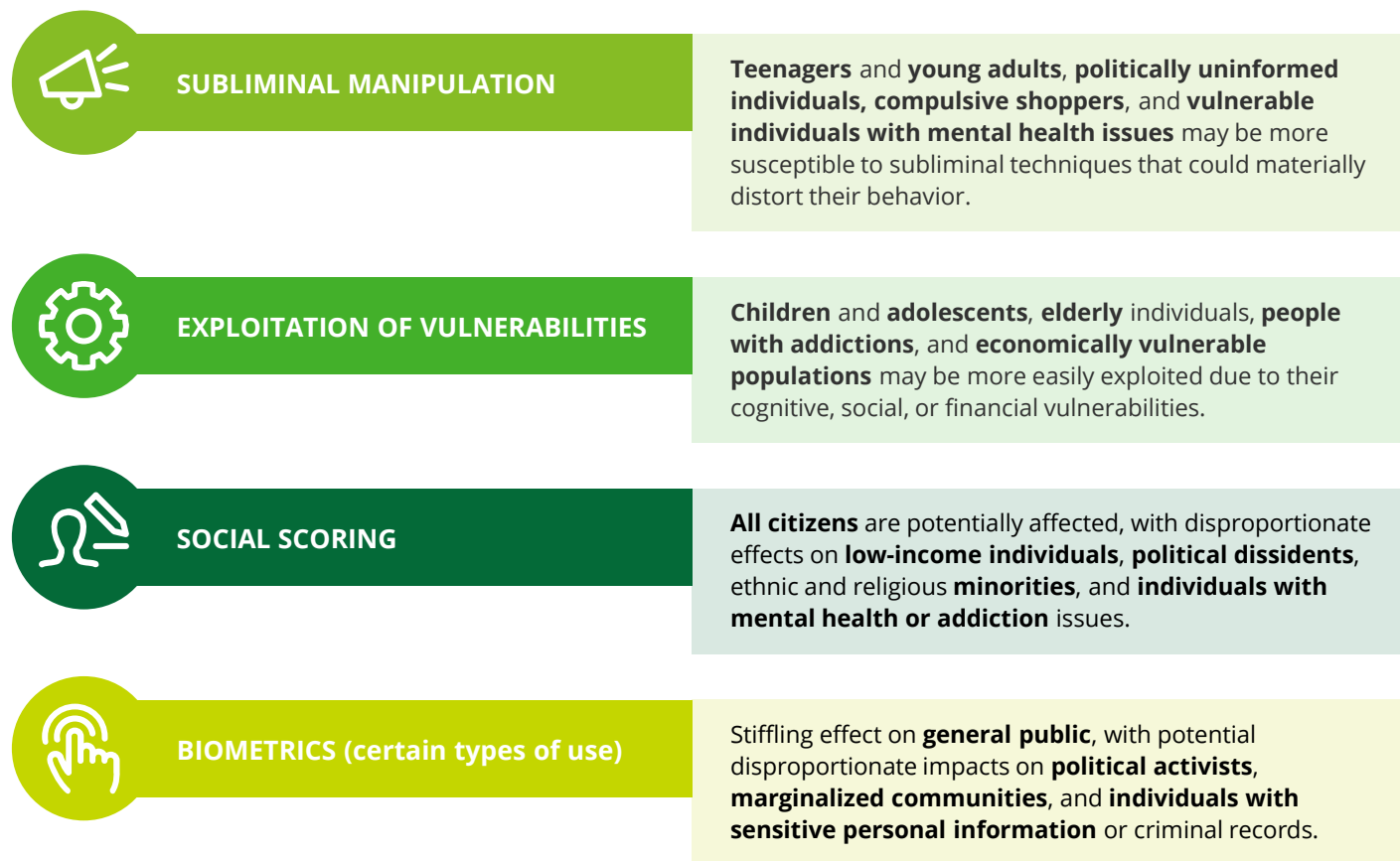
**Example:** Classifying people based on facial features to infer their religion or political beliefs.

The AI Act prohibits systems that manipulate user behavior and exploit vulnerable populations, and which result in **significant harm** due to privacy violations, misuse of personal data, potential for discrimination, or disregard for safety.

Such systems have been noted **in various sectors**, which include social media and online platforms, gaming and gambling, political campaigning, healthcare and fitness, education, financial services and law enforcement and criminal justice.

## Affected groups of (selected) unacceptable AI practices

*An indicative selection of key population groups which are impacted and affected by unacceptable practices.*



# 4

## Specific Examples of Unacceptable AI Practices

To provide a clearer understanding of what constitutes unacceptable AI practices, let's examine specific examples of selected systems or algorithms from various industries and business functions:

### 4.1

#### Subliminal Manipulation

##### SOCIAL MEDIA ENGAGEMENT ALGORITHMS

use **imperceptible visual or auditory cues** in videos to influence users' emotional states and **increase platform engagement**. For example, an algorithm might subtly alter the rhythm or tone of video content to trigger specific emotional responses, leading to increased time spent on the platform without the user's conscious awareness.

##### HEALTH AND FITNESS AI COACH

can **create unrealistic body image expectations** and promote extreme diet regimens, potentially exacerbating body image issues and **promoting unhealthy behaviors**. They can lead to an increase in eating disorders, dangerous fitness practices, and psychological distress.

### 4.2

#### Exploitation of Vulnerabilities

##### AGE-TARGETED SOCIAL MEDIA ALGORITHMS

could potentially **exploit** younger **users' vulnerabilities** by promoting content that **encourages harmful behaviors** or excessive platform use. This might include algorithms that identify and target users who are more susceptible to peer pressure or have shown interest in dangerous trends.

##### AI-POWERED GAMBLING APPLICATIONS

use AI to **identify individuals prone to gambling addiction** and target them with personalized offers or content designed to **encourage continued gambling**. For instance, an app might analyze user behavior to detect patterns indicative of addiction and then serve tailored promotions during times when the user is most vulnerable.

### 4.3

#### Social Scoring

##### AI-DRIVEN EMPLOYEE EVALUATION SYSTEMS

assess workers based on **multiple data points of social behavior**, potentially leading to **unfair treatment in unrelated contexts**. For example, an AI might analyze an employee's social media activity, spending habits, or personal relationships to make decisions about promotions or job assignments, even when these factors are not relevant to job performance.

##### AI-POWERED INSURANCE RISK ASSESSMENT

uses **social behavior data unrelated to health** for insurance decisions, potentially **creating discriminatory insurance practices** based on lifestyle choices. It can lead to unfair denial of coverage or increased premiums based on non-health-related factors, discrimination against certain social groups, erosion of risk pooling principles in insurance, and privacy concerns regarding personal data use.

# 5

## Identification of Unacceptable Approaches

Risk classification of AI systems can depend on **specific decisions or effects** along the **AI lifecycle** which can result in **violations of existing legal rules**.

Organizations must take proactive steps to identify and address any potentially unacceptable AI practices **throughout their inventory**.



For example, inadequate AI governance or management practices can introduce **unacceptable elements or performance** into an otherwise lower risk system, inadvertently converting it into a prohibited practice.

**Appropriate AI governance and risk management procedures** can help **identify and remediate** problematic approaches.

Often, unacceptable classification or prohibition of a particular system can be avoided by using appropriate **alternative approaches**, resulting in reclassification of the system to a lower risk category (depending on other characteristics).

| SYSTEM                                | IDENTIFICATION   | ALTERNATIVE COMPLIANT APPROACH (indicative)  |
|---------------------------------------|--|--|
| SOCIAL MEDIA ENGAGEMENT ALGORITHMS    | Analyze use of subtle <b>visual and auditory cues</b> in video content, focusing on their potential to trigger specific emotional responses. | Transparent recommendation systems with user-defined preferences.                    |
| HEALTH AND FITNESS AI COACH           | Analyze <b>fitness and nutrition advice</b> against established medical guidelines and best practices for diverse body types.                | AI health assistants with medical professional oversight and body-positive approach. |
| AGE-TARGETED SOCIAL MEDIA ALGORITHMS  | Assess <b>how the algorithm tailors and delivers content</b> to different age groups, with a focus on protecting minors.                     | Age-appropriate content recommendation systems with parental oversight options.      |
| AI-POWERED GAMBLING APPLICATIONS      | Analyze <b>user profiling algorithms</b> to identify how it detects and targets potentially vulnerable individuals.                          | Responsible gambling tools with self-exclusion options and spending limits.          |
| AI-DRIVEN EMPLOYEE EVALUATION SYSTEMS | Evaluate <b>use of social behavior data</b> in employee assessments, focusing on relevance to job performance.                               | Skills-based assessment tools with transparent evaluation criteria.                  |
| AI-POWERED INSURANCE RISK ASSESSMENT  | Examine the <b>types of social behavior data</b> used in risk assessments and their relevance to actual health risks.                        | Risk assessment based on verified health data and objective risk factors.            |

# 6

## Alternative Compliant Approaches

Various **mitigation and remediation measures** can be implemented to prevent unacceptable results, prevent substantial harm, and achieve compliance. Systems must be compliant with other legislation relevant to the industry or affected users, not only the AI Act. Below is a brief indication of approaches for selected systems.

| SOCIAL MEDIA ENGAGEMENT ALGORITHMS   | HEALTH AND FITNESS AI COACH   | AGE-TARGETED SOCIAL MEDIA ALGORITHMS  | AI-POWERED GAMBLING APPLICATIONS   | AI-DRIVEN EMPLOYEE EVALUATION  | AI-POWERED INSURANCE RISK ASSESSMENT   |
|--|---|---|--|--|--|
| <ul style="list-style-type: none"> <li>Implement transparent <b>content ranking</b> systems</li> <li>Develop <b>user-controlled engagement</b> settings</li> <li>Establish <b>time limit features</b> and usage alerts</li> <li>Conduct regular <b>impact assessments</b></li> <li>Offer <b>alternative, non-algorithmic feed</b> options</li> </ul> | <ul style="list-style-type: none"> <li>Implement clear health risk <b>disclaimers</b></li> <li>Develop <b>diverse body type representation</b> in AI models</li> <li>Establish <b>professional healthcare oversight</b></li> <li>Conduct regular <b>impact assessments</b></li> <li><b>Offer alternative</b>, body-positive fitness approaches</li> </ul> | <ul style="list-style-type: none"> <li>Implement strict <b>age verification</b> processes</li> <li>Develop age-appropriate <b>content filters</b></li> <li>Establish <b>parental control</b> mechanisms</li> <li>Conduct regular <b>impact assessments</b></li> <li>Offer educational resources on <b>digital literacy</b></li> </ul> | <ul style="list-style-type: none"> <li>Implement mandatory <b>loss limits and cooling-off</b> periods</li> <li>Develop AI-powered <b>addiction detection</b> systems</li> <li>Provide real-time responsible gambling <b>interventions</b></li> <li>Offer <b>self-exclusion options</b> with biometric verification</li> <li>Conduct regular <b>fairness audits</b> of game outcomes</li> </ul> | <ul style="list-style-type: none"> <li>Implement <b>transparent evaluation</b> criteria</li> <li>Develop <b>diverse and inclusive training datasets</b></li> <li>Establish <b>human oversight and appeal</b> processes</li> <li>Conduct regular <b>bias and fairness audits</b></li> <li>Offer <b>complementary, traditional evaluation</b> options</li> </ul> | <ul style="list-style-type: none"> <li>Implement <b>transparent risk assessment</b> criteria</li> <li>Develop <b>diverse and representative training data</b></li> <li>Establish <b>human oversight</b> for high-risk decisions</li> <li>Conduct regular <b>bias and fairness audits</b></li> <li>Offer <b>alternative, traditional risk assessment</b> options</li> </ul> |





# Immediate Steps for Identifying Unacceptable AI Practices



## 7.1 Comprehensive AI Inventory

*Conduct a Thorough Audit*

- Develop a comprehensive **inventory of all AI systems** currently in use or under development and ensure **regular updates**.
- Consider **all IT systems**, regardless of their current AI capabilities.
- Include AI systems **used in all departments**, from customer service chatbots to HR recruitment tools and financial risk assessment models. Also consider systems used in physical infrastructure, such as biometrics in elevators or at entrances.
- Don't forget to include AI systems provided by third-party vendors or partners that your organization uses.
- **Document** each system's **details** and identify key stakeholders.



## 7.2 Risk Assessment Framework

*Develop a Structured Evaluation Approach*

- Create a **standardized framework for evaluating** AI systems against the AI Act
- Include **clear guidelines** for assessing potential unacceptable practices.
- Develop a **scoring system** or risk matrix to quantify the level of risk associated with each AI system.
- Develop **policies and procedures** for identification of risk factors in the design and development procedures, and for **application of appropriate compliant technologies**.



## 7.3 Regular Compliance Reviews

*Implement Periodic Reviews*

- Establish a schedule for **regular reviews** of all AI systems to ensure ongoing compliance with the AI Act.
- Conduct **more frequent reviews for high-risk** systems or those operating in sensitive areas.
- Include both **internal reviews and external audits** in your compliance strategy.

*Stay Informed on Regulatory Developments*

- Assign responsibility for **monitoring updates to the regulatory framework**, including new guidelines or interpretations from EU authorities.
- Participate in **industry forums and working groups** focused on AI regulation and compliance.
- Establish a **process for quickly disseminating regulatory updates throughout your organization** and updating compliance procedures accordingly.



# 8

## Strategic Approach: Governance, Awareness, and Monitoring

### 8.1 Establish AI Governance Framework

#### Develop Clear Guidelines

- Create **policies and guidelines for AI development and deployment**.
- Ensure these guidelines **align with the AI Act's requirements** and reflect ethical AI principles.

#### Create a Cross-functional AI Ethics Committee

- Establish a **diverse committee** with representatives from legal, technical, ethical, and business backgrounds.
- **Review and approve AI projects**, particularly those with potential high-risk applications.
- **Define clear escalation paths** for addressing concerns or potential violations of the AI Act.

#### Implement Accountability Measures

- Clearly **define roles and responsibilities** for AI governance within your organization.
- **Establish key performance indicators (KPIs)** for measuring compliance and ethical AI practices.
- Create a system of **checks and balances to ensure oversight** at all stages of AI development and deployment.

### 8.2 Employee Training and Awareness

#### Implement Comprehensive Training Programs

- Develop **tailored training modules** for different roles within the organization as part of AI Literacy.
- Include both **theoretical knowledge and practical application** of ethical AI principles.
- Regularly **update training content**.

#### Foster a Culture of Responsible AI

- **Integrate ethical considerations** into all stages of AI development and deployment processes.
- **Encourage open dialogue** about potential risks and ethical implications of AI projects.
- **Recognize and reward employees** who demonstrate commitment to responsible AI practices.

#### Provide Ongoing Support and Resources

- Establish an AI ethics helpdesk or support team to **address questions and concerns**.
- Create and maintain a **knowledge base** of AI ethics resources, case studies, and best practices.
- Regularly **communicate updates and insights** related to AI ethics and compliance.

### 8.3 Continuous Monitoring and Auditing

#### Deploy Monitoring Tools

- Implement automated tools for **ongoing monitoring of AI system** behaviors and outputs.
- Establish **alert systems** to flag potential anomalies or deviations from expected performance.
- Develop dashboards to provide real-time visibility into AI system **operations and compliance metrics**.

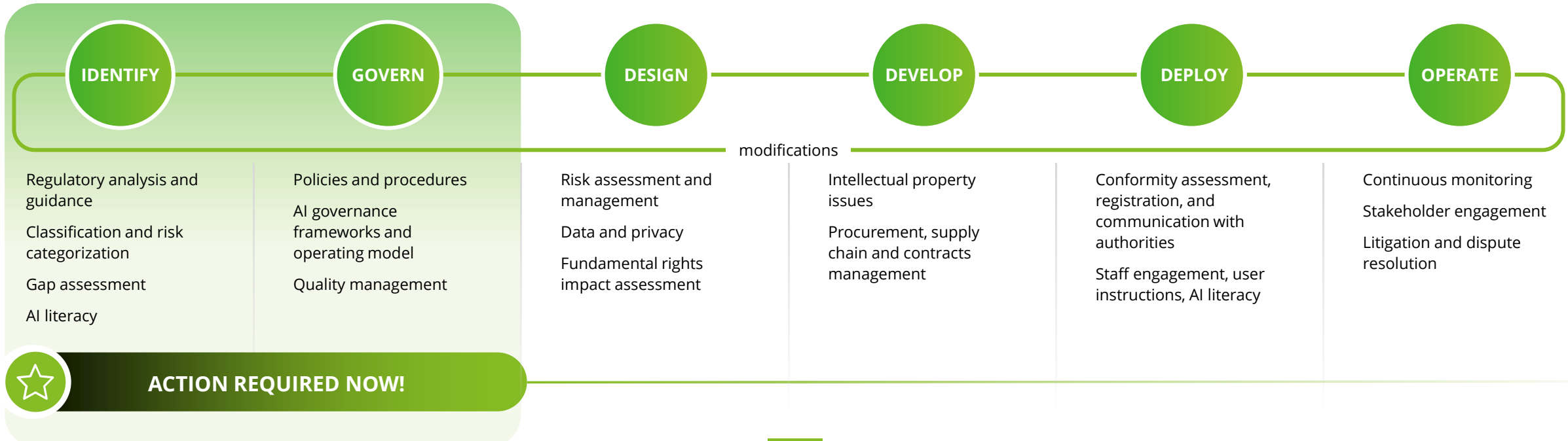
#### Conduct Regular Audits

- Schedule **periodic internal audits** of AI systems, focusing on high-risk applications.
- **Engage external auditors** to provide independent assessments of compliance and ethical practices.
- Develop a **standardized audit framework** aligned with the AI Act's requirements and industry best practices.




#### Implement Feedback Loops

- Establish mechanisms for **collecting and analyzing feedback** from users and stakeholders affected by AI systems.
- Create processes for rapidly **addressing identified issues** or potential non-compliance.
- Use insights from monitoring and audits to **continuously improve AI governance practices**.

# Conclusion: Preparing for Compliance



As the enforcement of the **EU AI Act** approaches, organizations must take proactive steps to identify and address potentially unacceptable AI practices. By implementing robust governance structures, conducting thorough assessments, and staying informed about regulatory developments, businesses can navigate the complex landscape of AI regulation, ensure compliance and manage risks.

- 
**Conduct a comprehensive AI inventory** and risk assessment across your organization.
- 
**Establish robust AI governance structures**, including clear policies and a cross-functional ethics committee.
- 
**Implement training and awareness programs** to foster a culture of quality and AI literacy.





# How Can Deloitte Help?



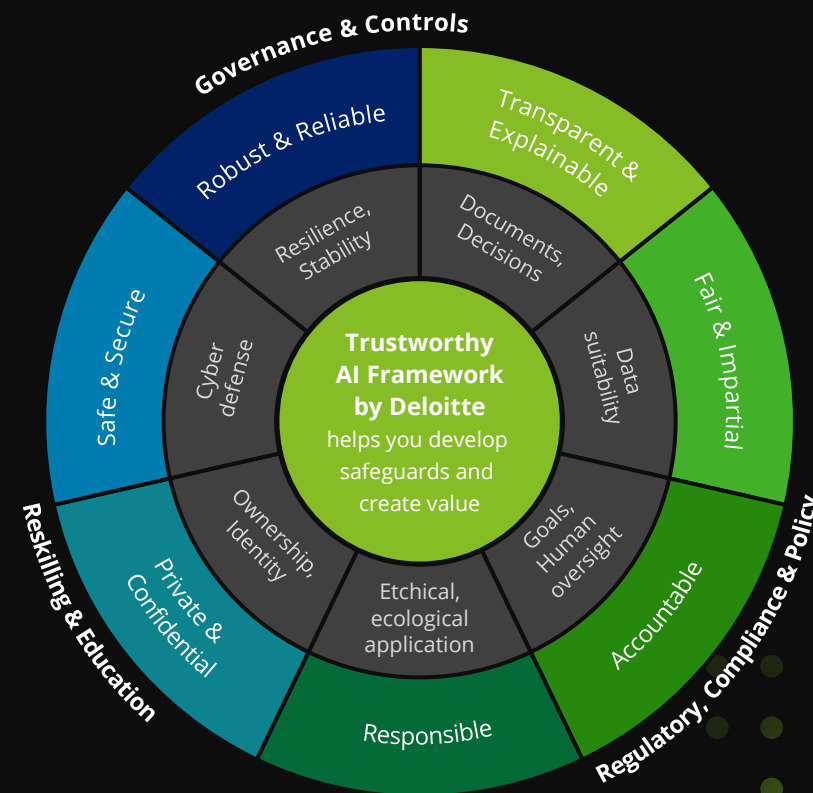
To prevent blind spots during the initial steps, or to find optimal solutions at other stages of the process, compliance activities benefit from a holistic approach.

**Through its multidimensional Trustworthy AI Framework, Deloitte helps organizations develop safeguards for trustworthy AI development and deployment at all levels of the supply chain.**

Our multidisciplinary capabilities in legal, risk, ethics, audit, assurance, business, and technology consulting enable tailored, efficient, and effective support through all lifecycle stages of AI systems, on a global level and with an in-depth understanding of local specifics.

Deloitte's experience ranges from high level AI governance and improving operations to providing support for regulatory activities to access the markets and supply chain alignment for specific applications. We assist clients in bridging gaps, developing specific solutions, or assessing the value of proposals and implementations.

## Deloitte's Trustworthy AI Framework





## Get In Touch

### Contact us now

*to find out more about this legislation and how we can support you in your AI journey.*



#### Jan Michalski

Partner  
Central Europe GenAI Leader

[jmichalski@deloittece.com](mailto:jmichalski@deloittece.com)



#### Simina Mut

Partner at Reff & Associates | Deloitte Legal  
Leader of Deloitte Legal Central Europe

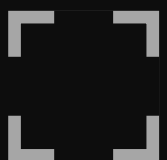
[smut@deloittece.com](mailto:smut@deloittece.com)



#### Gregor Strojcin

Deloitte Legal Central Europe  
AI Regulatory CoE Leader

[gstrojcin@deloittelegal.si](mailto:gstrojcin@deloittelegal.si)





# Get In Touch



## Albania



**Ened Topi**  
Senior Manager  
etopi@deloittece.com



**Ina Cota**  
Manager  
icota@deloittece.com

## Baltics



**Ruta Passos**  
Manager  
rpassos@deloittece.com

## Bosnia & Herzegovina



**Elma Delalic-Haskovic**  
Manager  
edelalic@deloittece.com



**Zerina Pacariz**  
Manager  
zpacariz@deloittece.com

## Bulgaria



**Adelina Mitkova**  
Senior Managing Associate  
amitkova@deloittece.com



**Mila Goranova**  
Manager  
mgoranova@deloittece.com

## Croatia



**Zrinka Vrtarić**  
Attorney-at-law  
zvrtaric@kip-legal.hr



**Ratko Drča**  
Director  
rdrca@deloittece.com

## Czech Republic

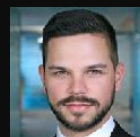


**Jaroslava Kracunova**  
Partner  
jkracunova@deloittece.com



**Jakub Holl**  
Director  
jholl@deloittece.com

## Hungary



**Daniel Nagy**  
Managing Associate  
dnagy@deloittece.com



**Gergő Barta**  
Senior Manager  
gbarta@deloittece.com



# Get In Touch



## Kosovo



**Donika Ahmeti**  
Senior Manager  
dahmeti@deloittece.com



**Ardian Rexha**  
Senior Manager  
arrexha@deloittece.com

## Poland



**Ścibor Łapieś**  
Partner  
slapies@deloittece.com



**Tomasz Ciećwierz**  
Partner  
tciecwierz@deloittece.com

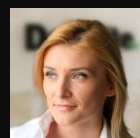


**PhD Michał Mostowik**  
Senior Managing Associate  
mmostowik@deloittece.com

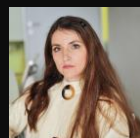
## Romania



**Andrei Paraschiv**  
Partner  
anparaschiv@deloittece.com



**Simina Mut**  
Partner  
smut@deloittece.com



**Silvia Axinescu**  
Senior Managing Associate  
maxinescu@reff-associates.ro

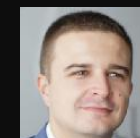
## Serbia



**Miroslava Gaćeša**  
Director  
mgacesa@deloitteCE.com



**Stefan Ivic**  
Partner  
stivic@deloittece.com



**Stefan Antonic**  
Attorney-at-law  
santonic@deloittece.com

## Slovakia



**Pavol Szabo**  
Senior Managing Associate  
pszabo@deloittece.com



**Dagmar Yoder**  
Partner  
dyoder@deloittece.com

## Slovenia



**Ana Kastelec**  
Local Partner  
akastelec@deloittelegal.si



**Lan Filipič**  
Director  
lfilipic@deloittece.com

## Ukraine



**Mykhailo Koliadintsev**  
Manager  
mkoliadintsev@deloittece.com



**Dmytro Pavlenko**  
Partner  
dpavlenko@deloittece.com



**Author:** Gregor Strojnj, Deloitte Legal Central Europe AI Regulatory CoE Leader, [gstrojnj@deloittelegal.si](mailto:gstrojnj@deloittelegal.si)

#### **About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

Deloitte Central Europe is a regional organization of entities organized under the umbrella of Deloitte Central Europe Holdings Limited, a member firm in Central Europe of Deloitte Touche Tohmatsu Limited. Services are provided by the subsidiaries and affiliates of Deloitte Central Europe Holdings Limited, which are separate and independent legal entities. The subsidiaries and affiliates of Deloitte Central Europe Holdings Limited are among the region’s leading professional services firms, providing services through more than 13,000 people in 45 offices in 19 geographies.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

©2025. For information, contact Deloitte Legal Central Europe.