Overdose EU-Regulations

AI-Act, NIS-2, DORA & DSA

Dr. Alexander Deicke, MBA, LL.M. K11 Consulting GmbH, 12.03.2026

AI-generated content

Contents overview

K11, your experts for governance and AI regulation

Dr. Alexander Deicke, MBA, LL.M:

- Lawyer and manager
- Over 20 years of experience in commercial law and over 40 assignments as ad interim
- Author of AI Regulation Made Easy (DE/EN) and other publications
- External functions by K11 (information security, AI, data protection, ombudsman)
- Interlinked and structured management systems (book: simple governance – soon available from Kohlhammer)
- K11 Law Firm is the only one in Germany with an active ANÜ permission (lawyers via temporary employment)

Overview of the legal framework for the use of AI in companies

Module 1

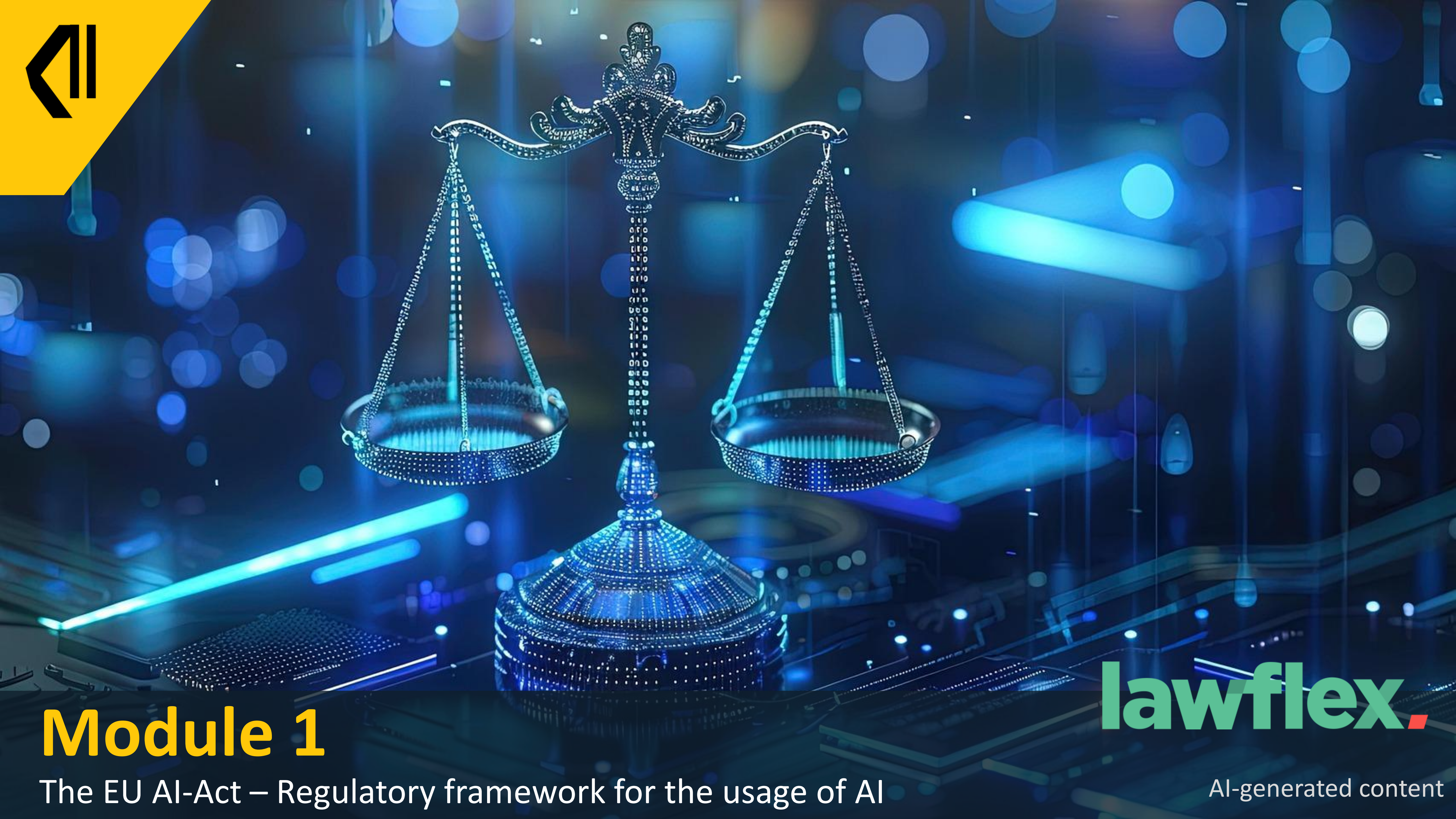
- AI-Act (AI Agents)
- Extraterritorial effect
- Risk classification
- Transparenz & Kennzeichnungspflicht

Module 2

- NIS-2 (ISO27001)
- DORA
- DSA, Data Act

Module 3

- AI policy & AI team
- AI repository
- AI officer



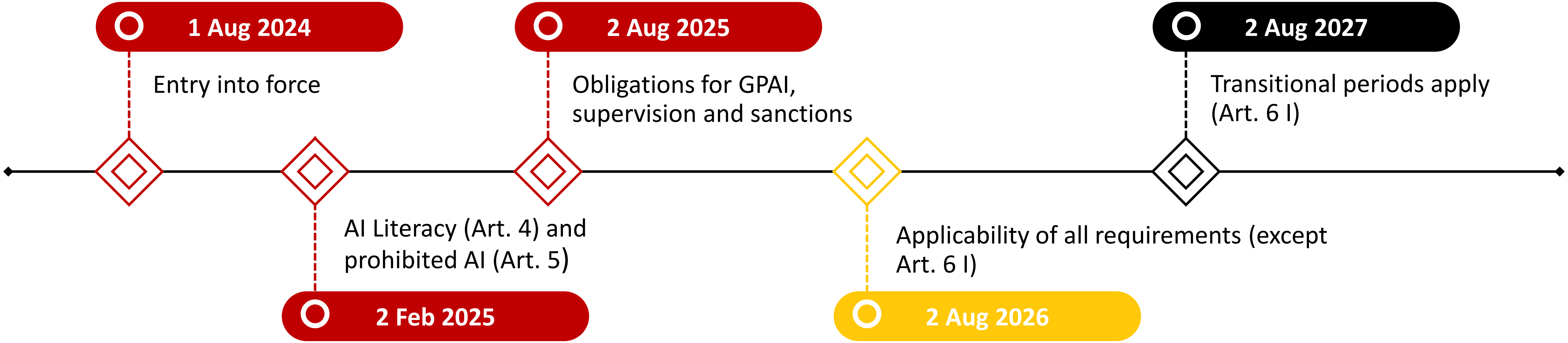
Module 1

The EU AI-Act – Regulatory framework for the usage of AI

AI-generated content

Implementation deadlines for the AI-Act

Companies should prepare for requirements at an early stage and establish governance structures



1 Aug 2024

Entry into force

2 Feb 2025

AI Literacy (Art. 4) and prohibited AI (Art. 5)

2 Aug 2025

Obligations for GPAI, supervision and sanctions

2 Aug 2026

Applicability of all requirements (except Art. 6 I)

2 Aug 2027

Transitional periods apply (Art. 6 I)

EU AI Act Deadline #1 [2. Februar 2025]

AI inventory

Inventory and risk classification of existing and planned AI systems

AI literacy

Awareness-raising and training for all those working with AI (Art. 4)

EU AI Act Deadline #2 [2. August 2026]

AI strategy

Define the target vision for AI deployment. Strategic roadmap and guiding principles

AI policy

Binding set of rules for the use and handling of AI. Responsibilities and approvals

AI governance

Internal control processes, committee formation, and integration into existing governance frameworks

Extraterritorial effect

Effectiveness of the EU AI-Act

European single market

AI systems or models are placed on the EU market

Compannies based in the EU

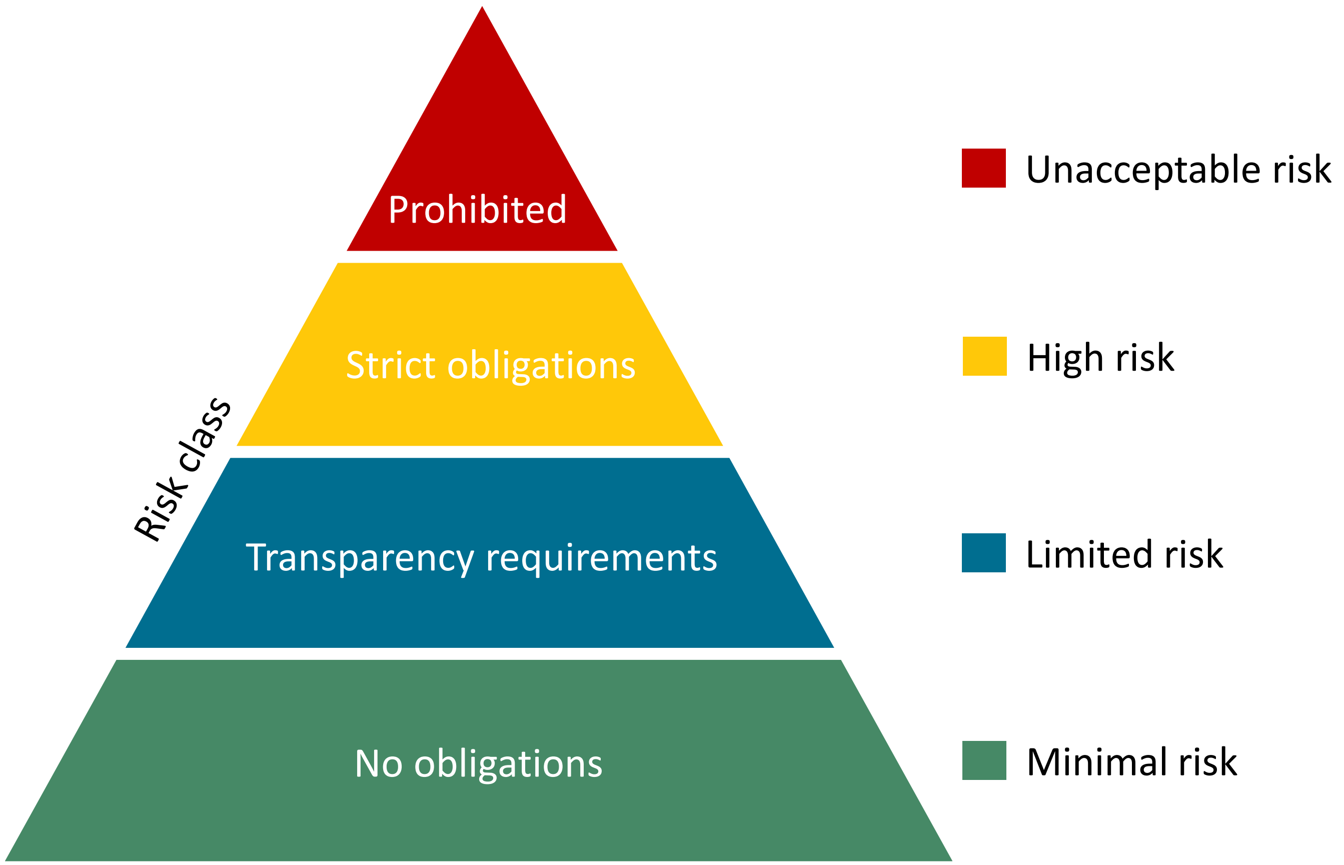
- Full application of the AI-Act
- Market surveillance and sanctions

International companies targeting the EU market

- Market access only with compliance with the AI Act
- EU representative for high-risk systems

Risk-based approach

The AI Act differentiates obligations according to risk potential



Prohibited

Strict obligations

Transparency requirements

No obligations

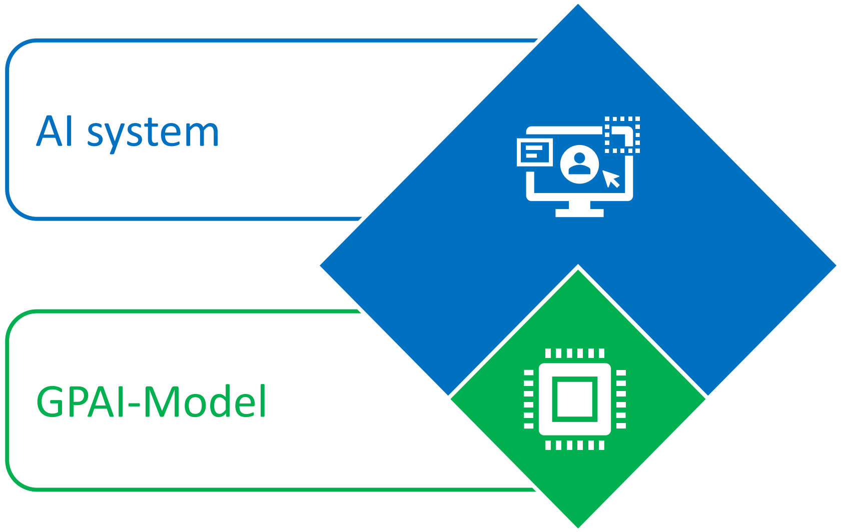
Risk class

🟥 Unacceptable risk

🟨 High risk

🟦 Limited risk

🟩 Minimal risk



AI system

GPAI-Model

What does the AI Act require of GPAI?

- Transparency regarding training data, risks, and model performance.
- Obligations also apply to providers who “reuse” GPAI models or integrate them

Requirements for AI with limited risk

Transparency and labeling in AI use according to Art. 50 AI Regulation

01 Transparency obligations

Users must be informed when they are interacting with an AI system. Example: A customer service chatbot must clearly inform users that they are interacting with an AI system and not a human employee.

02 Labeling requirement

If an AI system generates or edits images and it is not clearly recognizable to the persons involved that the images are AI-generated, this must be disclosed in an unambiguous manner. Example: When using AI-supported image generation systems (e.g., for marketing visuals, product images, or artistic representations), it must be clearly indicated that the image was generated or modified using an AI algorithm.

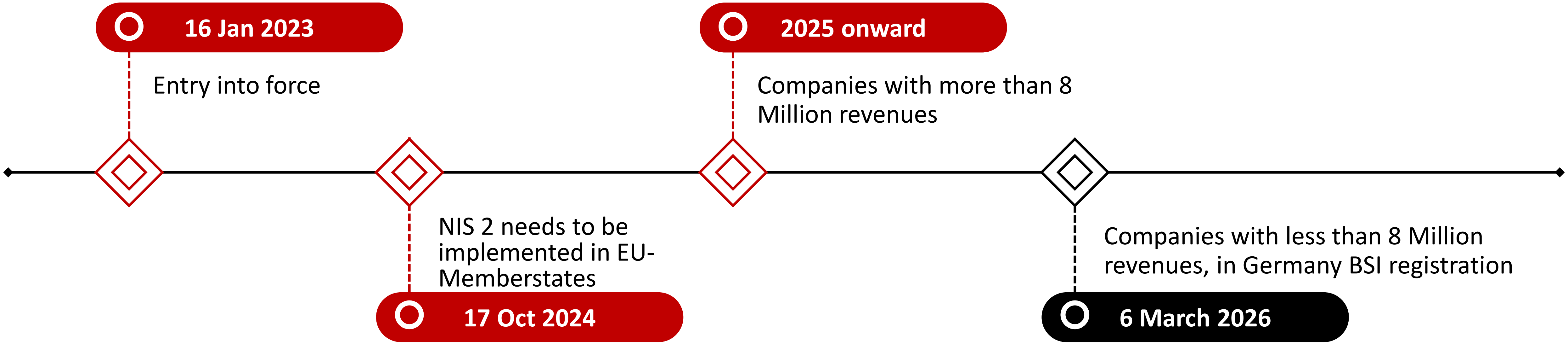
Module 2

Interface regulation – NIS-2, DORA & DSA

AI-generated content

Implementation deadlines for the NIS-2 (ISO27001)

Companies should prepare for requirements at an early stage and establish governance structures



16 Jan 2023

Entry into force

17 Oct 2024

NIS 2 needs to be implemented in EU-Memberstates

2025 onward

Companies with more than 8 Million revenues

6 March 2026

Companies with less than 8 Million revenues, in Germany BSI registration

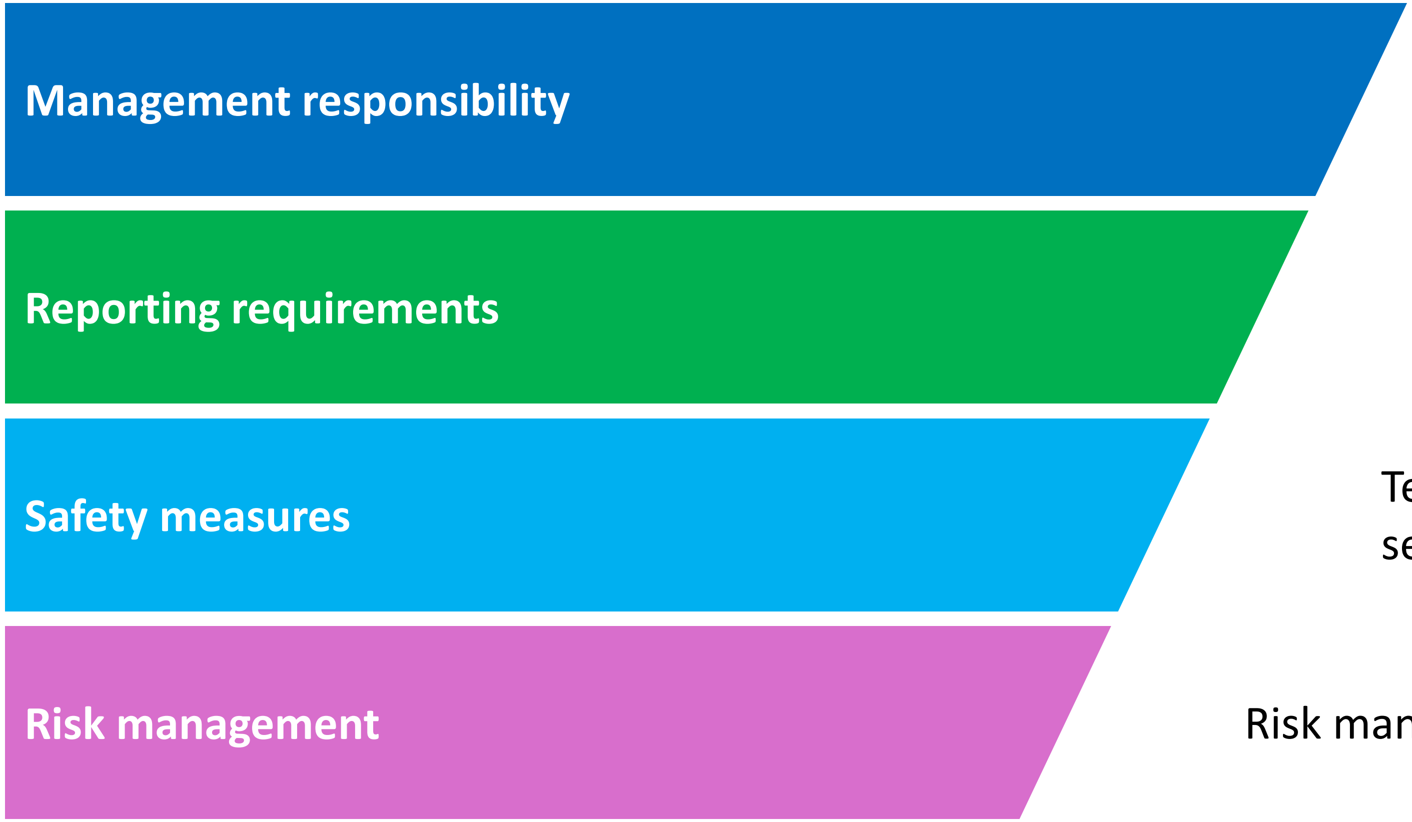
NIS-2 Preparation Phase

Scope assessment	Cybersecurity rm	Incident reporting	Governance
Identify if entity is **essential or important**	Policies, controls, risk assessments	24h early warning 72h incident notification	Management responsibility Security training Supply chain security

NIS-2 directive & AI security

Strengthening IT security and risk management measures

Requires “essential” and “important” facilities to comply with strict security measures. AI systems must be developed, operated, and monitored securely.



Management responsibility

Implementation of cybersecurity measures

Reporting requirements

In the event of significant security incidents

Safety measures

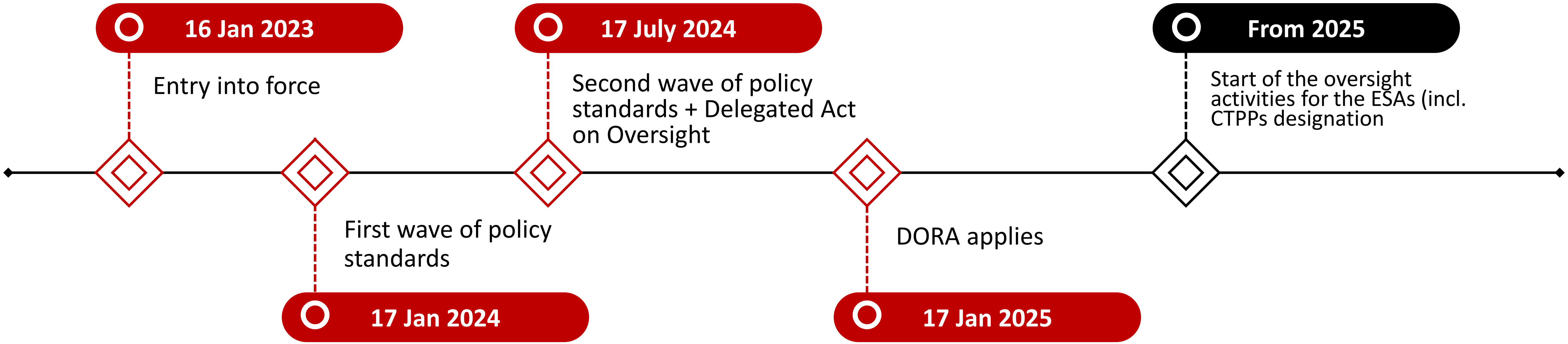
Technical and organizational security measures

Risk management

Risk management for IT and AI

Implementation deadlines for the DORA

Companies should prepare for requirements at an early stage and establish governance structures



16 Jan 2023

Entry into force

17 Jan 2024

First wave of policy standards

17 July 2024

Second wave of policy standards + Delegated Act on Oversight

17 Jan 2025

DORA applies

From 2025

Start of the oversight activities for the ESAs (incl. CTPPs designation

DORA Preparation Phase

ICT RM framework	Incident management	Third-Party risk management	Testing & resilience
Risk identification Resilience controls	ICT incident classification Reporting processes	ICT vendor oversight Contractual requirements	Operational resilience testing Threat-led penetration testing (TLPT)

Digital Operational Resilience Act, Data Act & AI security

DORA relevance for AI

Digital resilience for the financial sector (Data Act general):

ICT risk management

Comprehensive risk management is essential for AI in the financial sector

Resilience tests

e.g., penetration tests are required for AI systems

Incident reports

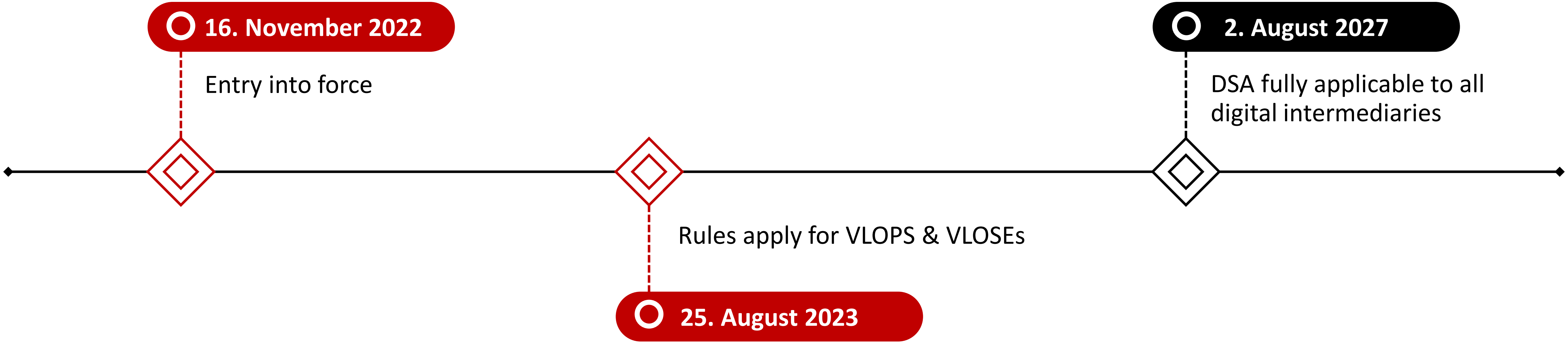
Reporting serious incidents to the financial supervisory authority

Third-party requirements

Strict requirements for third-party providers (e.g., cloud or AI service providers)

Implementation deadlines for the DSA

Companies should prepare for requirements at an early stage and establish governance structures



16. November 2022

Entry into force

25. August 2023

Rules apply for VLOPS & VLOSEs

2. August 2027

DSA fully applicable to all digital intermediaries

DSA Preparation Phase

Plattform mapping	Content governance	Transparency	Risk management
Identify role (hosting service, online platform, marketplace)	Notice-and-action procedures Illegal content handling	Transparency reports Ad transparency & recommender system transparency	Systemic risk assessments Independent audits

Digital Services Act & AI security

Regulations on digital services and online platforms

Transparency	Disclosure of the functional logic of ranking algorithms
Risk asessment	Risk assessments for systemic risks (e.g., disinformation)
VLOP obligations	Special obligations for very large platforms
Prohibition of manipulative practices	Prohibition of certain manipulative practices (“dark patterns”)

Data Act

Enabling users to access data from connected products

Key Data Act Timeline Milestones:

1. **11 January 2024: The Data Act entered into force.**
2. **12 September 2025: General application of the Regulation; users gain rights to access.**
3. **12 September 2026: Design requirements for products come into force, directly accessible.**
4. **12 January 2027: Abolition of switching charges for data processing services (cloud services).**

The Act applies directly across EU Member States, though, national legislation may be introduced to define specific penalties and supervisory authorities. Not so far in Germany (DADG – is in production).

Module 3

AI Governance – Organization, responsibility, and control

AI-generated content

AI policy

The foundation of good AI governance

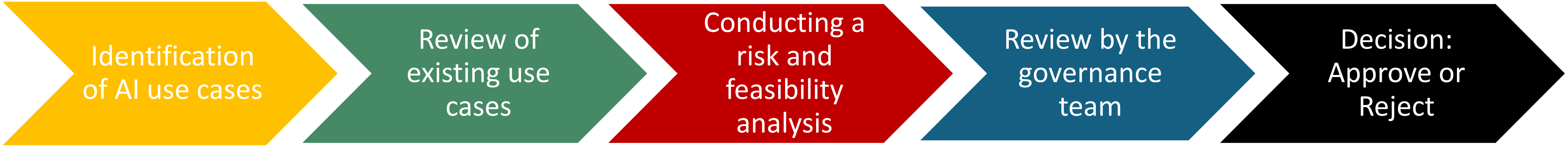
An effective AI policy should include the following points:

- 01 AI principles that are consistent with the company's vision and values
- 02 Obligation to comply with relevant regulatory and security requirements
- 03 Clear distribution of roles and responsibilities
- 04 A structured training concept for building AI expertise
- 05 List of all approved AI tools

Adoption process for new AI systems

Process for approving new AI systems

- Standardized procedure for selecting new AI systems
- Whether in-house development or third-party product/service
- Particularly relevant for high-risk AI systems


Identification of AI use cases
Review of existing use cases
Conducting a risk and feasibility analysis
Review by the governance team
Decision: Approve or Reject

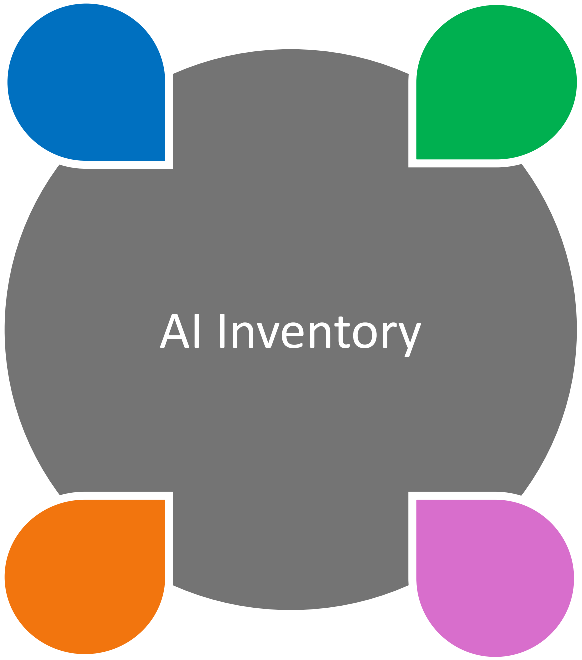
- Quality assurance of AI used through regular audits throughout the entire life cycle

Inventory of AI systems

Keep track of the systems you use

Identification data
e.g., model name, version, type, and owner of the data

Purpose & context of use
What tasks does the AI system or model perform?



Technische characteristics
e.g., architecture, training data, interfaces

Lifecycle-Information
e.g., last validation, retraining data

AI officer

What does an AI officer do?

Advantage: Clear responsibilities prevent gray areas

Comparison: Similar to the data protection officer

Analysis & Classification

- Gap Analysis
- AI Inventory
- Risk Asessment

Strategy & Governance

- AI Policy
- Guidelines
- Access controls

Implementation & Compliance

- Technical Documentation
- Conformity Assessment
- Data-Governance

Training & Awareness

- Raising employee awareness
- AI competence certification

Monitoring

- Legal action
- Policy updates

K11 Consulting GmbH

Your expert for regulatory issues

We offer tailored advice to help you solve and simplify your regulatory challenges. With our expertise, we support companies in efficiently navigating the complex requirements of the digital and regulatory landscape and ensuring their compliance.

Learn more about AI:
KI-Regulatorik – leicht gemacht | Duncker & Humblot

1. Auflage
Ihr Plus: 38 Übersichten, 21 Leitsätze

KI-Regulatorik
leicht gemacht ✓

KI-Kompetenz nach Art. 4 EU AI Act

Alexander Deicke
Francois Heynike
Hannes Deuerling

Edition Wissenschaft & Praxis EWP

www.k11consulting.de

Contact:

Kaffeeberg 11, 71634 Ludwigsburg

T: +49 (0) 177 6333972

E: Alexander.d@lawflex.com