The EU AI Act Enters Into Effect
What You Should Know and What Should You Do?

This snapshot provides a practical, "at a glance" summary of the EU AI Act, with a clear timeline of key dates and what you need to do, by when.

Fundamentals

What does it focus on?

- Through a **harmonized legal framework**, 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.
- Establishes **human-centered AI principles**.

Who does it apply to?

Broad territorial scope:
- Providers of AI systems that are put into service or placed on the market in the EU.
- Deployers of AI systems established in the EU.
- Providers or deployers of AI systems where the output from the system is used in the EU. The "Brussels effect" is popular (among the EU rulemakers).
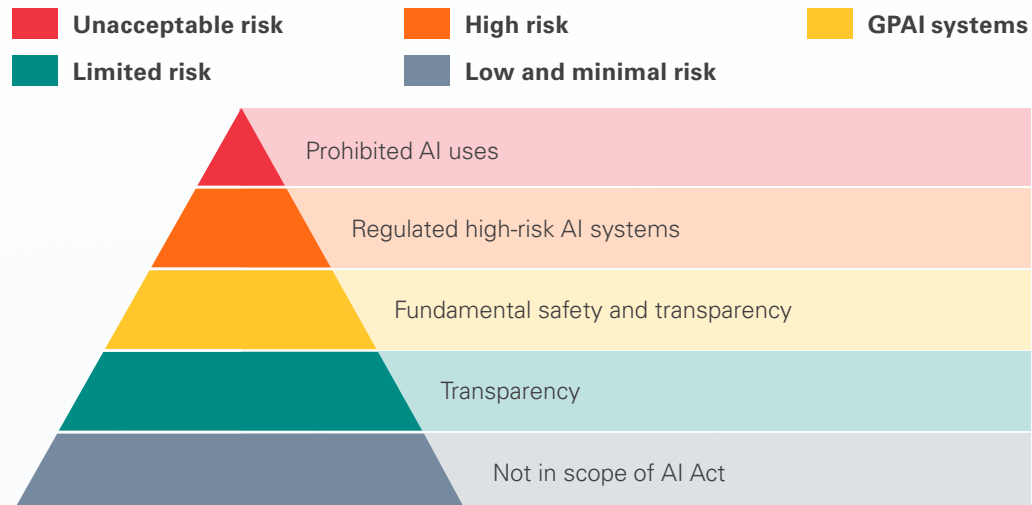
Different legal obligations and responsibilities for providers and deployers
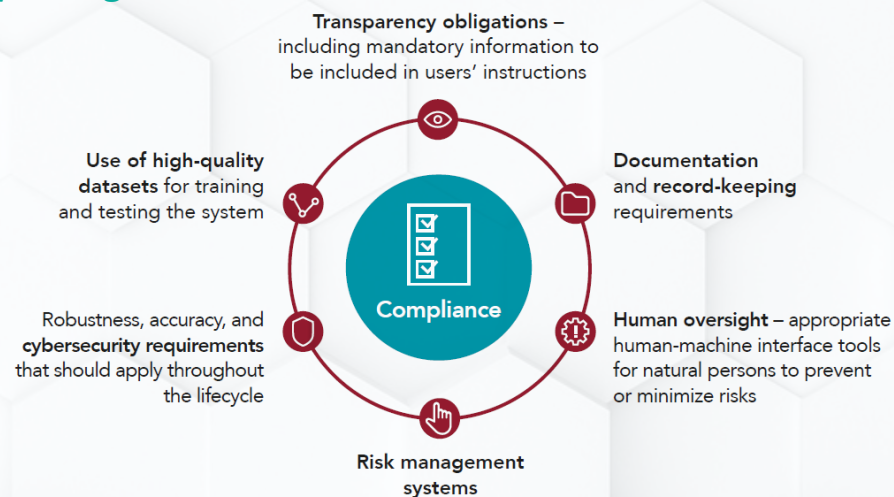
Scope

All AI systems (under the OECD definition), **unless** they are:
- Falling within the national security remit of member states (MS)
- Used for military or defense purposes
- Used for research and innovation
- Free and open-source software – unless they qualify as high-risk system or prohibited AI
- Used by international organizations and non-EU public authorities using AI in the context of law enforcement and judicial cooperation
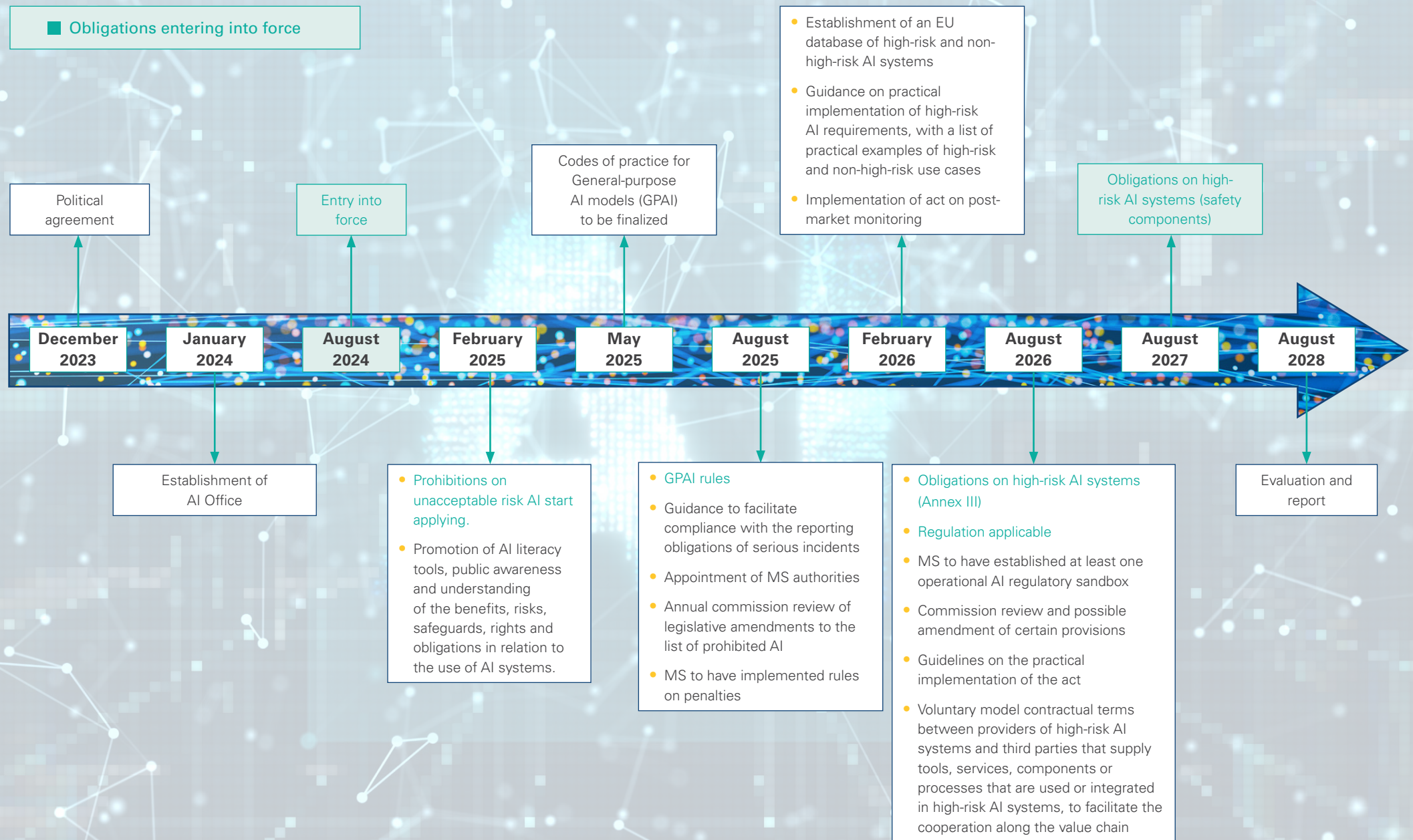- Used by individuals for purely personal nonprofessional activities

Key Considerations

- 🟥 **Unacceptable risk**
- 🟧 **High risk**
- 🟨 **GPAI systems**
- 🟩 **Limited risk**
- 🟦 **Low and minimal risk**

Prohibited AI uses

Regulated high-risk AI systems

Fundamental safety and transparency

Transparency

Not in scope of AI Act

Key Obligations

Transparency obligations – including mandatory information to be included in users' instructions

Use of high-quality datasets for training and testing the system

Documentation and **record-keeping** requirements

Compliance

Robustness, accuracy, and **cybersecurity requirements** that should apply throughout the lifecycle

Human oversight – appropriate human-machine interface tools for natural persons to prevent or minimize risks

Risk management systems

EU AI Act – Overarching Policy & Compliance Timeline

Political agreement — December 2023

Entry into force — August 2024

Codes of practice for General-purpose AI models (GPAI) to be finalized — May 2025

- Establishment of an EU database of high-risk and non-high-risk AI systems
- Guidance on practical implementation of high-risk AI requirements, with a list of practical examples of high-risk and non-high-risk use cases
- Implementation of act on post-market monitoring

(February 2026)

Obligations on high-risk AI systems (safety components) — August 2027

Timeline

December 2023 | January 2024 | August 2024 | February 2025 | May 2025 | August 2025 | February 2026 | August 2026 | August 2027 | August 2028

Establishment of AI Office — January 2024

February 2025:
- Prohibitions on unacceptable risk AI start applying.
- Promotion of AI literacy tools, public awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems.

August 2025:
- GPAI rules
- Guidance to facilitate compliance with the reporting obligations of serious incidents
- Appointment of MS authorities
- Annual commission review of legislative amendments to the list of prohibited AI
- MS to have implemented rules on penalties

August 2026:
- Obligations on high-risk AI systems (Annex III)
- Regulation applicable
- MS to have established at least one operational AI regulatory sandbox
- Commission review and possible amendment of certain provisions
- Guidelines on the practical implementation of the act
- Voluntary model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems, to facilitate the cooperation along the value chain

Evaluation and report — August 2028

EU AI Act – Focus on Prohibited AI Systems Timeline

| December 2023 | January 2024 | August 2024 | February 2025 | May 2025 | August 2025 | February 2026 | August 2026 | August 2027 | August 2028 |

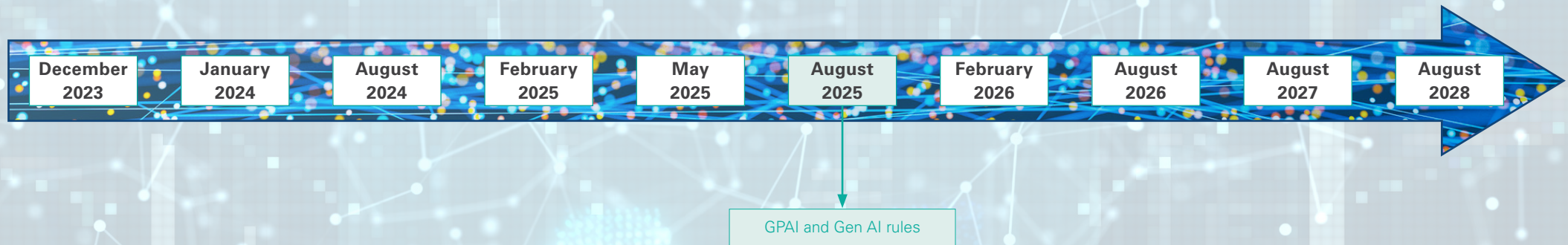**Prohibitions on unacceptable risk AI**

To Do – **Check if your organization develops or uses any of the following prohibited AI practices:**

- **Use of subliminal, purposefully manipulative or deceptive techniques**

- **Exploiting vulnerabilities** of persons due to age, disability or a specific social or economic situation

- **Biometric categorization** to deduce or infer a person's race, political opinion, trade union membership, religious or philosophical belief, sex life or sexual orientation

- **Evaluation or classification of persons** over a period of time based on their social behavior or known, inferred or predicted personality characteristics leading to detrimental or unfavorable treatment that is unrelated to the data context, or unjustified or disproportionate

- **Real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement**

- **Profiling or assessment of personality traits or characteristics of persons to asses or predict the risk of them committing criminal offences**, except for assisting human risk assessments of specific persons involved in a crime

- **Creation or expansion of a facial recognition database** based on untargeted scraping on the internet or CCTV footage

- **Inferring emotions of persons in workplace areas or in education institutions** except where intended for medical or safety reasons
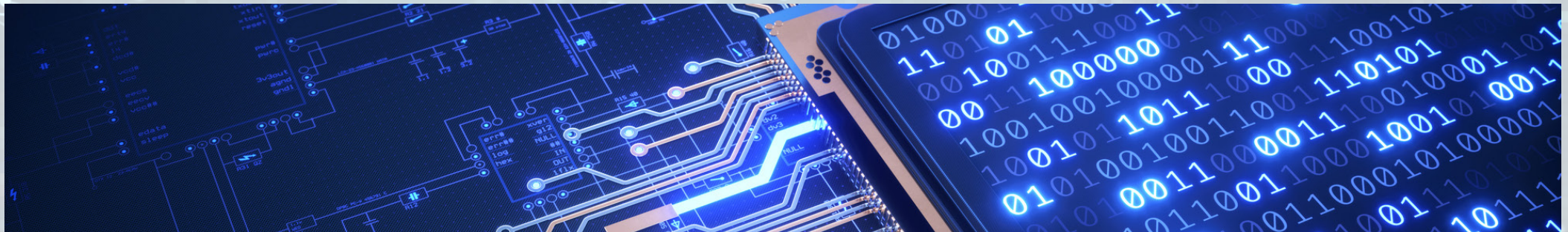
EU AI Act – GPAI Obligations

| December 2023 | January 2024 | August 2024 | February 2025 | May 2025 | August 2025 | February 2026 | August 2026 | August 2027 | August 2028 |

GPAI and Gen AI rules

To Do – **If you are a GPAI provider, you should:**

- Maintain and update detailed technical documentation of the model for the attention of the market surveillance authorities.
- Maintain and update less detailed documentation of the model for the attention of the users of the GPAI.
- If you are located outside the EU, you must appoint a representative in the EU.
- Introduce internal rules to comply with EU copyright law.
- Publicly summarize the content you have used to train your models.

To Do – **If you are a Gen AI provider, you should:**

Ensure, if your AI system generates synthetic audio, image, video or text content, that:

- The outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.
- Your AI system is effective, interoperable, robust and reliable, as far as this is technically feasible.

To Do – **If you are a Gen AI deployer, you should:**

- Disclose that the image, audio or video content constituting deepfake content has been artificially generated or manipulated.
- Disclose that the text published with the purpose of informing the public on matters of public interest has been artificially generated or manipulated.

EU AI Act – High-risk AI Systems

December 2023	January 2024	August 2024	February 2025	May 2025	August 2025	February 2026	August 2026	August 2027	August 2028

Obligations on high-risk AI systems (Annex III) → August 2026

Obligations on high-risk AI systems (safety components) → August 2027
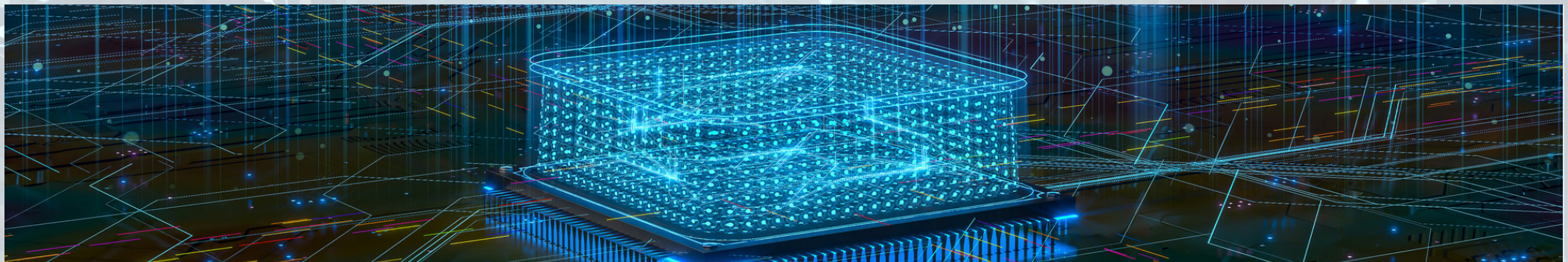
Key considerations:

- **Two broad categories** of high-risk AI systems: (1) those listed in Annex III and (2) those that are products, or safety components of products, regulated by specific EU product safety laws.

- **Different entry into force dates**.

- **All high-risk AI will have to be registered in the public EU database**.

To Do – Check if your organization develops or uses any of the following:

Annex III: High-risk AI Systems

- **Biometrics** – Remote biometric identification, biometric categorization and emotion recognition systems

- **Critical infrastructure** – Safety components for critical infrastructure operations (road traffic, water, gas, etc.)

- **Education and vocational training** – Determining access or admissions, evaluating learning outcomes, and monitoring prohibited behavior

- **Employment and management of workers** – Recruitment, hiring and job ads; promotion, termination and salary; task allocation and performance

- **Essential services and benefits** – Eligibility for public benefits, life and health insurance pricing, emergency services response and creditworthiness assessments

- **Law enforcement AI usage** – Victim risk assessment prediction, polygraph tests and evaluating reliability of evidence

- **Migration, asylum and border control** – Asylum and visa applications, identifying individuals, assessing security risks and polygraph tests

- **Judicial and democratic processes** – Researching and interpreting facts, applying the law, influencing outcome of elections and referendums

---

To Do – Check if you organization develops or uses safety components or products covered by the following EU secondary laws:

Products or Product Safety Components

- Machinery
- Toys and toy safety
- Medical devices, in vitro devices (IVD)
- Vehicles
- Aviation
- Marine equipment
- Rail system

- Appliances burning gaseous fuel
- Personal protective equipment
- Cableway installations
- Pressure equipment
- Personal watercraft
- Lifts
- Radio equipment

EU AI Act – High-risk AI Systems

December 2023	January 2024	August 2024	February 2025	May 2025	August 2025	February 2026	August 2026	August 2027	August 2028

Obligations on high-risk AI systems (Annex III) (August 2026)

Obligations on high-risk AI systems (safety components) (August 2027)

Key considerations:

High-risk systems must comply with key requirements that include detailed rules on:

- Data quality and governance
- Transparency
- Accuracy, robustness and cybersecurity
- Human oversight
- Risk and quality-management systems
- Technical documentation
- Record-keeping

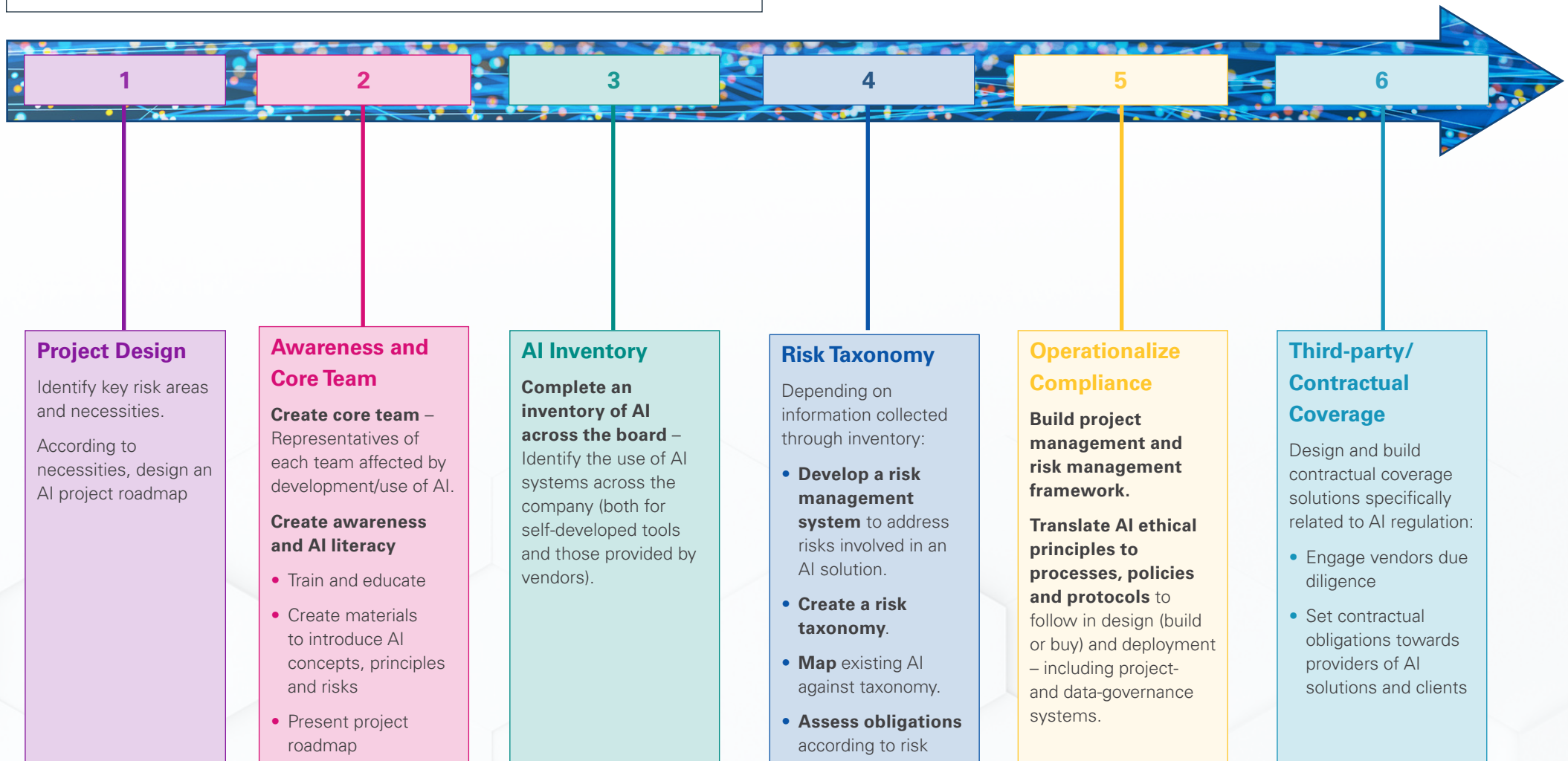**To Do** – **To demonstrate compliance with these requirements, providers must:**

- Have **appropriate documentation** of their compliance
- Have a quality-management system
- **Keep the logs generated** by their AI system in use (if they have them)
- **Register the AI system in an EU database** (except those used in the context of critical infrastructure)
- Have a **conformity assessment** carried out by an appropriate third party
- **Mark the AI system with a conformity mark** ("CE") and their contact details
- **Notify the supervisory authorities** if the AI system poses a risk to the health, safety or fundamental rights of persons affected, or if a serious incident occurs

To Do – **Deployers of high-risk systems must:**

- Carry out a **Fundamental Rights Impact Assessment**, if applicable
- Comply with provider instructions using technical and organizational measures
- **Assign human oversight** to competent, trained and supported personnel
- **Ensure relevant and representative input data** for the AI system's intended purpose
- Fulfil monitoring, **record-keeping and incident-reporting obligations** to providers and competent authorities
- Ensure that, when a high-risk AI system is used in the workplace, the employees concerned are informed
- Ensure that affected persons are informed when a high-risk AI system is used for decisions concerning them

EU AI Act – How To Prepare: Design and Implementation of a Responsible AI Roadmap

To Do – Develop a governance and compliance program based on these six pillars

| 1 | 2 | 3 | 4 | 5 | 6 |

Project Design
Identify key risk areas and necessities.

According to necessities, design an AI project roadmap

Awareness and Core Team
Create core team – Representatives of each team affected by development/use of AI.

Create awareness and AI literacy
- Train and educate
- Create materials to introduce AI concepts, principles and risks
- Present project roadmap

AI Inventory
Complete an inventory of AI across the board – Identify the use of AI systems across the company (both for self-developed tools and those provided by vendors).

Risk Taxonomy
Depending on information collected through inventory:

- **Develop a risk management system** to address risks involved in an AI solution.
- **Create a risk taxonomy**.
- **Map** existing AI against taxonomy.
- **Assess obligations** according to risk

Operationalize Compliance
Build project management and risk management framework.

Translate AI ethical principles to processes, policies and protocols to follow in design (build or buy) and deployment – including project- and data-governance systems.

Third-party/ Contractual Coverage
Design and build contractual coverage solutions specifically related to AI regulation:

- Engage vendors due diligence
- Set contractual obligations towards providers of AI solutions and clients

EU AI Act – Governance and Enforcement

Key considerations:

- Many different authorities involved in different stages: enforcement, implementation, interpretation and application

- At least two regulators in each MS as well as the AI Office and AI Board at the EU level

- Different obligations apply at different times

Member State Regulators:

Market Surveillance Authority

- To carry out procedures for conformity assessments of high-risk AI systems

- To coordinate and cooperate activities with other authorities

Notifying Authority

- To assess, designate, notify and monitor conformity assessment bodies

- To investigate and take necessary actions

- To coordinate and cooperate activities with other author

Notified bodies

- Independent bodies accredited at the MS level

- To exercise powers independently and impartially

- To monitor and investigate AI system's compliance with the Act

- To adopt measures against non compliant AI systems

- To handle companies' and individuals' complaints concerning infringements

- To collect serious incident reports from high-risk AI system providers and adopt necessary measures

Penalties and fines:

- Up to **7% of global annual turnover or €35 million** (whichever is higher) – noncompliance with prohibition of AI practices

- Up to **3% of global annual turnover or €15 million** (whichever is higher) – obligations for providers and deployers of high-risk AI systems

- Up to **1% of global annual turnover or €7 million** (whichever is higher) – supply of incorrect or misleading information to regulators

Each EU MS to establish a penalty system within these parameters.

Lower, more proportionate fines for SMEs and startups.

European Regulators:

AI Office

- Part of the EC Directorate-General for Communications Networks, Content and Technology

- Exercise powers independently and impartially Personnel having expertise in fields such as information technologies, AI and law, as well as fundamental rights

- To harmonize implementation across the EU

- To assess and monitor GPAIs and aid investigations into rule violations

- To provide administrative support to oher bodies

- To cooperate with other DG and services internationally

- To enforce rules and develop codes of practice and guidance on GPAI

- To coordinate enforcement at European level

AI Board

- One representative per MS

- To promote harmonized interpretation of the act

- To issue opinions and guidance

- Supported by **Advisory Forum** and **Scientific Panel**

Responsible AI Roadmap

Our firm has deep experience assisting clients in navigating the multifaceted issues around AI. We have a wealth of resources to help you understand your risk profile and compliance requirements, develop safety protocols and build a robust AI governance program. If you would like help with charting a responsible AI roadmap for your organization, please contact us for more information.

About Us

We are a multidisciplinary global team of leading legal, policy and technology experts dedicated to supporting our clients in connection with the deployment and acquisition of AI systems, services and businesses and the protection of your most valuable IP assets.

Whether you are a trailblazing AI business at the cutting edge of AI service provision or a global corporate embedding or deploying AI, we can support you through the challenges that come with operating in a market that is being rapidly shaped by competitive forces as well as a highly complex regulatory environment.

Our experience working with companies, policymakers and regulators worldwide uniquely enables us to provide first rate advice on the complex commercial, contractual, data privacy, intellectual property, regulatory, policy and other legal issues arising from the adoption and use of AI. Our experts are recognized leaders in their field, bringing an unrivaled depth of experience and insight and the ability to add significant value to your transactions, regulatory and policy projects and disputes.

We help global businesses across a multitude of sectors on AI-related issues, including:

- Global AI regulatory strategy and compliance
- The rollout and commercialisation of AI solutions and services
- M&A and fundraising for AI-enabled companies
- The design and rollout of global AI governance models
- The acquisition and use of training data and foundational models
- AI and intellectual property ownership and infringement issues
- The regulation of profiling and automated decision-making

- Contracting for AI contracting solutions and services
- Employment issues including managing works council co-determination processes for their AI related rights
- Export control licensing requirements for AI products or solutions
- Assessing risk in clearing transactions involving M&A, JVs and other AI business deals
- Corporate finance (including VC) and M&A involving AI companies

Visit our **AI Law and Policy Hub** for the latest insights on the rapidly evolving AI legal and policy developments from around the world.
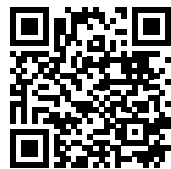
Keep informed with our latest insights and events.
Subscribe to our AI mailing list.

Contacts

Annette Demmel
Partner, Berlin
T +49 30 72616 8000
E annette.demmel@squirepb.com

Bartolomé Martín
Partner, Madrid
T +34 91 426 4867
E bartolome.martin@squirepb.com

Mareike Lucht
Senior Associate, Berlin
T +49 30 72 616 8131
E mareike.lucht@squirepb.com

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

GDR

Ranked "Elite" by Global Data Review

Recognised in

The Legal 500 US and *UK*, *Chambers USA* and *UK*, *Chambers Europe*, *Global Data Review* and *World Trademark Review's WTR 1000*

Mergermarket

Ranked 1st for Technology M&A Transactions during 2024