EU AI ACT Primer

- Goals of the EU AI Act
- EU AI ACT TIMELINE
- **AI ACT and GDPR**
- **AI ACT RISK BASED CATAGORIZATIONS**
- **Key areas to ensure AI compliance with the EU AI Act**

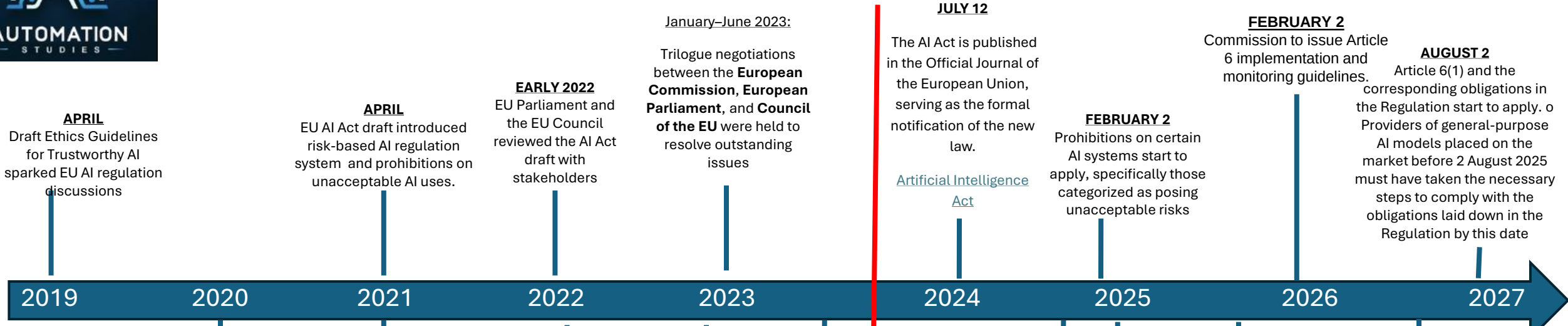
Goals of the EU AI Act

- Promote trust in AI technologies.
- Ensure safety, transparency, and accountability.
- Prevent harmful practices while fostering innovation within ethical boundaries.

The Act is a pioneering regulatory framework, likely influencing global AI governance standards.

The **EU AI Act** aligns closely with the principles and structure of the **General Data Protection Regulation (GDPR / See Slide 4)**, building on its emphasis on transparency,

EU AI ACT TIMELINE



APRIL
Draft Ethics Guidelines for Trustworthy AI sparked EU AI regulation discussions

FEBRUARY
EU proposed AI regulatory framework in "White Paper on Artificial Intelligence

APRIL
EU AI Act draft introduced risk-based AI regulation system and prohibitions on unacceptable AI uses.

MID 2021
Public consultations and stakeholder engagements were conducted to refine the proposal

EARLY 2022
EU Parliament and the EU Council reviewed the AI Act draft with stakeholders

DECEMBER
EU Council agreed on AI Act's structure

January–June 2023:

Trilogue negotiations between the **European Commission**, **European Parliament**, and **Council of the EU** were held to resolve outstanding issues

JUNE 14
EU Parliament approved stricter AI Act for general-purpose AI.

OCTOBER
EU institutions finalized AI Act text.

JULY 12

The AI Act is published in the Official Journal of the European Union, serving as the formal notification of the new law.

Artificial Intelligence Act

AUGUST 1

The AI Act enters into force. At this stage, none of the Act's requirements apply; they will begin to apply gradually over time.

Artificial Intelligence Act

FEBRUARY 2
Prohibitions on certain AI systems start to apply, specifically those categorized as posing unacceptable risks

MAY 2
The European Commission is expected to have codes of practice ready by this date.

NOVEMBER 2
Member States must identify and publicly list the authorities or bodies responsible for fundamental rights protection and notify the Commission and other Member States

FEBRUARY 2
Commission to issue Article 6 implementation and monitoring guidelines.

AUGUST 2

Several provisions come into effect:

Rules on AI models, governance, and penalties.

Pre-2027 AI models must comply by August 2027

Member States must designate authorities and share details publicly.

States must set and enforce penalty rules, notifying the Commission

AUGUST 2
Article 6(1) and the corresponding obligations in the Regulation start to apply. o Providers of general-purpose AI models placed on the market before 2 August 2025 must have taken the necessary steps to comply with the obligations laid down in the Regulation by this date

AUGUST 2
AI Act applies (except Article 6(1)); high-risk systems with major changes must comply; states must establish AI sandboxes.

Key Changes During the Legislative Process

- Increased focus on **foundation models** and **generative AI**, mandating transparency and data governance.
- Prohibition of **real-time biometric surveillance** with narrow exceptions for law enforcement.

Strengthened rules on transparency for AI-generated content.
By the end of 2023, the finalized text was prepared for formal adoption, paving the way for its entry into force in 2024

AI ACT and GDPR

Shared Goals: Protecting Individuals and Promoting Accountability

Both regulations aim to safeguard individuals against misuse of technology:

- **GDPR** focuses on protecting personal data and privacy.
- **EU AI Act** focuses on mitigating risks from AI, including safety, fairness, and ethical concerns.

AI Act's Impact on Data Protection Obligations

AI systems often rely on large datasets, which may include personal data. GDPR applies to these systems in several ways:

- **Data Minimization**: GDPR requires processing only necessary data. This principle applies to training AI systems to avoid excessive data collection.
- **Lawful Basis for Processing**: Organizations using personal data for AI systems must have a legitimate legal basis under GDPR (e.g., consent, legitimate interest).
- **Right to Explanation**:
  - GDPR provides individuals with the right to understand decisions made by automated systems.
  - The AI Act reinforces this by mandating transparency for high-risk AI and requiring human oversight.

Penalties

The penalties under both regulations are significant:

- **GDPR**: Fines up to **€20 million** or **4% of global revenue** for non-compliance.

AI Act: Fines up to **€30 million** or **6% of global revenue** for violations

Overlapping Requirements

Transparency:

GDPR: Requires clear information about data processing.

AI Act: Mandates transparency about how AI systems function, particularly for high-risk and generative AI systems

Accountability

GDPR: Organizations must appoint a Data Protection Officer (DPO) and demonstrate compliance.

AI Act: High-risk AI systems require robust documentation, risk management systems, and human oversight.

Data Quality

GDPR: Emphasizes accurate, up-to-date data.

AI Act: Requires high-quality, unbiased datasets for training AI systems to prevent discrimination.

Enforcement and Governance

Both regulations rely on multi-tiered enforcement:

- **GDPR**: Enforced by national Data Protection Authorities (DPAs) with cross-border cases managed by the European Data Protection Board (EDPB).

AI Act: Establishes national supervisory authorities and a European Artificial Intelligence Board, echoing the GDPR structure

Synergy and Overlap

- Organizations subject to GDPR will likely already have systems for data governance that can help meet AI Act compliance requirements.
- For AI systems that process personal data, compliance with GDPR is a prerequisite for compliance with the AI Act.

Wrap-Up

The EU AI Act complements GDPR by extending protections beyond data privacy to the broader implications of AI technologies. Organizations operating in the EU must align their AI practices with GDPR and AI Act requirements to ensure compliance, emphasizing transparency, fairness, and accountability.

The **EU Artificial Intelligence (AI) Act** establishes a phased implementation schedule leading up to its full enforcement in 2026. Below is a detailed timeline of key dates and corresponding obligations:

AI ACT RISK BASED CATAGORIZATIONS

The FOUR AI RISK CLASSIFICATION LEVELS

- **Unacceptable Risk**: Prohibited uses, including social scoring by governments, subliminal manipulation, and exploitation of vulnerable individuals (e.g., children).
- **High Risk**: AI systems used in critical areas like healthcare, law enforcement, education, and employment. These systems must comply with stringent regulations, including transparency, accountability, and human oversight.
- **Limited Risk**: AI systems requiring transparency obligations, such as chatbots or generative AI tools. Users must be informed when interacting with AI.
- **Minimal Risk**: Most AI systems, such as spam filters or recommendation engines with no specific requirements.

Prohibited Practices

- AI that exploits vulnerabilities of specific groups (e.g., children, elderly).
- Real-time biometric surveillance in public spaces, with limited exceptions for law enforcement.

AI systems that manipulate behavior to harm individuals or society

Requirements for High-Risk AI Systems

- **Data Governance**: Ensure high-quality datasets to prevent discrimination or bias.
- **Transparency**: Provide clear documentation about how the system works.
- **Human Oversight**: Systems must allow for intervention or override by human operators.
- **Robustness and Security**: AI systems must be resilient and mitigate risks.

Generative AI and Foundation Models

Developers of generative AI (e.g., large language models) must:

- Prevent the generation of illegal content.
- Disclose that content is AI-generated.
- Document training data sources and ensure compliance with intellectual property laws.

Regulatory Oversight

- Establishes a European Artificial Intelligence Board to oversee implementation.
- National authorities in each member state will enforce the Act.

Penalties

Non-compliance can result in fines up to **€30 million** or **6% of global annual revenue**, whichever is higher.

Key areas to ensure AI compliance with the EU AI Act

Risk Categorization:

Identify your AI system's risk level:

- **Unacceptable** (banned, e.g., manipulative AI).
- **High** (e.g., healthcare, law enforcement, requires strict controls).
- **Limited** (requires transparency, e.g., chatbots).
- **Minimal** (low-risk, no special rules. e.g., spam filters).

High Risk AI

•Ensure high-quality, unbiased data.
•Be transparent about how the system works.
•Guarantee reliability, accuracy, and security.
•Set processes to manage risks and allow human intervention.

Generative AI

•Label AI-generated content.
•Document training data sources.
•Prevent harmful outputs.

Transparency

- Inform users they're interacting with AI.
- Explain how the system works in simple terms.

Governance:

- Keep detailed records: (purpose, design, data, monitoring
- Be audit –ready and update documentation regularly

Data Protection (GDPR):

Ensure privacy, minimize data use, ands respect user rights (see more in the GDPR Shared Responsibilities)

Ethics and Impact

- Follow fairness, accountability, and non-discrimination standards
- Consider social effects and risks

Penalties

Noncompliance fines of up to 30M eros or 6% of global revenue

Perform internal checks to stay compliant

Quick Compliance Checklist:

•Have you assessed your system's risk category?
•Are your transparency and data governance practices sufficient?
•Is your system secure and regularly monitored?
•Can you handle audits or inspections confidently?

Regulatory Sandboxes:

•Use supervised testing environments to refine your system.

Cross-Border Operations:

•Ensure compliance across all EU countries where your AI operates.