TaylorWessing

EU Artificial Intelligence (AI) Act

Dr. Axel Freiherr von dem Bussche, LL.M. (L.S.E.), CIPP/E

2025

Outline

1.	AI Act – Introduction	
2.	AI Act – Applicability	
3.	Risked based approach under the AI Act	
4.	AI Act step plan	

1. AI Act – Introduction

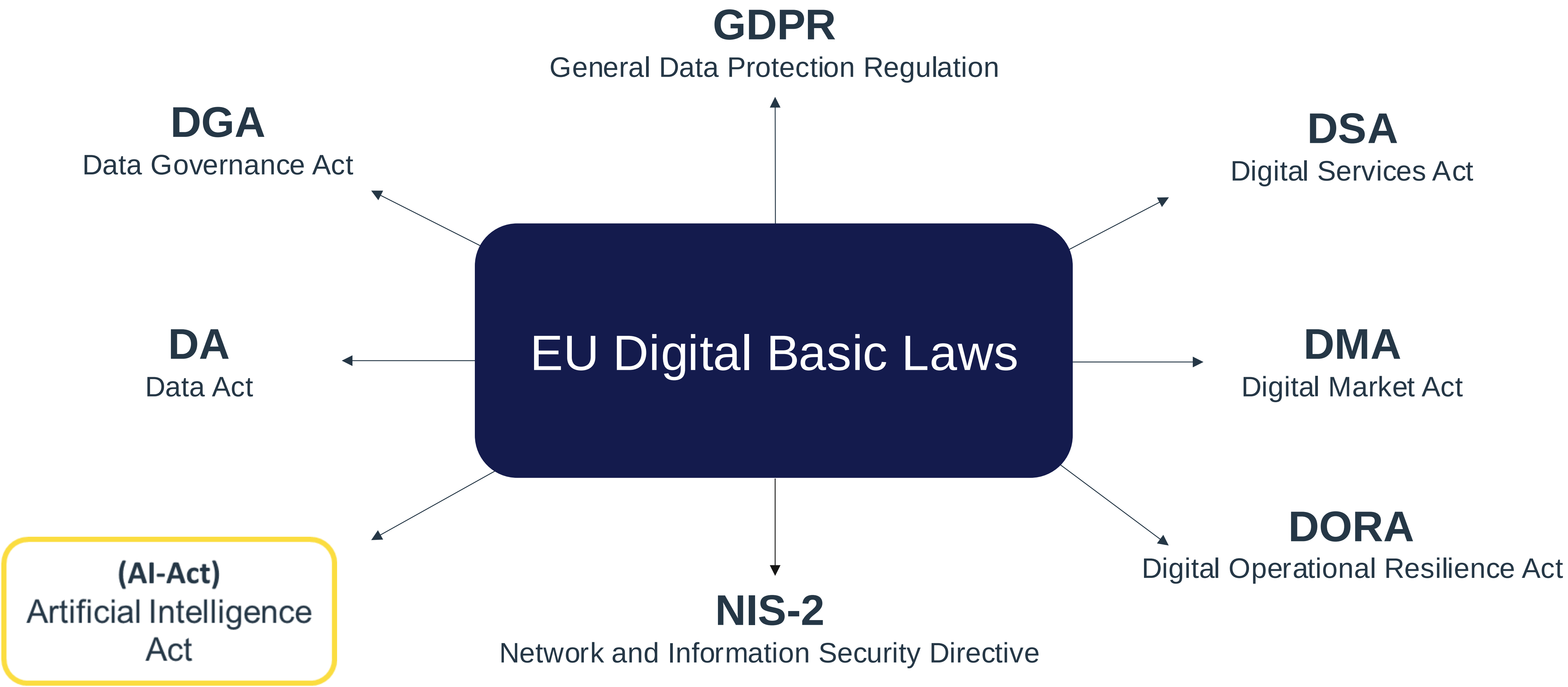
Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	European Statistics, (EC) 2009/223, 2023/0237(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/139, update soon	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	General Data Protection Regulation (GDPR), (EU) 2016/679	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive; (EC) 1998/6	Technology Transfer Block Exemption, (EC) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Regulation on the free flow of non-personal data, (EU) 2018/1807	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Regulation on terrorist content online, (EU) 2021/784	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Open Data Directive (PSI), (EU) 2019/1024	Design Directive, 2022/0392(COD)	Cybersecurity Regulation, 2022/0085(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	Radio Equipment Directive (RED), (EU) 2014/53	Directive on Consumer Rights (CRD), (EU) 2011/83, 2022/0147(COD)	P2B Regulation, (EU) 2019/1150	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Decision on a path to the Digital Decade, (EU) 2022/2481	.eu top-level domain Regulation, (EU) 2019/517	Data Governance Act (DGA Regulation), (EU) 2022/868	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), (EU) 2023/1781	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Directive on combating violence gainst women, 2022/0066(COD)	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)			Digitalization of travel documents	Machinery Regulation, (EU) 2023/1230	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Digital Market Act (DMA Regulation), (EU) 2022/1925	Remuneration of musicians from third countries for recoredd music played in the EU	Digital euro, 2023/0212 (COD)
	Net Zero Industry Act, 2023/0081(COD)	New radio spectrum policy programme (RSPP 2.0)	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106 (COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	Digital Networks Act	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		
	EU Space Law		Interoperable Europe Act, 2022/0379(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
	Initiative to open up European supercomputer capacity to AI start-ups		Harmonization of GDPR enforcement 2023/0202(COD)					Political Advertising Regulation, 2021/0381(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Access to vehicle data, functions and resources					Right to repair Directive, 2023/0083(COD)			
			GreenData4all					Multimodal digital mobility services (MDMS)			
								Consumer protection: strengthened enforcement cooperation			

Overview of EU legislation in the digital sector

Applicable law	Published in the Official Journal of the European Union
In negotiation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative

Quelle: https://www.bruegel.org/sites/default/files/2023-11/Bruegel_factsheet.pdf

Overview: “Digital Basic Laws”



GDPR
General Data Protection Regulation

DGA
Data Governance Act

DSA
Digital Services Act

EU Digital Basic Laws

DA
Data Act

DMA
Digital Market Act

DORA
Digital Operational Resilience Act

(AI-Act)
Artificial Intelligence Act

NIS-2
Network and Information Security Directive

AI Act

What is it about?

- First AI regulation worldwide: protection of fundamental rights (health, safety) and support innovation
- “Product Compliance”, market surveillance and monitoring
- EU-wide harmonised direct-acting legal act
- „Risk-based approach“ → categorisation of AI systems into different classes of risks

Threat of sanctions?

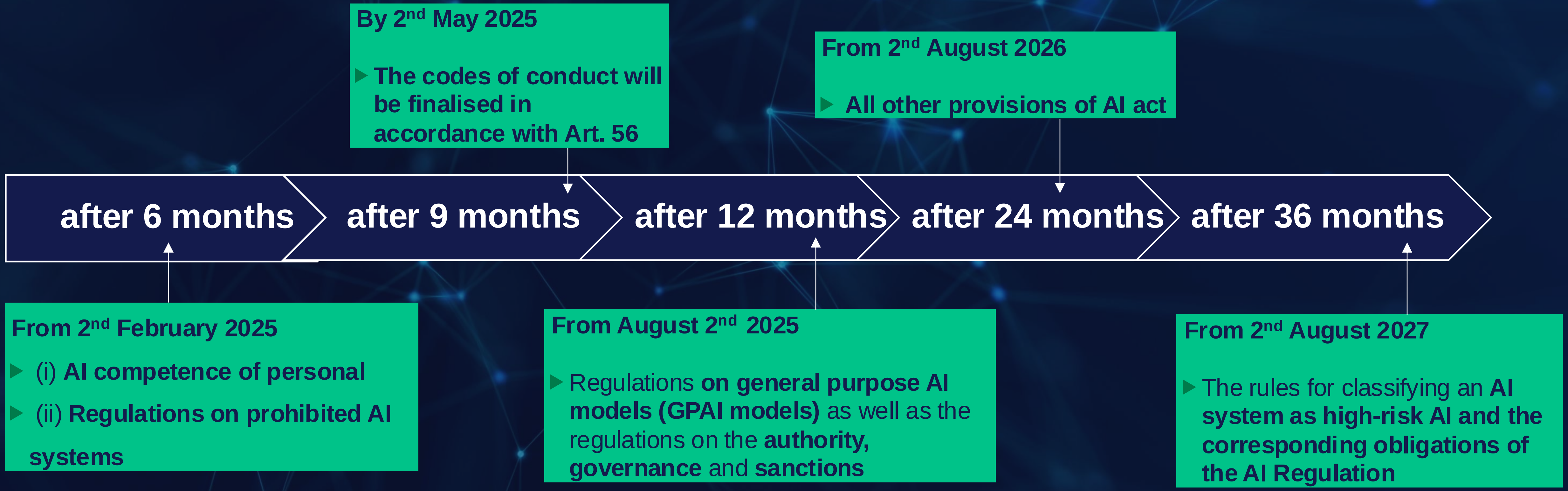
- Fines of up to 30 million euros or up to 7% of the worldwide annual turnover
- Regulatory restriction or even prohibition of the provision of AI systems

Who is affected?

- Providers of AI systems or models
- Operators of AI systems
- Product manufacturers who market AI systems together with their product
- Extraterritorial approach (may affect third country companies)

Entry into force and application (Art. 113)

- The AI act was officially published on **12 July 2024** in the Official Journal of the EU and entered into force 20 days later on **1st August 2024**. The following transitional periods are provided for until final effectiveness (Art 113 AI Regulation):



By 2nd May 2025

- **The codes of conduct will be finalised in accordance with Art. 56**

From 2nd August 2026

- **All other provisions of AI act**

after 6 months → **after 9 months** → **after 12 months** → **after 24 months** → **after 36 months**

From 2nd February 2025

- (i) **AI competence of personal**
- (ii) **Regulations on prohibited AI systems**

From August 2nd 2025

- Regulations **on general purpose AI models (GPAI models)** as well as the regulations on the **authority, governance** and **sanctions**

From 2nd August 2027

- The rules for classifying an **AI system as high-risk AI and the corresponding obligations of the AI Regulation**

For other AI systems that were placed on the market or put into operation before the start of applicability, the AI Act will only apply where significant changes are made.

2. AI Act – Applicability

Material Scope: Definition „AI system“ (Art. 3)

“a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments “

Material Scope

⚠ Corresponds to the definition in (US) EO 14110

1 machine-based

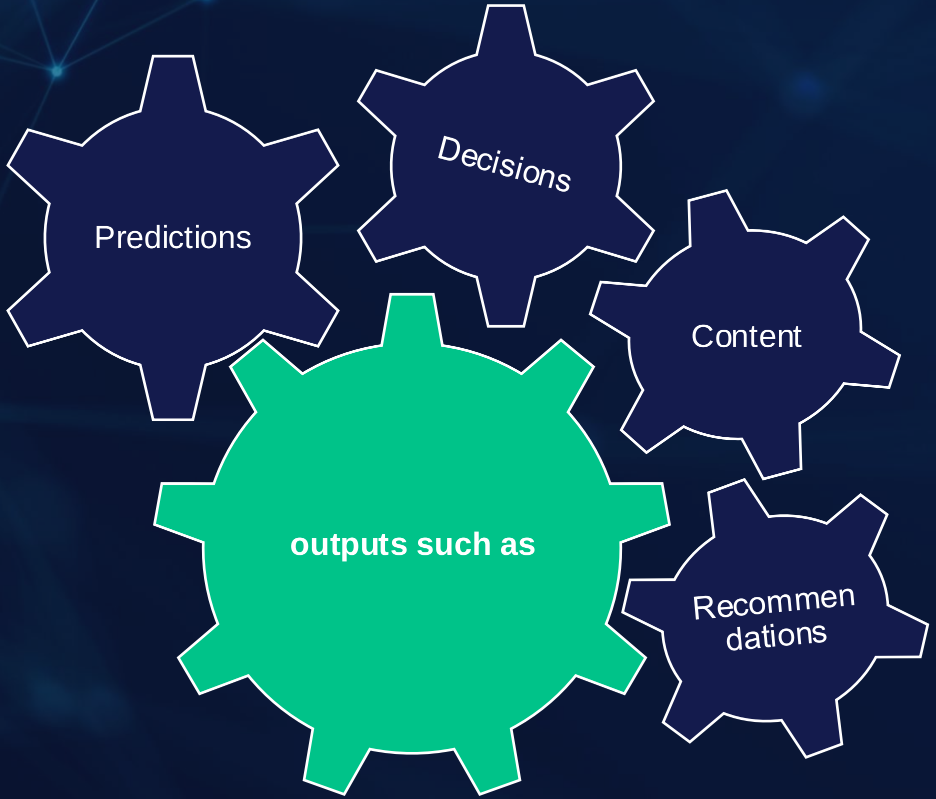
with varying levels of autonomy

→ independent of human control

2 adaptiveness after deployment

3 for explicit or implicit objectives

4 infers from inputs



outputs such as

Predictions

Decisions

Content

Recommendations

Personal and territorial Scope

Personal and territorial, Art. 2 (1)

a) **providers** placing on the market or putting into service AI systems or placing on the market general-purposes AI models **in the Union**, irrespective of whether those providers are established or located within the Union or in a third country;

b) **deployers** of AI systems that have their place of establishment or are located within **in the Union**;

c) **providers** and **deployers** AI systems that have their place of establishment or are located in a third country, where the output produced by the AI systems is used **in the Union**;

d) **importers** and **distributors** of AI systems;

e) **product manufacturers** placing on the market or putting into service an AI system [**in the Union**]* together with their product and under their own name or trademark;

f) **authorised representatives of providers**, which are **not established in the Union**;

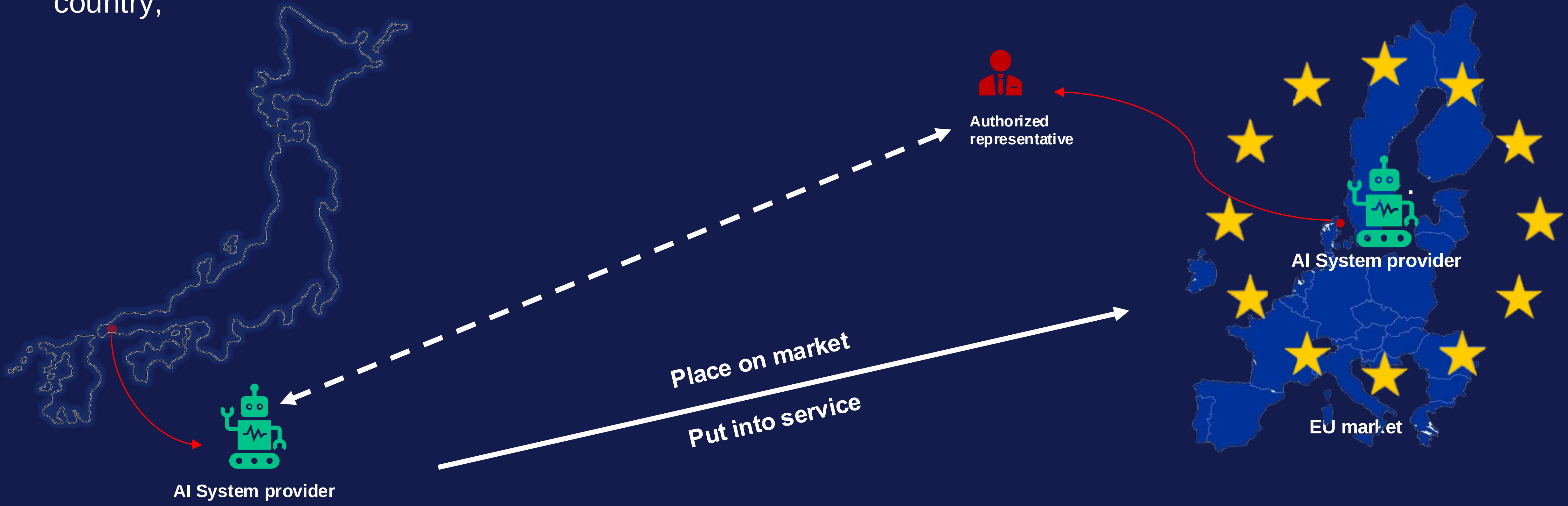
g) **affected persons** that are located **in the Union**.

*cf. Art. 1 (2) (a), Art. 25 (3) AI Act

Use Case 1: Place AI system on EU market

Where does the AI Act apply?

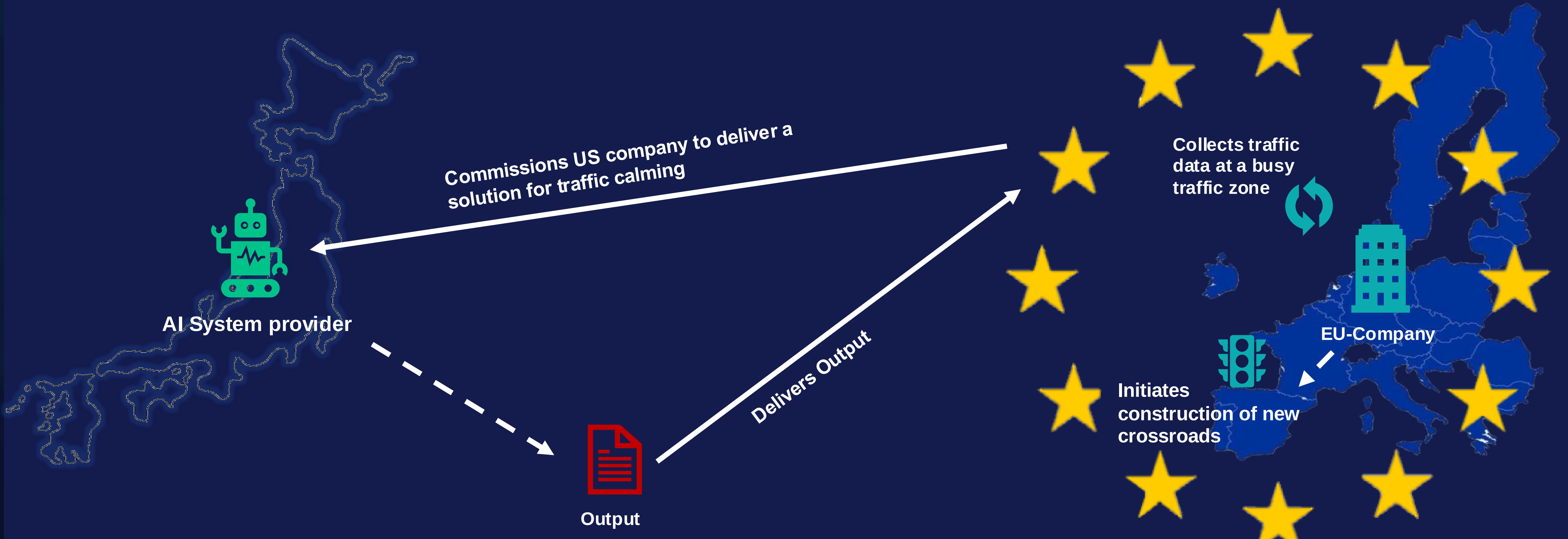
- **providers** placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country;



Use Case 2: Output used in the EU

Where does the AI Act apply?

- Third country providers and deployers where the **output produced by the AI system is used in the EU**


Commissions US company to deliver a solution for traffic calming
AI System provider
Output
Delivers Output
Collects traffic data at a busy traffic zone
EU-Company
Initiates construction of new crossroads

Authorised representatives of providers of high-risk AI systems

Article 22

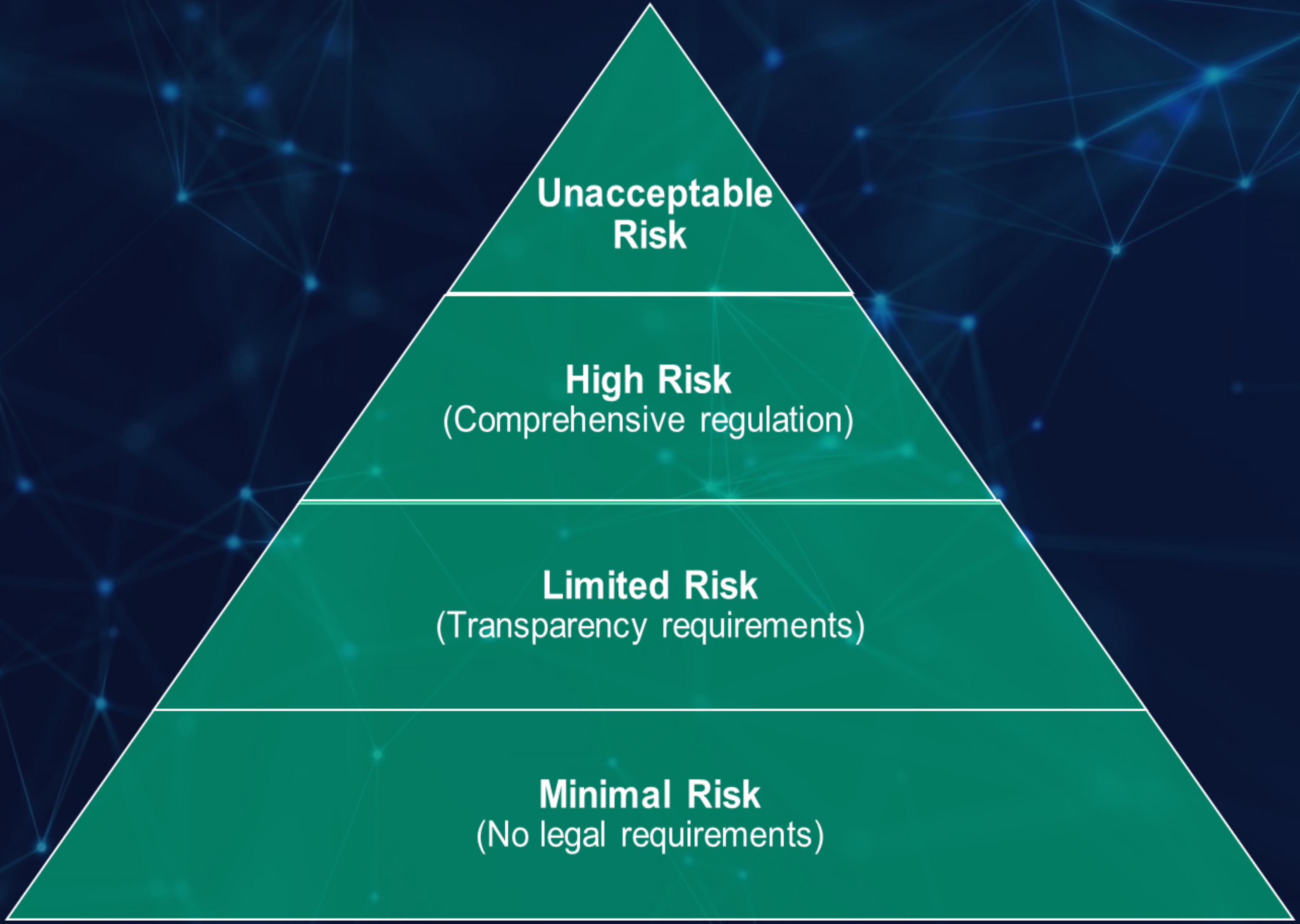
(1) Prior to making their high-risk AI systems available on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.

(2) The provider shall enable its authorised representative to perform the tasks specified in the mandate received from the provider.

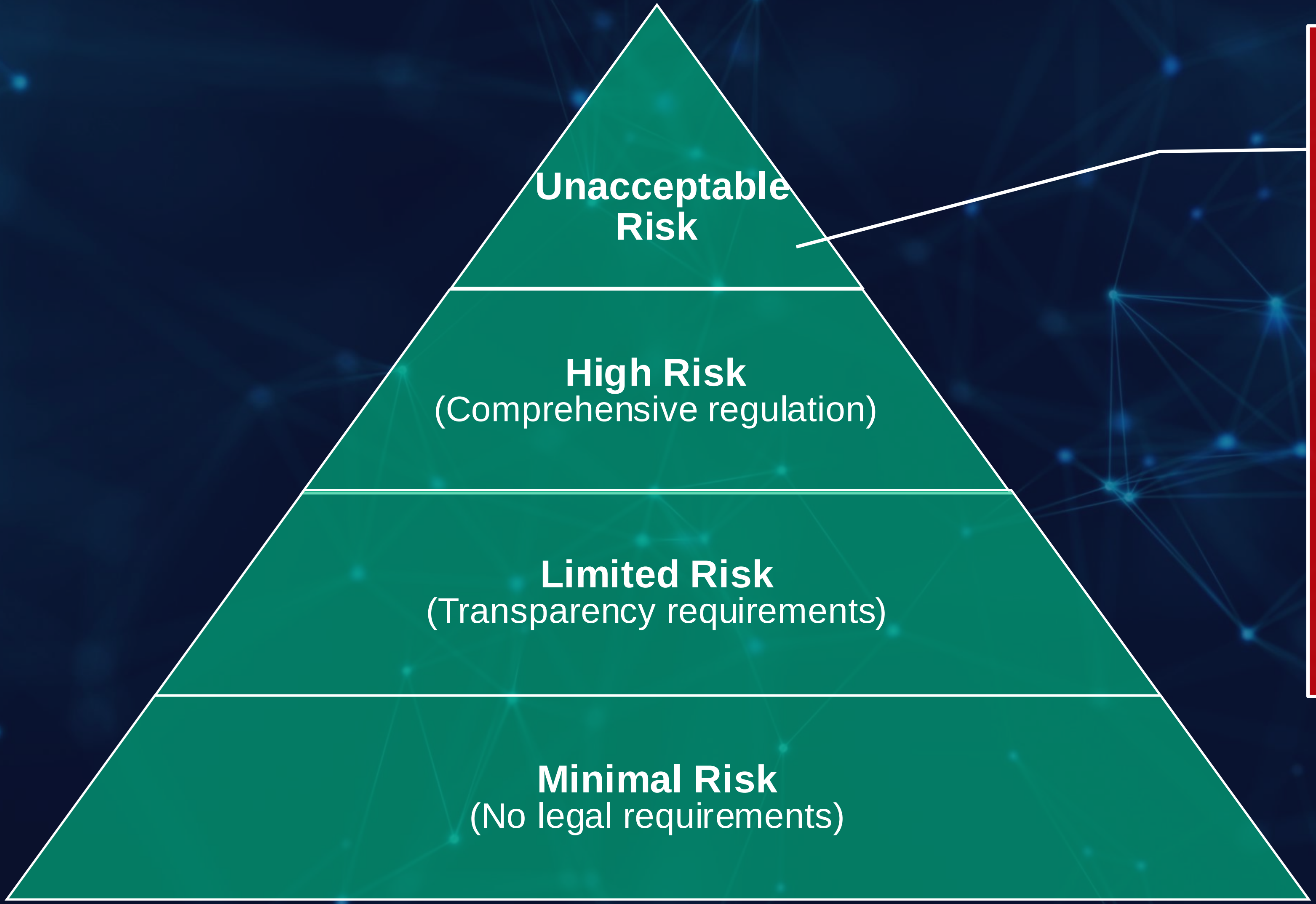
[…]

3. Risked based approach under the AI Act

AI Act – Risk based approach



AI Act – Risk based approach

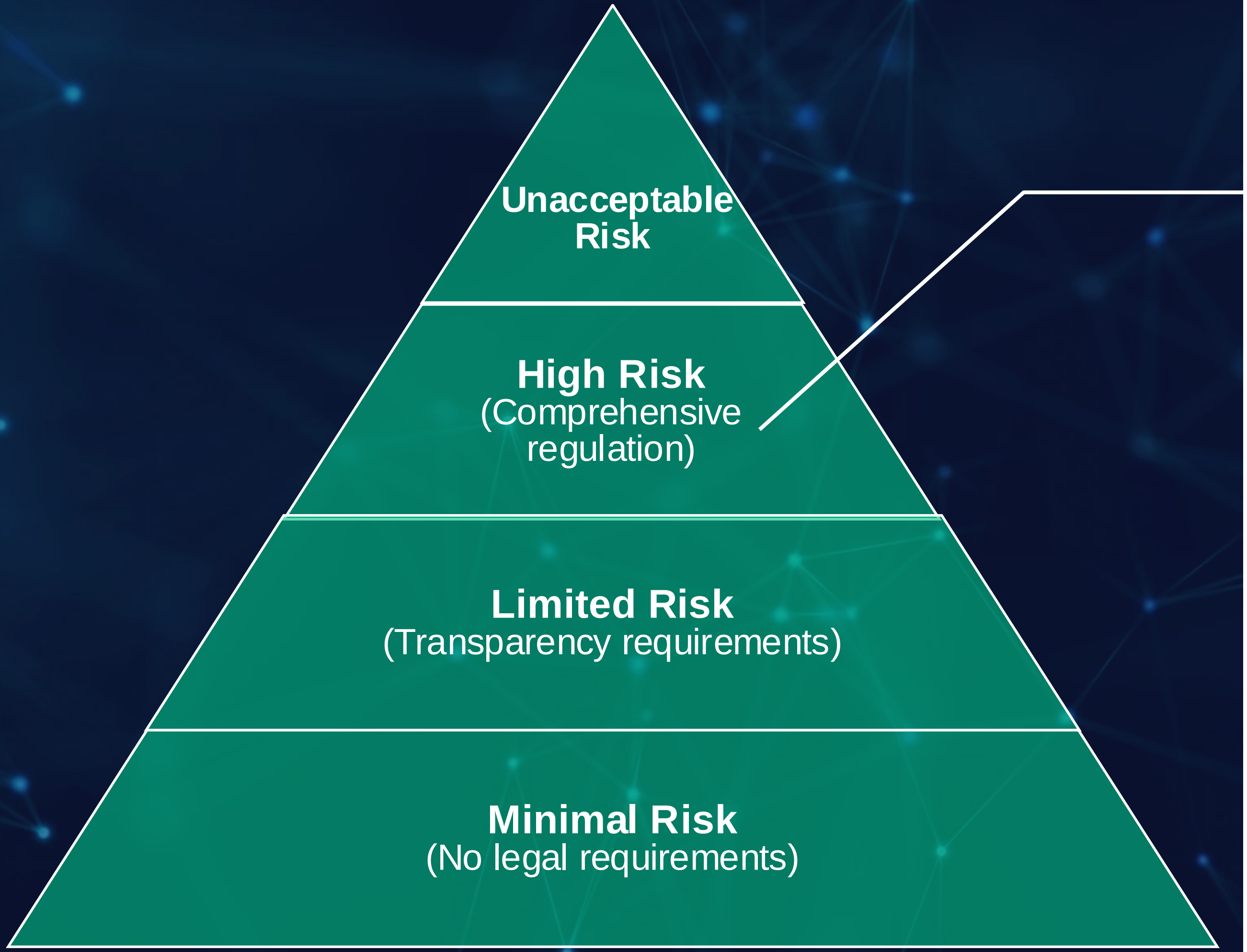


Banned applications:

- **Manipulative AI**
- **Exploitative AI**
- **Social Scoring**
- **Predicitive Policicing**
  - **Risk assessments**
  - **Facial recognition databases**
- **Emotion recognition (workplace / school)**
- **Biometric categorisation systems**
- **Real time biometric identification systems**

(but extensive exceptions for law enforcement)

AI Act – Risk based approach



Unacceptable Risk
High Risk (Comprehensive regulation)
Limited Risk (Transparency requirements)
Minimal Risk (No legal requirements)

High Risk AI:

Embedded AI

Safety component of a product or the product itself
+
Subject to a conformity assessment

Civil aviation

Recreational craft

Toys

Medical Devices

Agricultural verhicles

Listed products in Annex I

Non-embedded AI

Listed in Annex III

Education and vocational training

Work: Promotion / Termination decisions

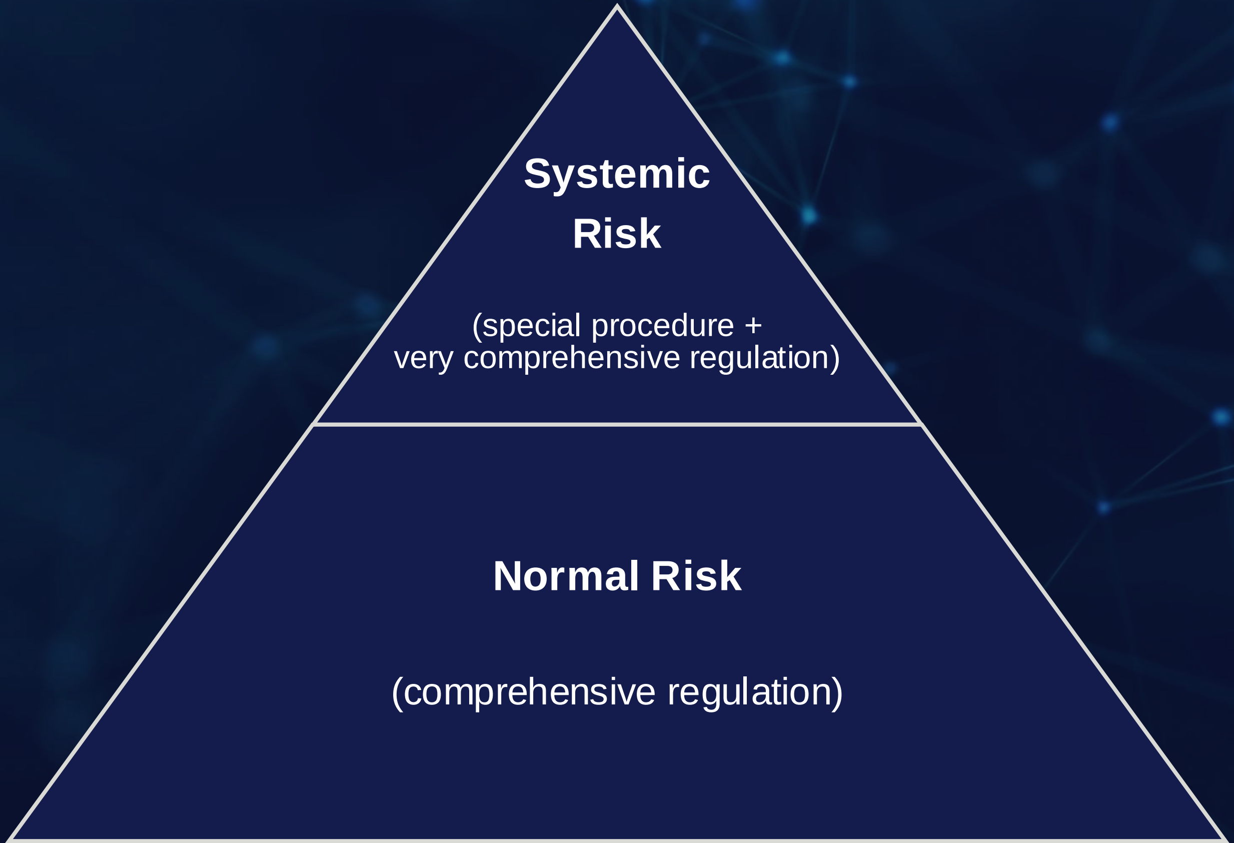
Border control

Recruitment

Supply of energy

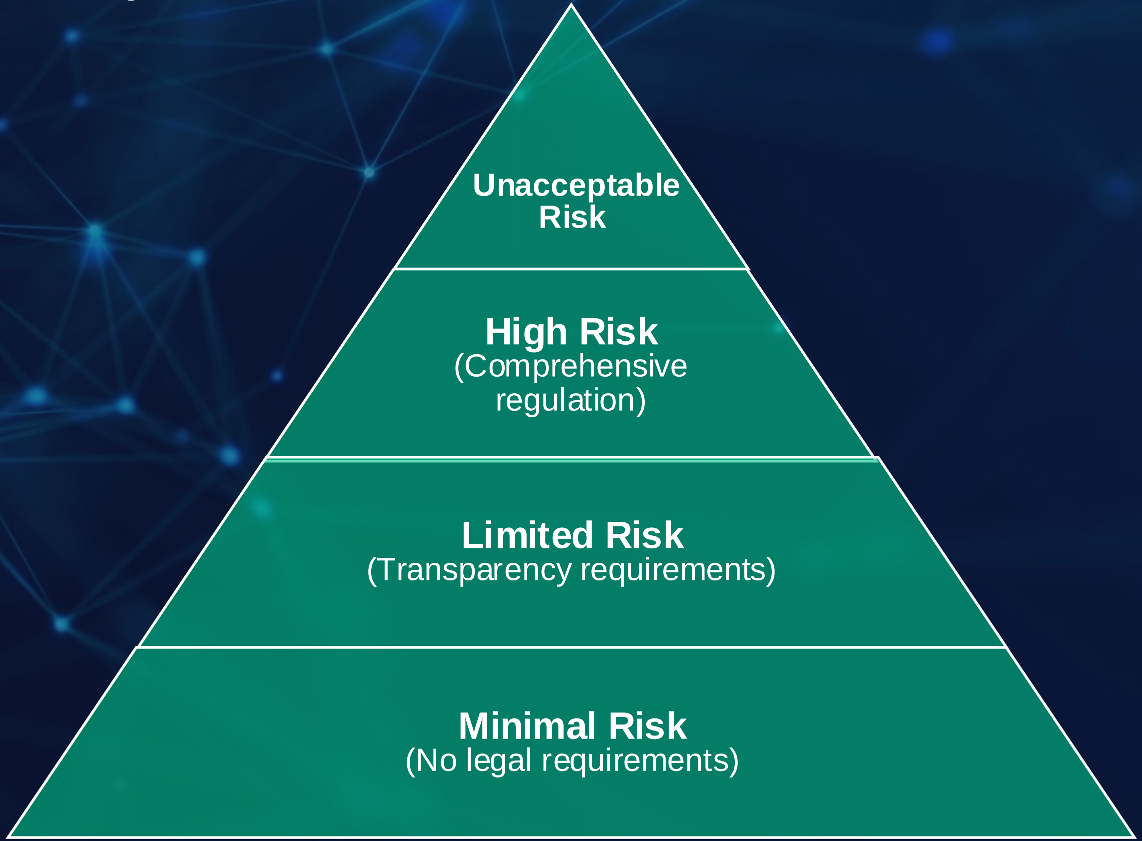
AI Act – Risk based approach

Risk assessment: General-purpose AI Models



Systemic Risk
(special procedure + very comprehensive regulation)
Normal Risk
(comprehensive regulation)

Risk assessment: AI Systems / General-purpose AI Systems



4. AI Act step plan

STEP 1 – AI mapping

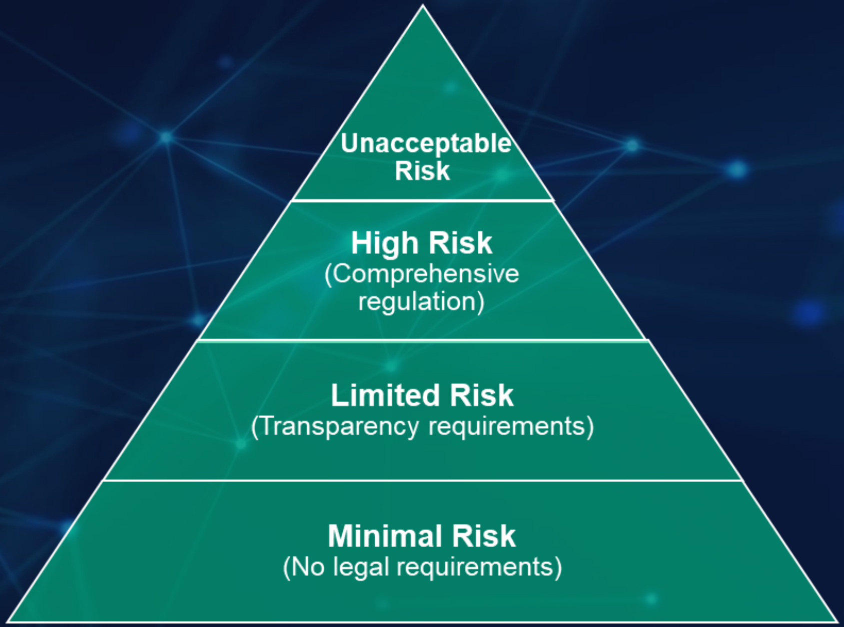
- Carry out a **gap analysis** between the current status of compliance and the obligations deriving from the AI Act
- As a first step, map your current and prospective use or development of AI by asking questions including:
  - What types of AI applications are developed or used by which departments?
  - What data is used when deploying AI?
  - Are there company guidelines regarding the development, distribution and use of AI?
  - Are internal guidelines clearly distributed?
  - What risks do you expect when implementing AI in your organization?
  - What measures are needed to control the risks of AI and avoid liability risks?
  - What steps are needed to build employee and customer trust in the use of AI?
  - What criteria should be considered when selecting AI tools and services to ensure long-term security and quality?

STEP 2 – Risk assessment

- Assess which AI Act requirements apply. This requires a detailed analysis of the risk category of each AI system or model and the company´s role for example, whether they are a provider, deployer, importer, distributor or product manufacturer in relation to relevant AI.

- The gap analysis and risk assessment will inform your governance requirements (STEP 4).

- **Remember:** you may have a lot to do in order to comply with the AI Act so focus on the areas of greatest risk.



Unacceptable Risk

High Risk (Comprehensive regulation)

Limited Risk (Transparency requirements)

Minimal Risk (No legal requirements)

Risk category: It is important to understand that the AI Act follows a risk-based approach. It divides AI systems into four groups and sets out rules for general-purpose AI (GPAI) models. GPAI models, also known as foundation models such as GPT-4, are AI models that are trained with a large amount of data and can be integrated into a variety of downstream applications.

Company´s role: Most of an AI Act´s obligations apply to providers of AI systems. However, users (deployers) are also regulated. Other addressees of the AI Act are importers, distributors, product manufactures and authorized representatives of providers.

STEP 3 – Resource and budget planning

- **Assign project responsibilities** to key personnel and have buy-in from the excecutive board.

- Allocate adequate resources: This should cover: additional personnel and administration, legal and IT costs (e.g. for data governance, technical documentation, record-keeping and cybersecurity). Legal costs as well as IT costs (e.g. for data governance, technical documentation, record-keeping, cybersecurity.

- **Integration with other compliance management systems is essential.** This means that it is important to consider existing approaches with regard to:

  - Information security and risk management
  - Outsourcing and vendor management
  - GDPR compliance and other data governance management
  - A company´s code of conduct and ethics compliance

STEP 4 – Implementation of an AI governance scheme

- Implement a targeted AI governance scheme based on the outcomes of steps 1 and 2. The higher the level of risk and subject to your role, the more obligations will apply. For example, for high-risk AI systems, obligations may include:

- AI literacy
- Quality management system
- Risk management system
- Transparency obligations
- Technical documentation
- Data requirements
- Reporting
- Human oversight
- Registration
- Cooperation with authorities
- Conformity assessment
- Cybersecurity, accuracy and robustness
- Automatic recording of events
- Post-market monitoring

- For deployers less intensive obligations apply including AI literacy, human oversight, data governance and transparency.

STEP 5 – Stay up to date

- The requirements under the AI Act make it necessary for companies to continously monitor regulatory developments, their AI system and model landscape and readjust their AI governance.

  - This means you will need to go through the **5 step** cycle on a regular basis

  - The European Commision will adopt delegating guidelines to adjust the scope and refine specific requirements under the AI Act.
    It is **crucial for companies to keep track of these changes** and consider future guidelines and codes for practices from the new established AI Office and competent national authorities

- Please note that the **AI Act is only one important piece of a cluster of horizontal and sectoral regulations regarding AI.**

Other relevant legal acts that must be considered are:

- The **General Data Protection Regulation** e.g. for AI training, the **Cyber Resilience Act** regarding AI cybersecurity requirements

- The **Data Act** for AI-based IoT-devices or to train third-party AI, the AI/Product Liability Directive when AI systems cause damages

- The **Digital Services** e.g. for AI content moderation

- The **Directive on Copyright on the Digital Single Market** for licensing and compensation for rightsholders

Employment law relevance

Obligations of employers as users of AI systems

- Implementation of technical and organizational measures to ensure a secure application (Art. 26 AI Act)
- Informing employees affected by an AI's decisions about the role of the AI in the decision-making process (Art. 86 AI-Act)
- Informing and training employees about the use of AI in the work process
- Observance of retention and documentation requirements

- HR applications are categorized as high risk
  - AI systems used in recruiting to select applicants or in the context of decisions to terminate employment

- AI applications with an “unacceptable risk” are generally prohibited
  - Systems for evaluating facial images to analyze emotions in the workplace or categorize biometric data

Current legal AI issues

Copyright Law

- Is the AI only trained using content that falls under “fair use”, or did the AI use copyrighted material of the internet?
- Is AI generated content protected under copyright?

Data Protection Law

- Lack of legal basis for processing for the data collected to train the AI.
- Issues with core principles of the GDPR (transparency, purpose limitation and data minimisation, accuracy, and storage limitation).

Confidential Information

- Training data may infringe secret information (e.g. AI translation of secret agreements)

Your Taylor Wessing Team

Axel Freiherr von dem Bussche is a specialist lawyer for information technology law in the Technology, Media & Telecoms practice group. He advises clients on national and international digital and data protection projects and is a recognised IT law and GDPR expert.

With his many years of experience and outstanding expertise, Axel von dem Bussche routinely guides clients on the provider and user side through complex, international transactions, contract drafting and regulatory issues. He advises corporations on the transformation towards digital and global business models, supports companies in the implementation of AI and data protection regulations, is a strategic advisor to management on compliance in digitalisation and conducts negotiations with the relevant supervisory authorities.

Languages

German, English, French

"

"Data protection specialist Axel von dem Bussche advises well-known clients on data issues (…). He also represents clients in proceedings on a regional and national level against data protection supervisory authorities."; "He has all the new updates, is very client-oriented and quickly analyses new laws," client, Chambers & Partners Europe 2021-2024
Ranked lawyer for data protection, Chambers Europe 2019 – 2024
Frequently recommended for information technology and data protection "one of the best, absolute strategist", "very strong client orientation, negotiation skills and assertiveness", "Excellent legal advice and technical knowledge coupled with a strong client focus", "Best lawyer in Germany for litigation cases in data protection," clients "very active, extremely strong", "absolute expert in the industry", "supports younger generations remarkably well", "Pleasant and very experienced", competitor; JUVE 2015/16-2024/25
Highlighted as a "Though Leader" for Data in Germany, Who`s Who Legal 2025
Leading individual: Information Technology & Digitalization, The Legal 500 2021 – 2024
Recommended lawyer for data protection, IT-Transaction and Outsourcing, The Legal 500 2024
Top-100- business lawyers Germany, Kanzleimonitor (diruj) 2023/24 – 2024/2025
Leading Lawyer for Data Protection, Kanzleimonitor (diruj) 2020/21 - 2024/2025
Leading Lawyer for Information Technology Law, Kanzleimonitor (diruj) – Kanzleimonitor 2021 / 2022
Top Lawyer for data protection WirtschaftsWoche 2019-2023
Outstanding Lawyer, Thomson Reuters 2022
One of the world's leading Data Privacy and Protection and Information Technology lawyers, Who's Who Legal 2019 – 2024
Highlighted as Lawyer of the Year in 2024 and Best Lawyer for IT, Best Lawyers in Germany, Handelsblatt 2018-2024

Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)

Partner
Hamburg

+49 40 36803-229
a.bussche@taylorwessing.com

Key areas of expertise

- IT & Telecoms
- Data Protection
- Copyright & Media Law
- Litigation & Dispute Resolution
- Technology, Media & Communications

The LEGAL 500 DEUTSCHLAND
LEADING INDIVIDUAL
2024

Chambers RANKED IN
Europe
2024
Axel von dem Bussche