Tech Me Up!

AI webinar series

by TaylorWessing

Session #5

The EU AI Act is live – Best practices for its implementation

Dr. Paul Voigt, Lic. en Derecho, CIPP/E, Séverine Bouvy, CIPP/E, Dr. Heather Simmons, AIGP, and Matthew Gratton, CIPP/US I July 2024

Introduction

An introduction to the AI Act

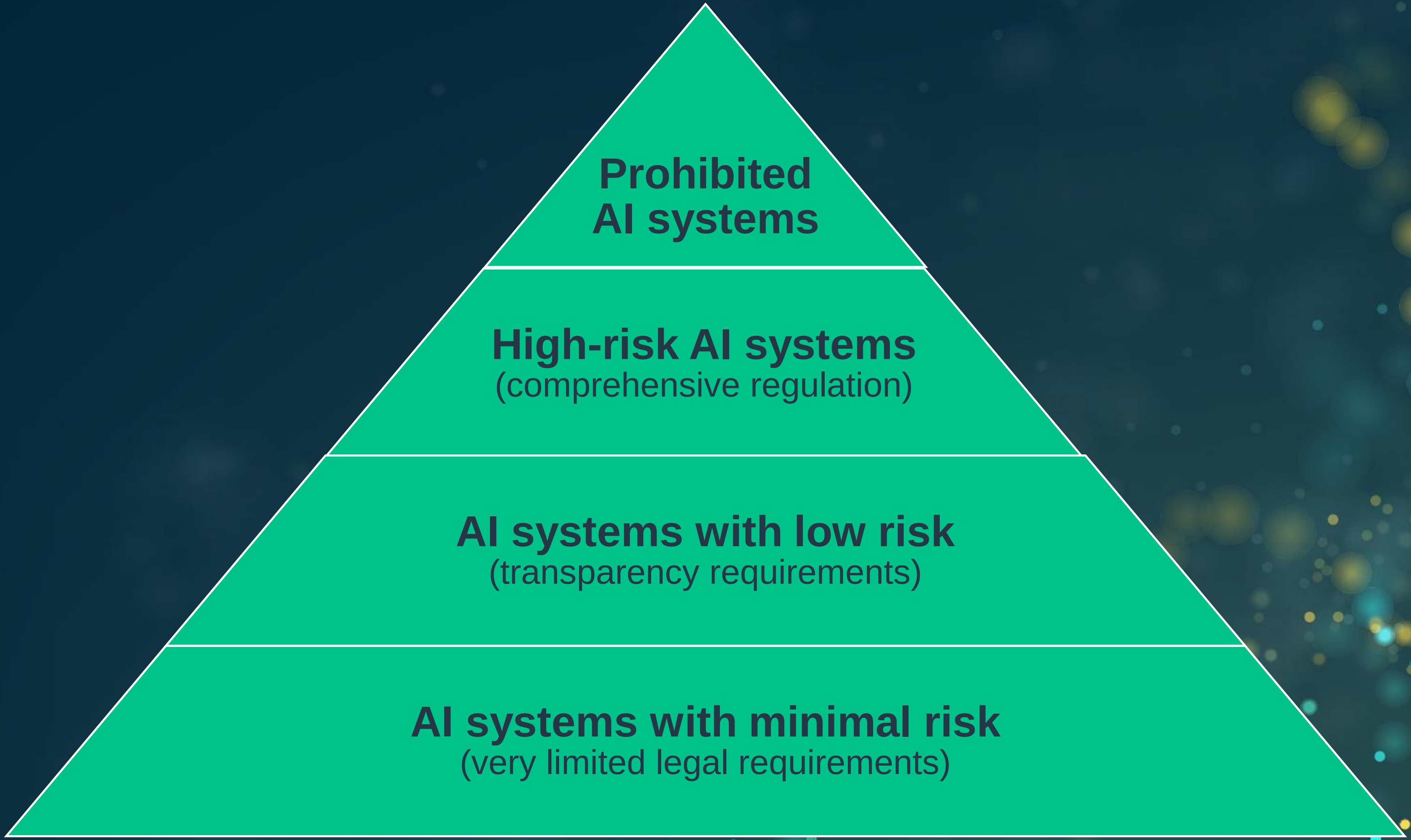
What legal requirements are in place already?

- Copyright
- Liability
- Data protection
- Contracts
- Employment law, …

The EU AI Act's compliance requirements

- EU AI Act – territorial application
  - Even non-EU companies heavily regulated
- Stakeholders involved, e.g.
  - Providers/developers of AI systems
  - Providers/developers of general purpose AI models
  - Importers of AI systems developed outside the EU
  - Deployers/users
  - Distributors of AI systems (w/out being importer)

Risk-based approach of the EU AI Act



Prohibited AI systems

High-risk AI systems
(comprehensive regulation)

AI systems with low risk
(transparency requirements)

AI systems with minimal risk
(very limited legal requirements)

Examples for prohibited, high-risk and low risk AI systems

Tech Me Up!
AI webinar series
by TaylorWessing

Prohibited AI systems:

- Social Scoring
- Predictive policing
- Facial recognition databases by scraping
- Emotion recognition (in certain areas)
- Exploitation of vulnerabilities
- …

Low risk AI systems → transparency requirements:

- Deep fake systems
- Interaction with AI systems
- Watermarking of AI generated content

High-risk AI systems (excerpt):

- Recruitment
- Promotion and termination of work relationships, to allocation of tasks based on individual behavior or personal traits…
- Evaluating creditworthiness
- Pricing in the case of life and health insurance
- …

Requirements for providers of high-risk AI systems

- Implement a risk management system
- Ensure that quality criteria are met / data governance
- Technical documentation
- Record-keeping / logs
- Transparency
- Human oversight
- Accuracy, robustness and cybersecurity
- Conformity assessments

- Quality management system
- Documentation retention obligation
- Log retention obligation
- Corrective actions and duty of information
- Cooperation with competent authorities
- Appointment of authorized representative for providers outside the EU
- Registration in the EU database
- …

Requirements for deployers of high-risk AI systems

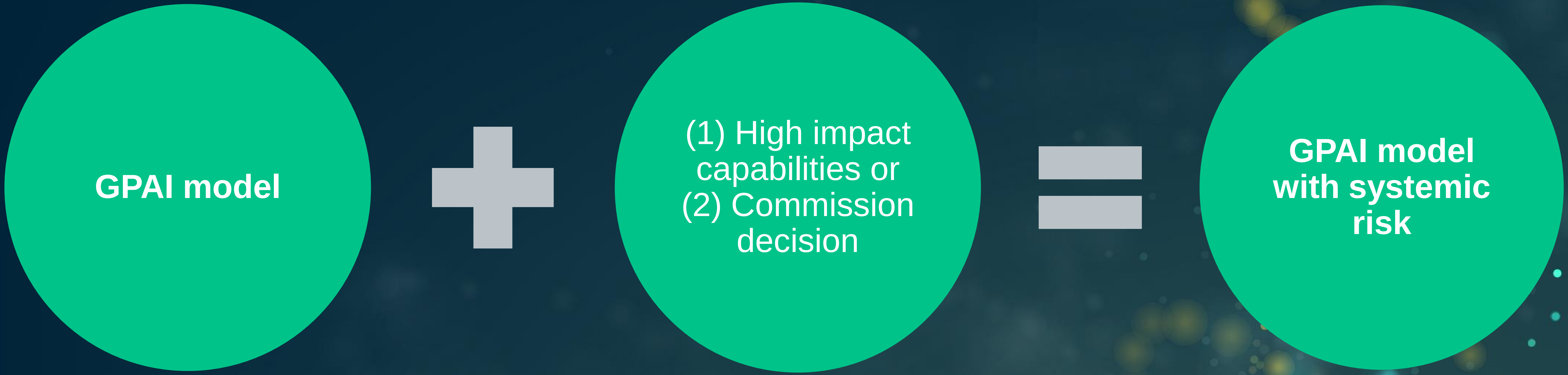
- Use the system (and monitor it) in accordance with the instructions
- Organize own resources and activities for the purpose of implementing human oversight measures
- Ensure that input data is relevant and representative in view of the intended purpose of the high–risk AI system
- Keep the logs generated by the high-risk AI system
- Cyber Security / TOMs
- Fundamental right impact assessments (limited scope of application)
- Transparency
- Notification obligations…

Generative AI/GPAI

Definition “General purpose AI model“ (Art. 3 (63))

“means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.”

GPAI model with systemic risk



GPAI model

+

(1) High impact capabilities or (2) Commission decision

=

GPAI model with systemic risk

Requirements for providers of GPAI models

Tech Me Up!
AI webinar series
by TaylorWessing

Requirements for GPAI model providers

- Extensive technical documentation and intelligible instructions
- Establishment of a policy to respect copyright law
- Publishing of a summary about content used for training, according to Commission template
- Partial exception for open source GPAI models

Additional requirements for Generative AI providers

- Evaluation of the model in accordance with standardized protocols and tools
- Assessment and mitigation of possible systemic risks from the development, placing on the market, or use of the model
- Documentation and notification of serious incidents and corrective measures
- Establishment of adequate cybersecurity

Fines under the EU AI Act

Art. 99 para. 3

Fines of up to EUR **35,000,000** or up to **7%** of annual worldwide turnover

Violation of

- **Art. 5**
  Placing on the market, putting into service or use of a prohibited AI system

Art. 99 para. 4

Fines up to EUR **15,000,000** or up to **3%** of the worldwide annual turnover

Violatio of

All other obligations, e.g.:

- **Art. 9:** Risk management system
- **Art. 11:** Technical documentation
- **Art. 12:** Record-keeping
- **Art. 14:** Human oversight
- **Art. 15:** Accuracy, robustness and cybersecurity
- **Art. 17:** Quality management system
- **Art. 18, 19:** Retention obligations
- **Art. 20:** Corrective actions and duty of information
- **Art. 22, 23, 24, 26, 31, 33, 34**
  Obligations of representatives, importers, distributors, deployers, notified bodies
- **Art. 43:** Conformity assessment
- **Art. 50:** Transparency

Art. 101

Fines up to EUR **15,000,000** or up to **3%** of the worldwide annual turnover

Due to

Providers of GPAI models

- Infringing relevant provisions, i.e. **Art. 53/55**
- Not complying with **request for document or information** or supplying **incorrect or incomplete information**
- Not complying with a **measure requested by the Commission**
- Not granting **access** to the Commission

Art. 99 para. 5

Fines of up to EUR **7,500,000** or up to **1%** of annual worldwide turnover

Due to

Incorrect or incomplete information to authorities

Building an AI Governance Structure: Discussion Topics

Tech Me Up!
AI webinar series
by TaylorWessing

- Policy & Procedure Development
- Roles & Responsibilities
- Stakeholder Engagement
- Risk Management
- Data Governance
- Education & Awareness
- AI Lifecycle Management
- Evaluation & Continuous Improvement

Building an AI Governance Strategy

- Understand how your organization operates
- Use existing policies & frameworks (interoperability)
- Determine your sector's effect on the strategy
- Determine the legal & regulatory landscape
- Engage your stakeholders
- Obtain leadership support
- Determine your organization's risk tolerance
- Overall approach to AI Governance should be:
  - Risk based
  - Human centric

Responsible AI Principles

- Potential harms posed by AI systems are substantial and include:
  - Economic
  - Cultural
  - Reputational
  - Acceleration
  - Legal & Regulatory

- AI principles can serve to identify, assess and mitigate harms
- Operationalize your RAI principles through a comprehensive set of guidelines & practices
- Guidelines & practices will bridge high-level policies and real-world implementations

Example Guidelines, Frameworks & Blueprints

- These are numerous and some examples include:
  - OECD AI Principles
  - US White House OSTP Blueprint for an AI Bill of Rights
  - UNESCO Principles
  - Asilomar AI Principles
  - There are many more including corporate polices, government etc.
- There are principles that are common amongst these guidelines, frameworks & blueprints

Common Responsible AI Principles

- Fairness
- Transparency
- Accountability
- Privacy
- Safety & Security
- Human autonomy
- Non-Discrimination
- Ethical use
- Stakeholder participation

Build an RAI policy that fits your organization’s culture, sector and risk tolerance

Risk Management Framework

- Establish organizational risk strategy and tolerance
- Review existing risk management programs
- Types of risk
  - Privacy
  - Security & Operational
  - Regulatory & Legal
- Calculating risk
- Framework should be law, industry and tech agnostic
- Don’t forget to manage third-party risk

Risk Management Frameworks & Standards

- ISO 31000:2018 Risk Management
- ISO 42001:2023 Artificial Intelligence Management System
- NIST AI Risk Management Framework
- HUDERIA Framework for AI Systems
- IEEE 7000-21 Standard Model Process for Addressing Ethical Concerns during System Design
- ISO/IEC Guide 51 Safety Aspects

AI Governance Framework: Development

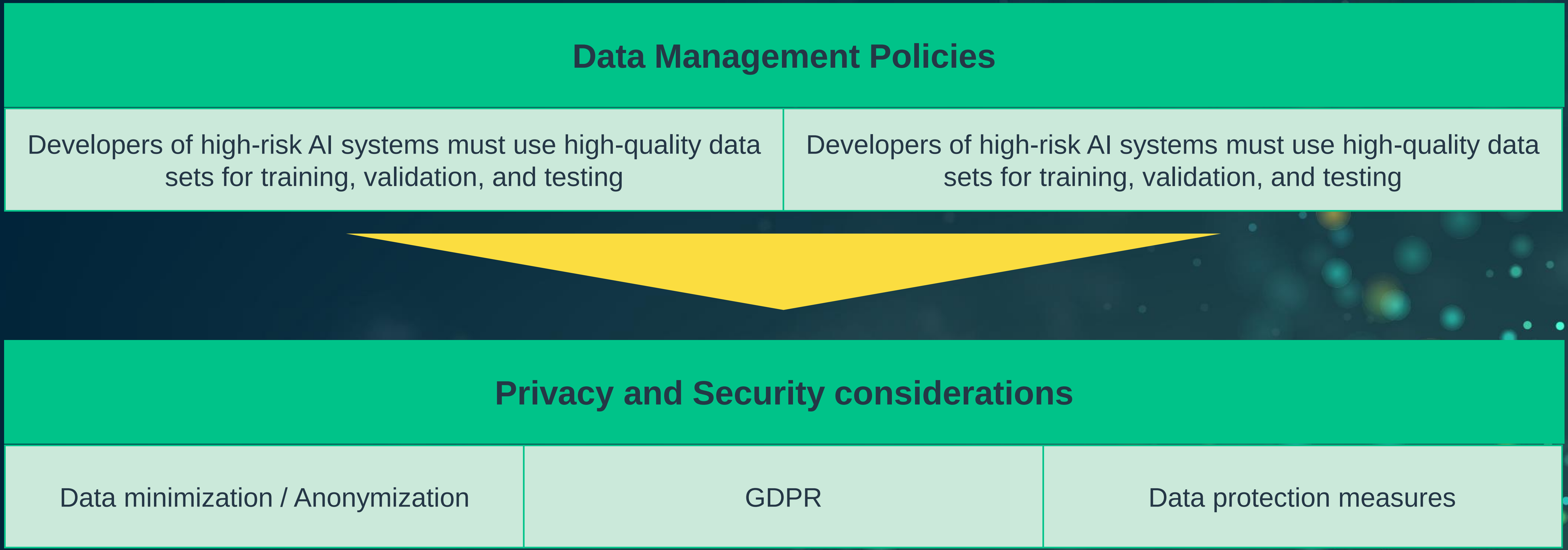
- Understand the key terms/definitions
- Identify key stakeholders in the organization
  - Privacy
  - Security
  - Legal
  - Accessibility
- Advocate for senior leadership support
- Leverage existing compliance structures
- Strongly defined roles & responsibilities

AI Inventory

Building vs. Buying: Considerations

- Capabilities
- Cost / Time
- Customization vs. Standardization
- Maintenance and Support
- Scalability
- Future-Proofing
- Risks

Data Governance



Data Management Policies

Developers of high-risk AI systems must use high-quality data sets for training, validation, and testing

Developers of high-risk AI systems must use high-quality data sets for training, validation, and testing

Privacy and Security considerations

Data minimization / Anonymization

GDPR

Data protection measures

Education and Awareness

Training Programs

- Technical training for AI practitioners
- Keeps AI practitioners up-to-date on changing/emerging regulations

Awareness Campaigns

- Builds trust and promotes transparency
- Opens dialog with diverse audience
- Builds a strong RAI community

AI Lifecycle Management

Planning
What is the business problem you're trying to solve for?

Design
Collection, storage, and retention of training data
Quantity and quality of the data

Development
AI model is built, trained, and evaluated

Implementation
Readiness assessments
Deploy into a production environment
Providers of high-risk systems will need a Conformity Assessment to be placed on the EU market

What is a Conformity Assessment

- Conformity assessments are required under the EU AI Act to ensure high-risk systems are safe, transparent, and trustworthy before they are placed on the EU market

- The process demonstrates that a high-risk system complies with the following requirements laid out in the Act:
- Risk management system
- Data governance
- Technical documentation
- Record keeping
- Transparency and provision of information
- Human oversight
- Accuracy, robustness, and cybersecurity

Tech Me Up! AI webinar series by TaylorWessing

Ongoing Evaluation and Continuous Monitoring

- Monitoring and Maintenance
- Feedback and Improvement
    - Stakeholder feedback mechanisms
    - Continuous improvement processes
    - Adaptation to technological advancements

- Incident Response Plan
    - Lean on existing incident response structures (Privacy, Security)
    - Response and resolution procedures
    - Post-incident analysis
    - Build an RAI Playbook

Summary

Determine AI principles and governance frameworks that fall within the organization’s culture, sector, and risk appetite

Ensure your approach is risk centric

Include a diverse group of stakeholders to evaluate AI goals, assess risk, and develop policies and procedures

Utilize established governance policies and frameworks (especially privacy and security)

Build a strong RAI community to foster a culture of responsible innovation

Can be daunting – start small and expand

Q&A

Speakers

Tech Me Up!
AI webinar series
by TaylorWessing

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Partner,
Taylor Wessing

Séverine Bouvy, CIPP/E
Counsel,
Taylor Wessing

Dr. Heather Simmons, AIGP
AI Services Leader,
Teleion

Matthew Gratton, CIPP/US
AI Services Leader,
Teleion

Tech Me Up!

AI webinar series

by TaylorWessing

taylorwessing.com

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at taylorwessing.com/en/legal/regulatory-information.