SQUIRE PATTON BOGGS

The EU Has a (Provisional) Political Agreement to Regulate AI

What You Should Know and What You Should Do

On December 8, 2023, after some intense rollercoaster rides, the European Union (EU) institutions reached a political agreement on the EU Artificial Intelligence Act (EU AI Act). The compromises reached after sleepless nights still need to find their way into a final text (and this one might only be available after the holiday season), but it seems the EU will have its first horizontal piece of AI legislation.

We summarize the essentials of what has been agreed and are also highlighting the changes* compared to the initial EU AI Act proposal back in April 2021. The EU AI Act has been one of the most lobbied pieces of regulation so far and its outcome reflects such tensions.

*changes are highlighted in bold and teal

Fundamentals

A horizontal approach to what?	• Creates the conditions for the development and use of trustworthy and human-centered AI systems in the EU. • Provides a technology-neutral definition of AI systems – **that aligns with the OECD**. • Sets a risk-based classification of AI systems: banned, high risks (strict rules), low risks and **foundation models**.
Who does it apply to?	• To developers and users in the EU. It also applies to global vendors selling or otherwise making their system or its output available to users in the EU. The "Brussels effect" is popular (among the EU rulemakers).
When will it apply?	Within: • **Six months following adoption (for prohibited uses)** • **12 months (for General Purpose AI)** • a 18-to-24-month transition period for all other rules (circa first half of 2026).

Key Considerations

Scope

All AI systems (under the OECD definition), unless they are:

- **Falling within the national security remit of member states.**
- **Used for military or defense purposes.**
- **Used for research and innovation.**
- **Free and open-source software – unless they qualify as a high-risk system or prohibited AI.**

Prohibited AI Uses

Uses of AI that pose "unacceptable risks", some new entrants:

- **Non-targeted scraping of facial images for facial recognition**
- **Emotion recognition in the workplace and educational institutions**
- **Biometric categorization using sensitive data such as sexual orientation or religious beliefs.**
- Some instances of predictive policing of individuals

Others, including, social scoring and real-time biometric identification in publicly accessible spaces by law enforcement authorities (except in limited and pre-authorized situations) remain. The same for AI systems manipulating cognitive behavior or exploiting people's vulnerabilities (age, disability, etc.).

General Purpose AI Systems

AI systems that can be used for many different purposes (GPAI) will have to comply with transparency obligations:

- Disclosing that the content was generated by AI.
- Inform individuals that they are interacting with an AI system.
- **Generate technical documentation.**
- **Preserve training data summaries.**
- **Protect copyright and IP.**

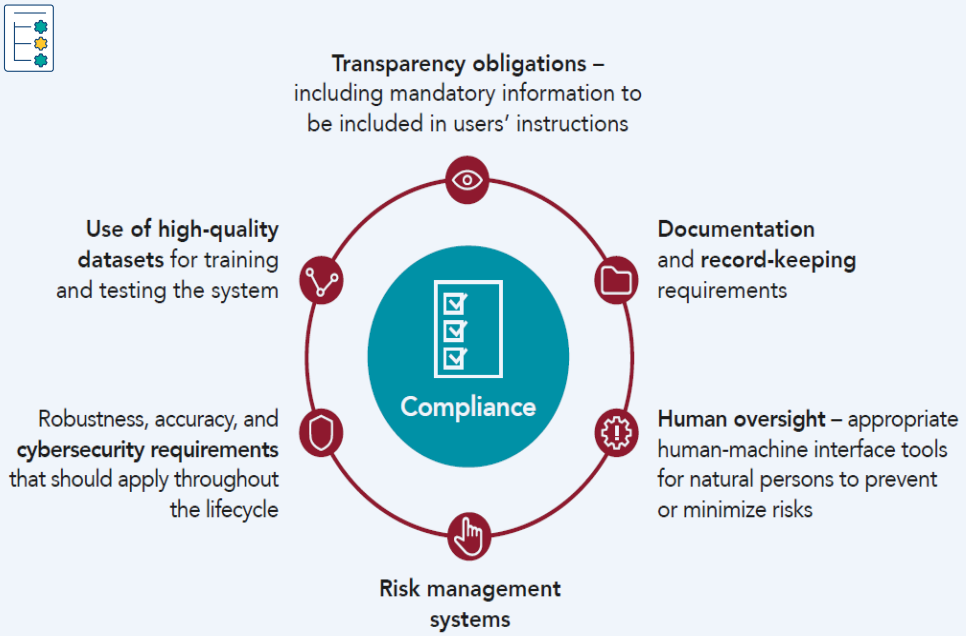
High-risk Systems

No drastic changes on the list, following areas are (amongst others) considered high risk:

- Medical devices
- Vehicles
- Education
- Employment
- Critical infrastructure
- Access to services
- Emotion recognition systems
- Biometric identification
- Law enforcement
- Border control
- Administration of justice and democratic processes

The Annex III taxonomy remains (safety component).

High-risks AI systems are authorized, subject to requirements and obligations to gain access to the EU market (Conformity (self-) assessment, **registration of the uses in either a public or private database**, and in some instances, a **Fundamental Rights Impact Assessment)**:



Foundation Models

What Are They?

These are large systems capable of competently performing a wide range of distinctive tasks (i.e., generating video, text, images, conversing in lateral language, computing or generating computer code).

These models must comply with **specific transparency obligations** before they are placed in the market, **including reporting on energy consumption, and publishing a sufficiently detailed summary of the training data "without prejudice of trade secrets."**

"High-impact" Foundation Models

These are foundation models trained with large amounts of data and with advanced complexity, capabilities and performance well above the average, as well as **a stricter applicable regime requiring model evaluations, risk assessments, incident reporting and cybersecurity protection.**

Enforcement & Governance

- Local enforcement – potentially complex cross-sectoral dialogue needed at the domestic level. Market surveillance authorities in EU countries to enforce the AI Act. Any individual should be able to file complaints for non-compliance.
- EU-wide enforcement & coordination:
  - **An AI Office (within the European Commission) will oversee, contribute to fostering standards and testing practices, and enforce specific cross-border cases.**
  - The AI Board survives as a coordination platform and an advisory body to the European Commission.
- Stakeholder involvement:
  - **A scientific panel of independent experts will advise the AI Office about GPAI models.**
  - **An advisory forum for stakeholders will be set up to provide technical expertise to the AI Board.**

Penalties

High level of fines:

- €35 million or 7% for violations of the banned AI applications
- €15 million or 3% for violations of the AI Act's obligations
- €7.5 million or 1.5% for the supply of incorrect information

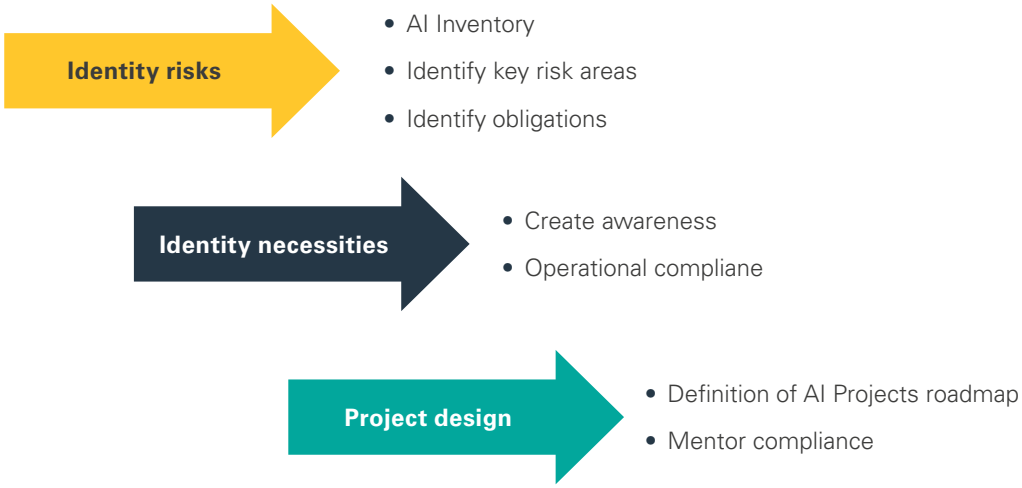
Proportionate administrative fines will be considered for SMEs and startups in case of infringements of the provisions of the AI Act.

Next Steps

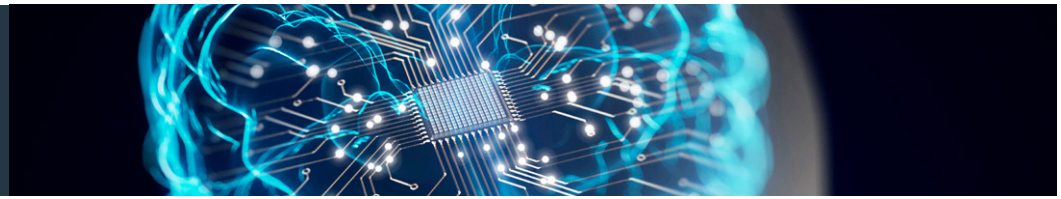
The details presented above (and the deviations from the initial EU AI Act proposal) are an overview based on what is known of the political agreement. The text must still be finalized and adopted by the Parliament and the Council to become EU law. Technical meetings have been arranged to finalize details and adoption in early 2024 seems realistic.

The AI Pact (i.e., the European Commission inviting AI developers to voluntarily commit to implementing key obligations of the AI Act ahead of the legal deadlines) is still alive, but its adoption and endorsement rates remain to be seen (no holiday season miracles here probably).

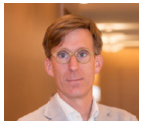
Those who started their AI journey now have a more definitive reference to benchmark progresses; all others have no excuses to postpone their work on the impact of the EU AI Act on their operations. There is no one-size-fits-all approach, but a responsible AI roadmap would typically entail three steps (and many iterations):



Sign up to our AI mailing list to receive our latest insights and invitations to events on this topical issue.



Authors



Charles Helleputte
Head of EU Data Privacy, Cybersecurity & Digital Assets, Brussels/Paris
T +32 2 627 1100
E charles.helleputte@squirepb.com

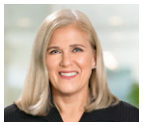
Claire Murphy
Associate, Madrid
T +34 91 520 0771
E claire.murphy@squirepb.com

Andrea Otaola
Associate, Brussels
T +33 2 627 1113
E andrea.otaola@squirepb.com

Contacts

David Elkins
Chair, Intellectual Property & Technology, Palo Alto
T +1 650 843 3378
E david.elkins@squirepb.com

Alan Friel
Chair, Data Privacy, Cybersecurity & Digital Assets, Los Angeles
T+1 213 689 6518
E alan.friel@squirepb.com



Julia Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Matthew Kirk
International Affairs Advisor
T +44 207 655 1389
E matthew.kirk@squirepb.com

Wolfgang Maschek
Partner, Brussels
T +322 627 11 04
E wolfgang.maschek@squirepb.com

David Naylor
Head of UK Data Privacy, Cybersecurity & Digital Assets, London
T +44 792 047 9619
E david.naylor@squirepb.com