AI Factory Austria AI:AT

Trustworthy AI: Legal Aspects

Michael Löffler
Lead Legal, Regulatory and Ethics

Krisztina Rozgonyi
Senior Scientist, Legal and Policy

17.02.2026

AI Factory Austria AI:AT - PUBLIC Consortium

Disclaimer:
The speakers are solely sharing their personal experiences. Therefore, this free seminar is not a substitute for professional/legal advice.

Beneficiaries

Advanced Computing Austria

AUSTRIAN INSTITUTE OF TECHNOLOGY

Affiliated Entities

TECHNISCHE UNIVERSITÄT WIEN

universität wien

BOKU UNIVERSITY

universität innsbruck

TU Graz

JOHANNES KEPLER UNIVERSITÄT LINZ

Institute of Science and Technology Austria

ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

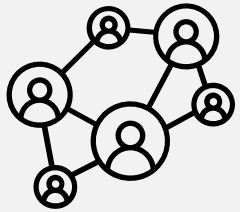
INiTS

eodc

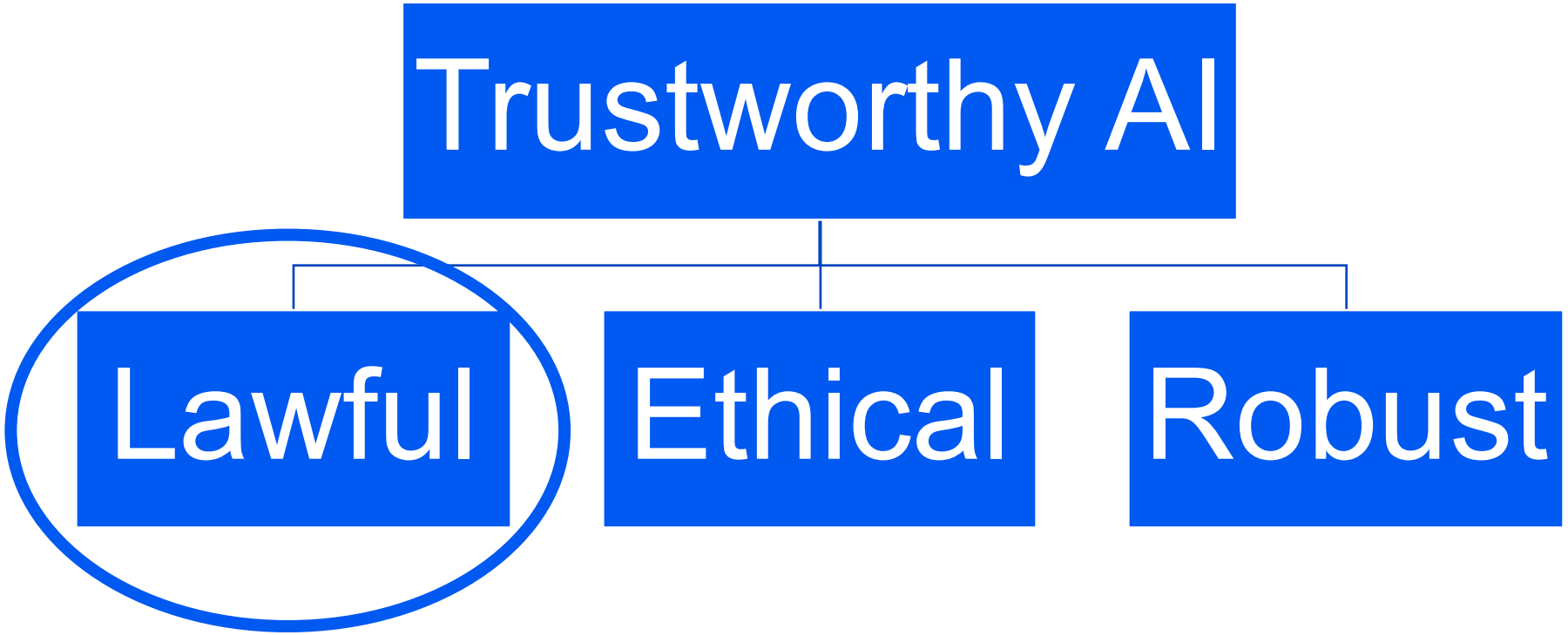
Why do we need AI Factory Austria?

Sovereignty

Ethics and Trustworthiness



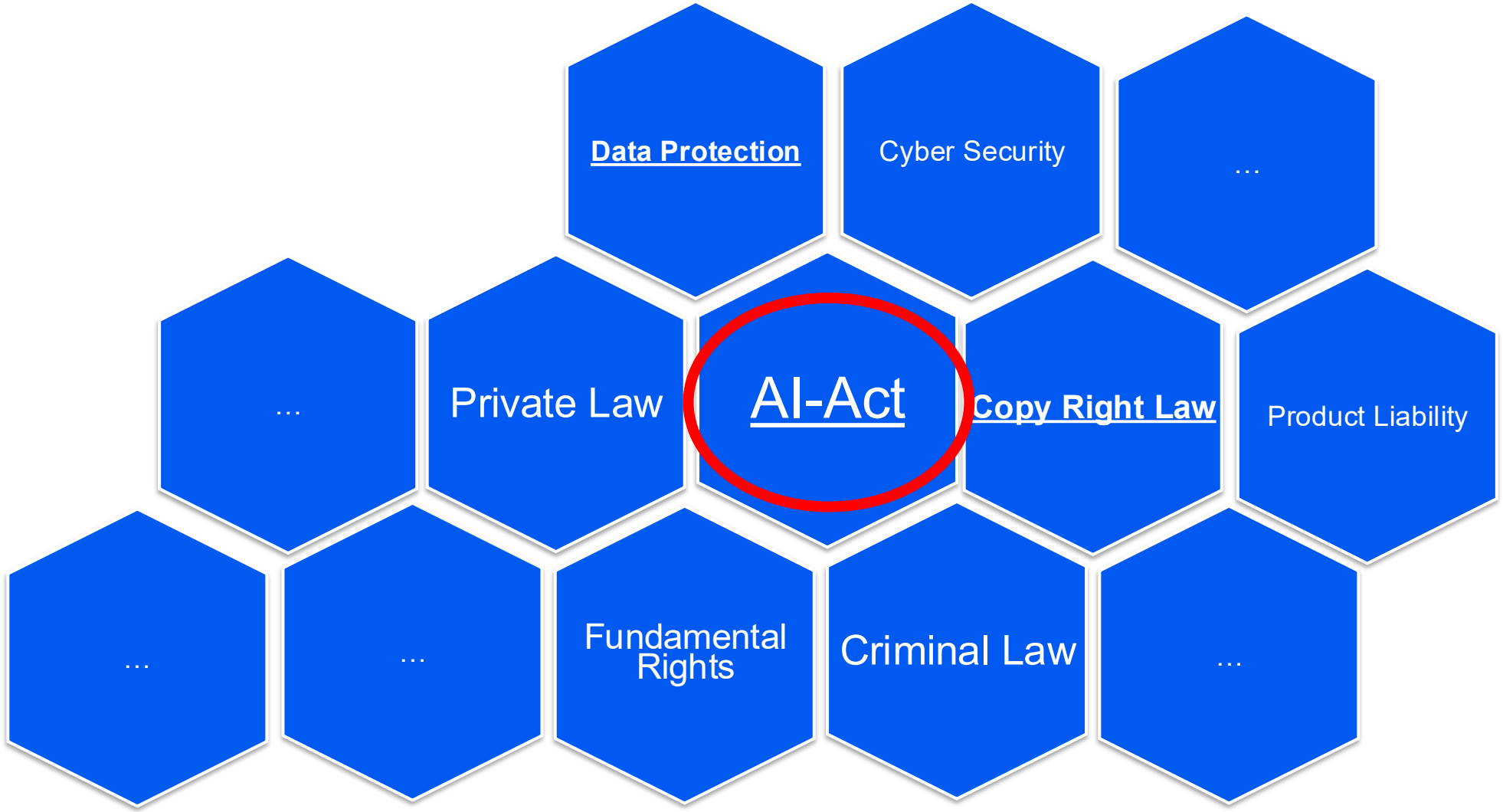
Connecting the Ecosystem



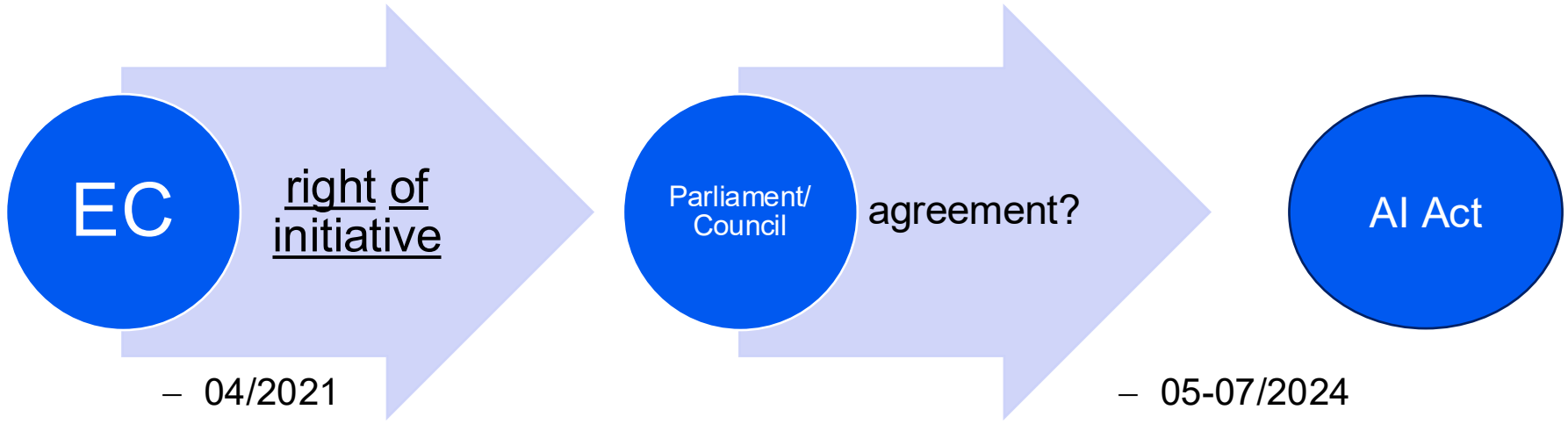
High-Level Expert Group on Artificial Intelligence (HLEG), Ethics guidelines for trustworthy AI, 08.04.2019.

Coester/Pohlmann, Warum Vertrauenswürdigkeit der Grundstein für die Digitalisierung ist, Datenschutz und Datensicherheit - DuD 2025, 11–15.

Legal Landscape



European Legislation (simplified)



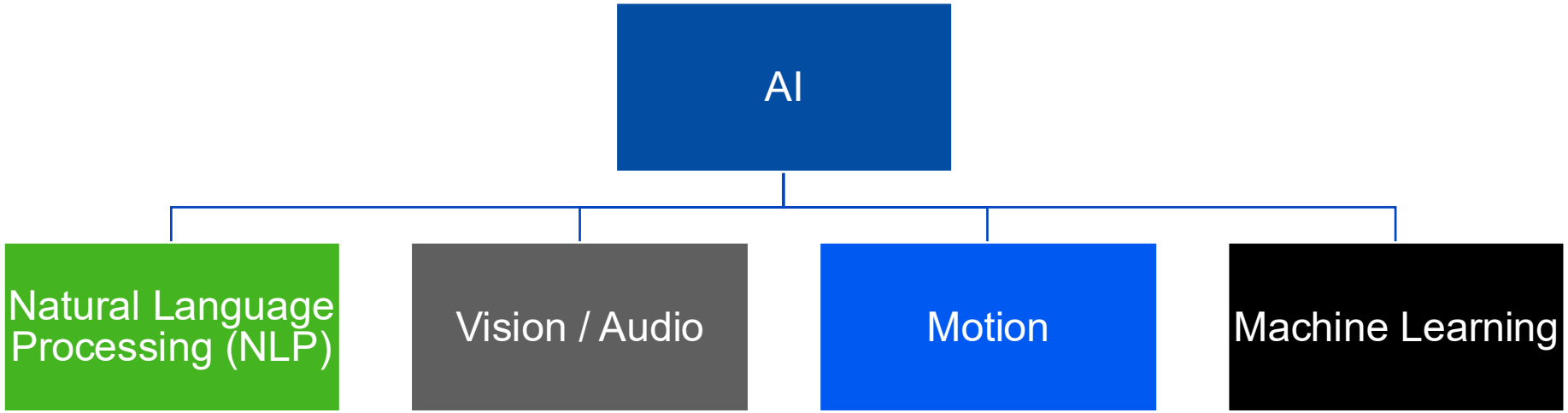
Vaswani et al, Attention Is All You Need, 06/2017.

Release of ChatGPT 11/2022

Release of Gemini 12/2023

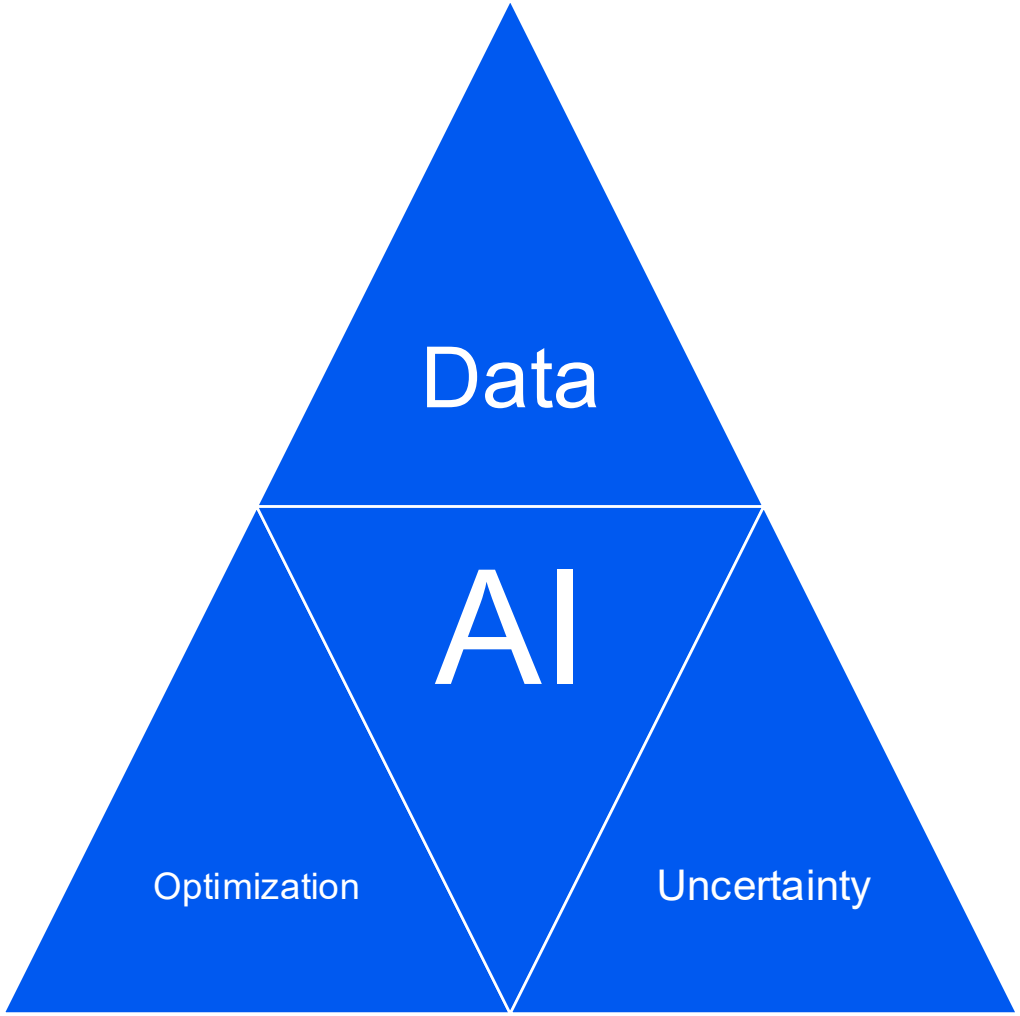
Era of agentic AI 2025/2026

What is "artificial intelligence"?



IBM Technology, AI vs Machine Learning (https://www.youtube.com/watch?v=4RixMPF4xis).

What is "artificial intelligence"?



Wendehorst et al, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605.

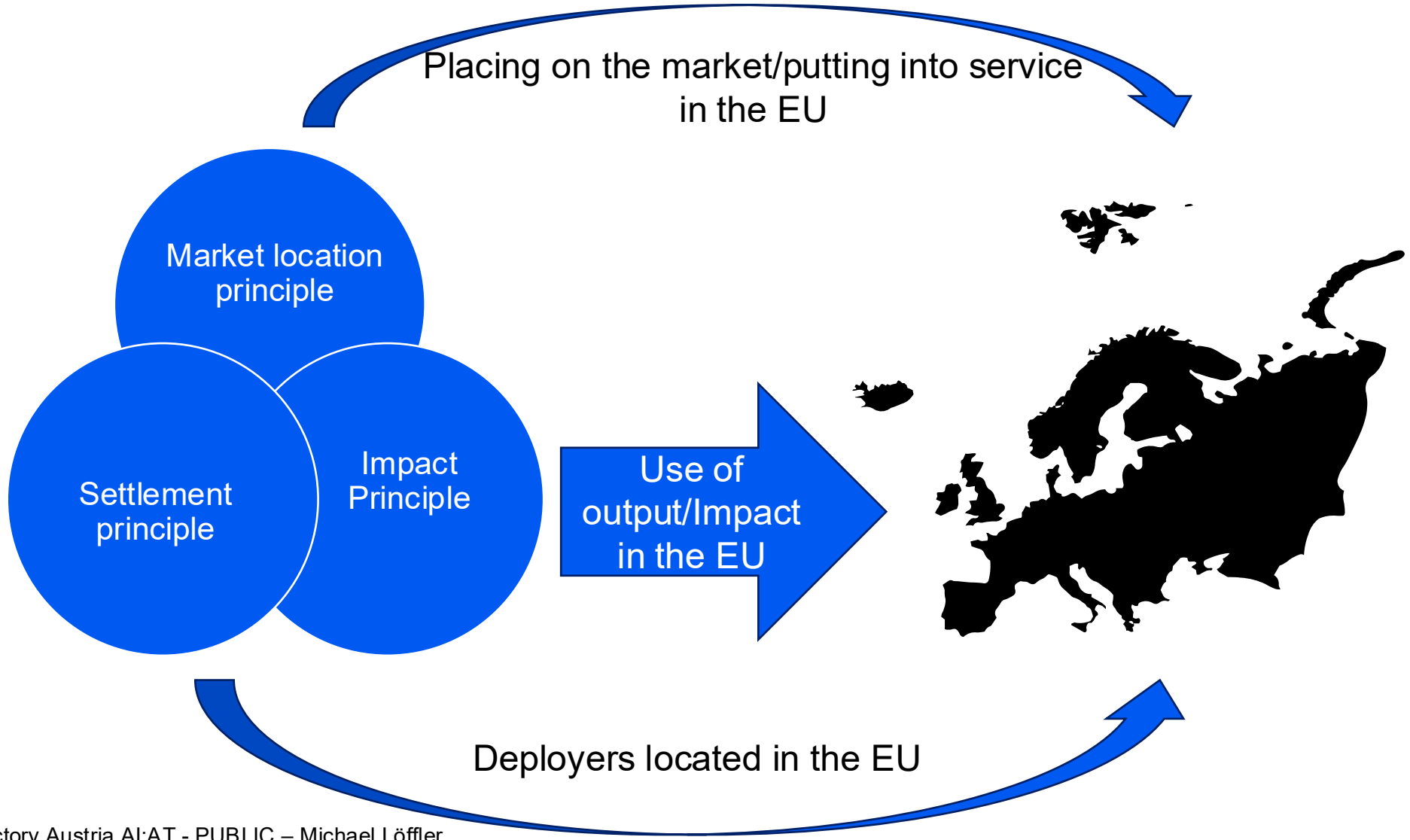
What is "artificial intelligence"?

AI system:[1]

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

1: Sec 3 Num 1 AI-Act; European Commission (EC), Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), 06.02.2025.

When does the AI-Act apply?

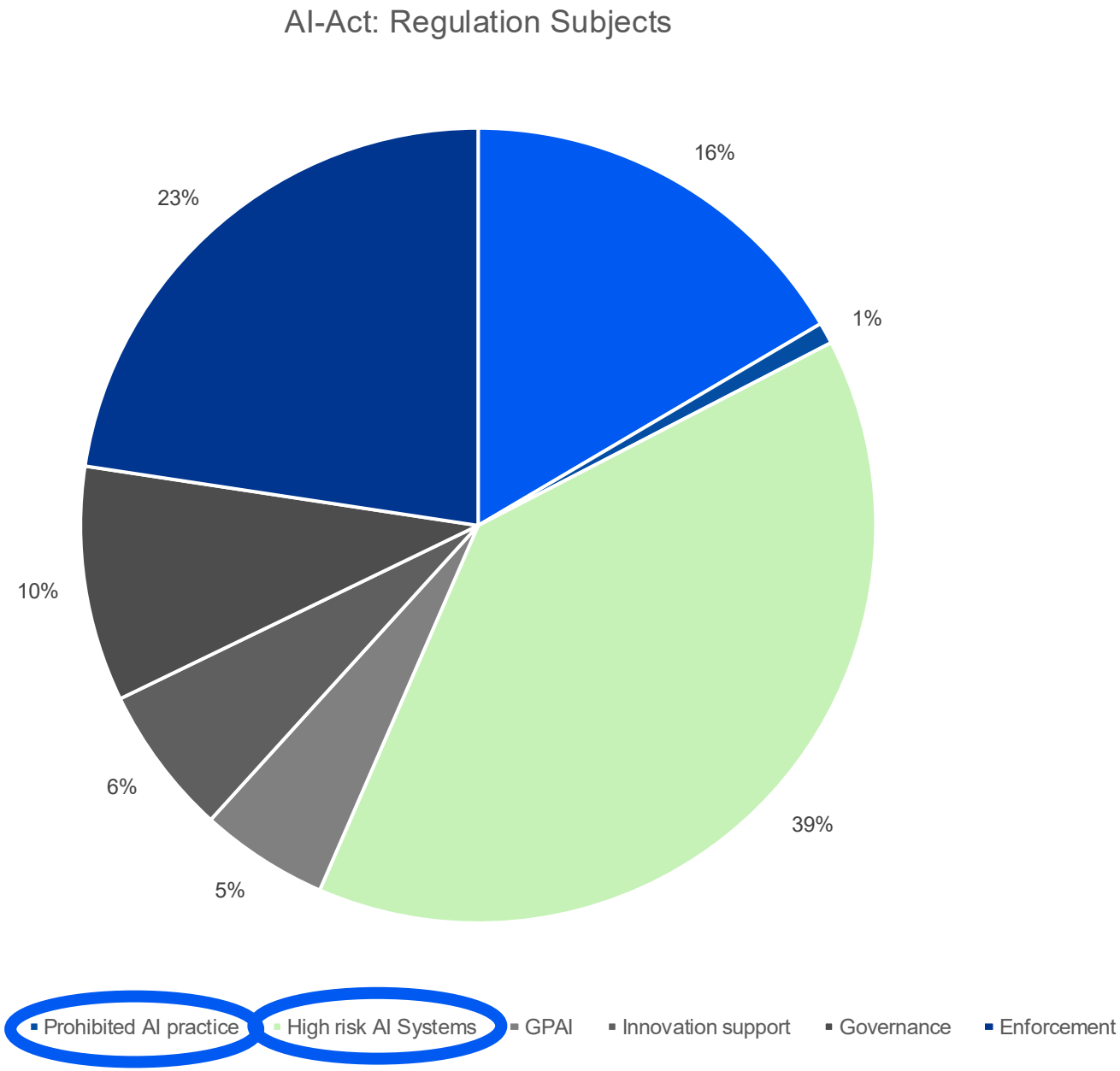


When is the AI-Act not aplicable?

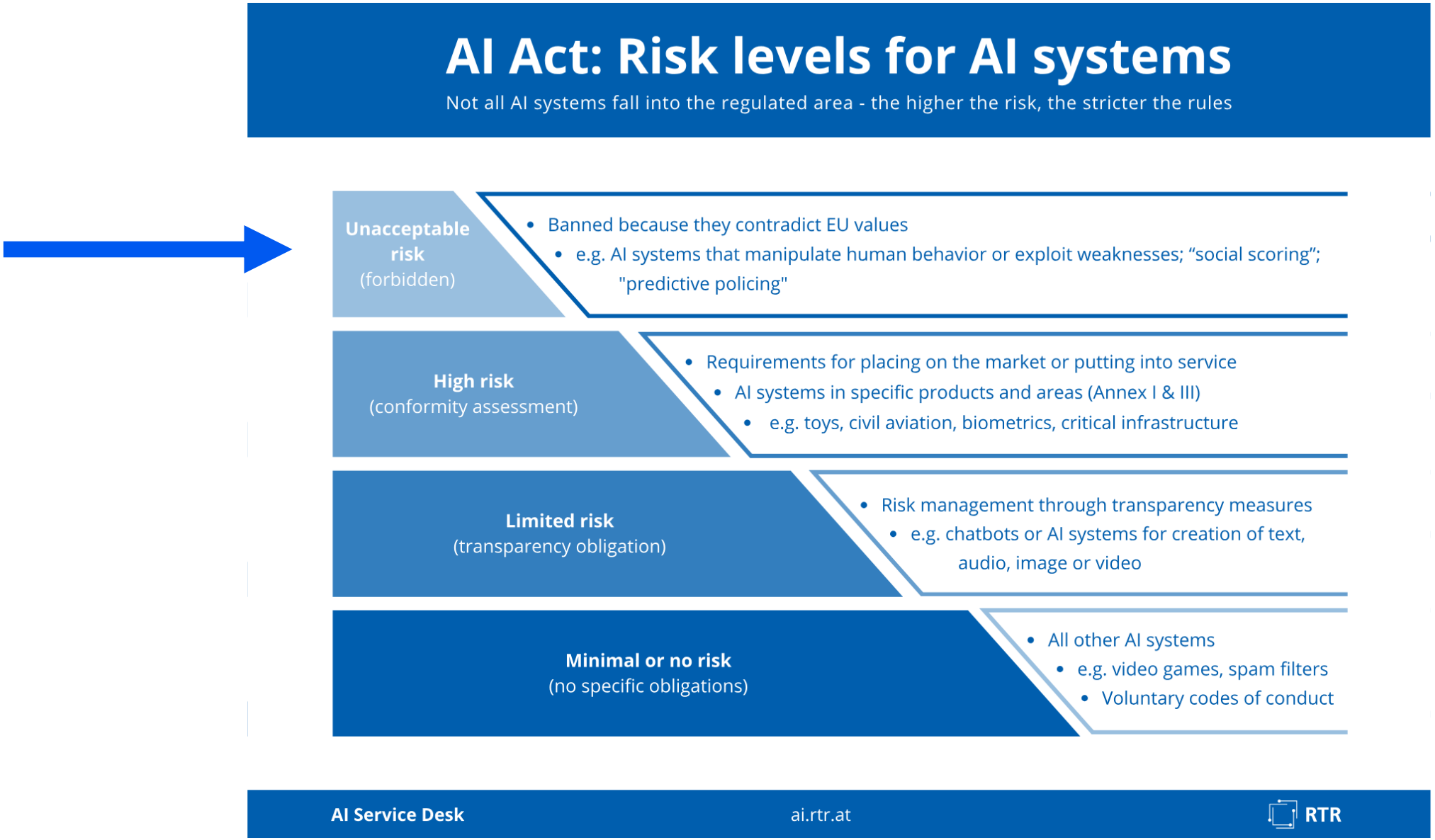
The AI-Act does **not** govern:

- AI systems or AI models, including their output, specifically developed and put into service for the **sole purpose** of **scientific research and development**;
- research, testing or **development** **prior** market placing/putting into service;
- AI systems released under **free and open-source licences**, **unless** they are placed on the market or put into service as high-risk AI systems or as an AI system that is prohibited or an Art 50 AI-Act System;[1]
- the use of AI-Systems by natural persons using AI systems in the course of a **purely personal** non-professional **activity**;

1: *Ziegler/Jürges*, „Open-Source" in der KI-Verordnung, RDi 2026, 77.


AI-Act: Regulation Subjects
16%
1%
39%
5%
6%
10%
23%
General Rules
Prohibited AI practice
High risk AI Systems
GPAI
Innovation support
Governance
Enforcement

AI-Act Risk Levels



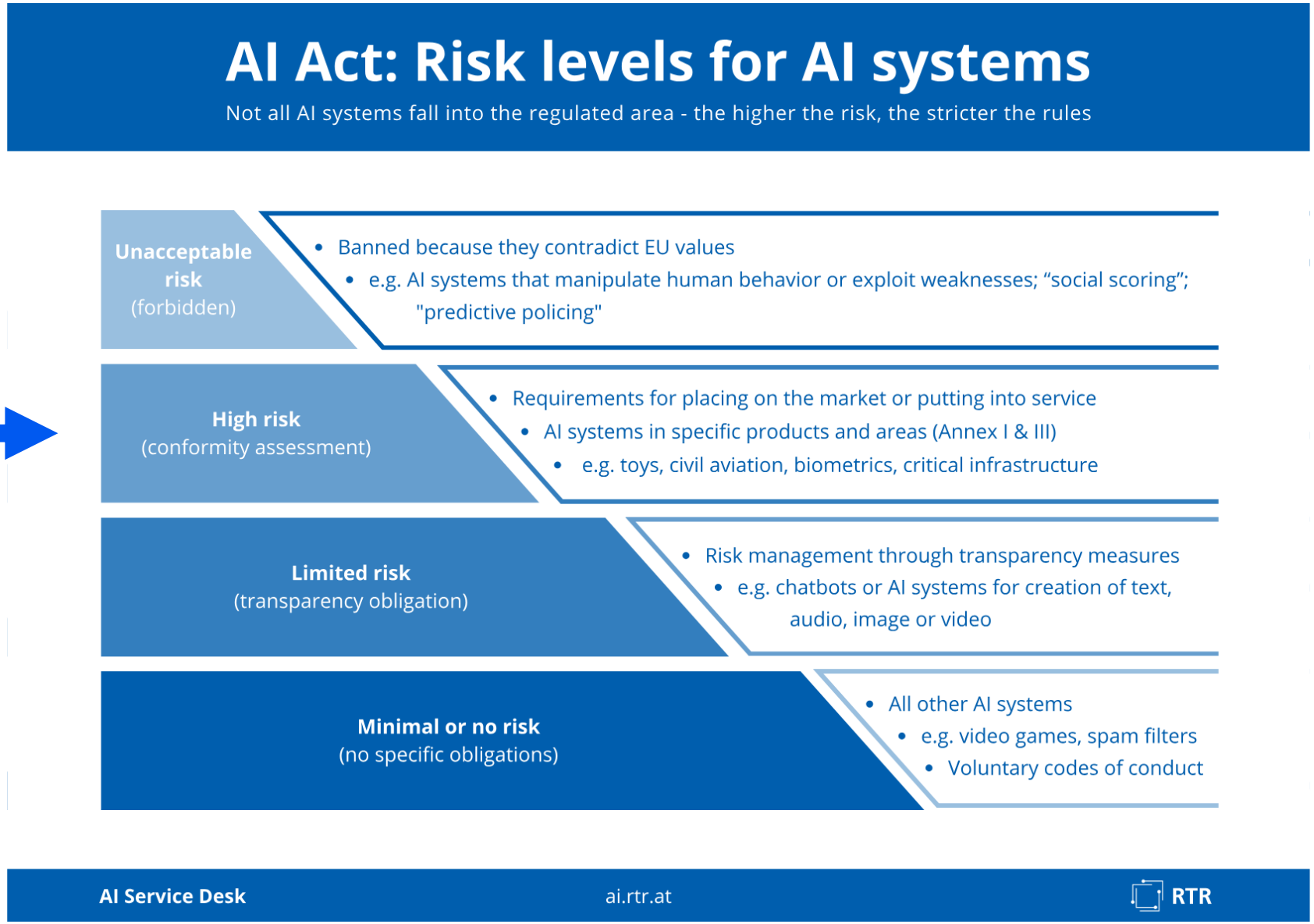
Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Risk levels of AI systems, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.en.html>.

Prohibited AI practices

- Subliminal **manipulation** with considerable damage
- **Exploiting** vulnerable groups of people
- **Social** scoring with negative impact
- **Profiling** to assess whether a crime will be committed
- Creation of databases for **facial recognition** from images from the Internet
- **Emotion recognition** in the workplace or in educational institutions
- **Biometric categorization** to obtain sensitive data
- **Remote biometric identification** (with strict exceptions for law enforcement purposes)

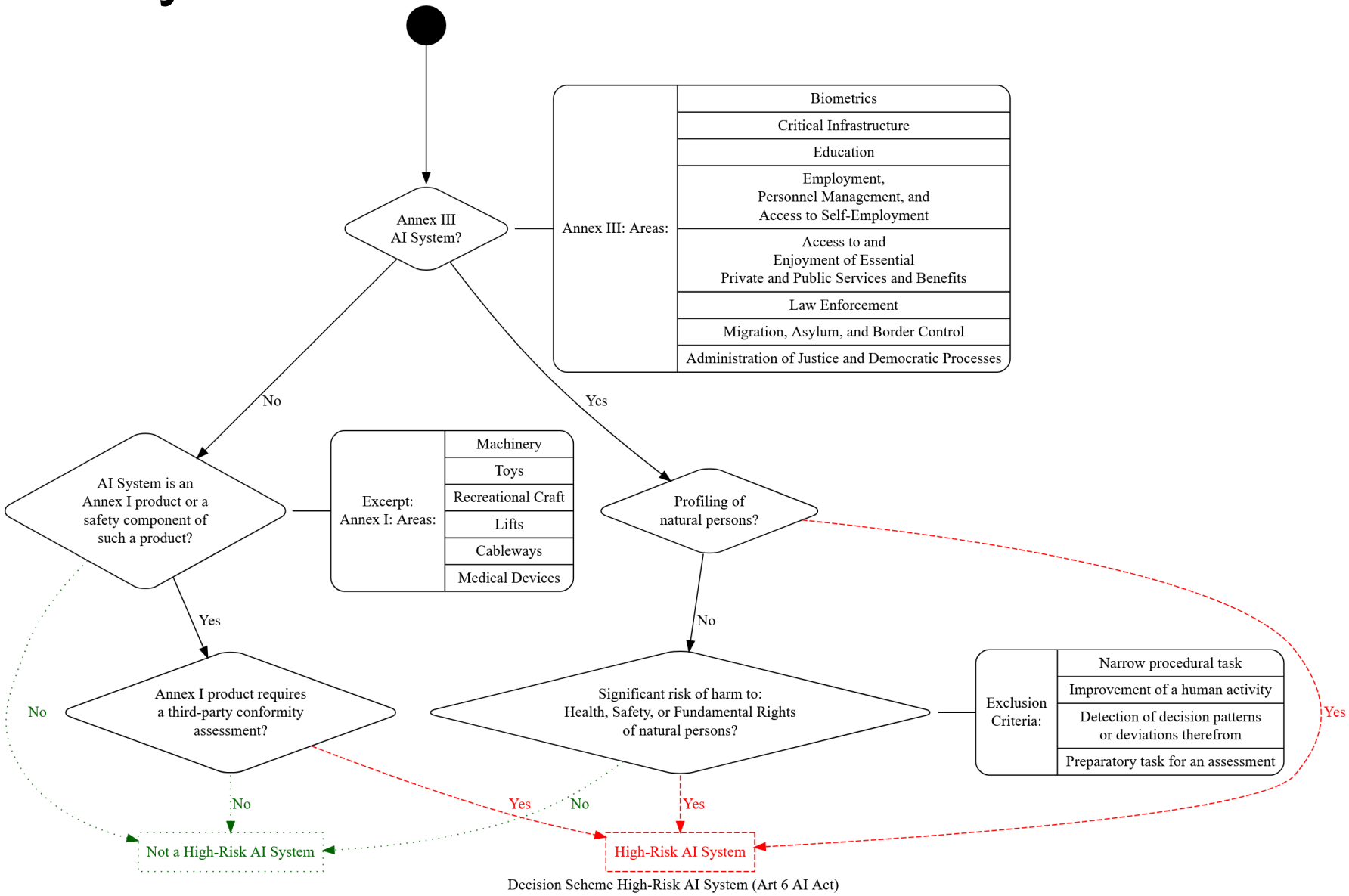
Art 5 AI-Act.

AI-Act Risk Levels



Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Risk levels of AI systems, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.en.html>.

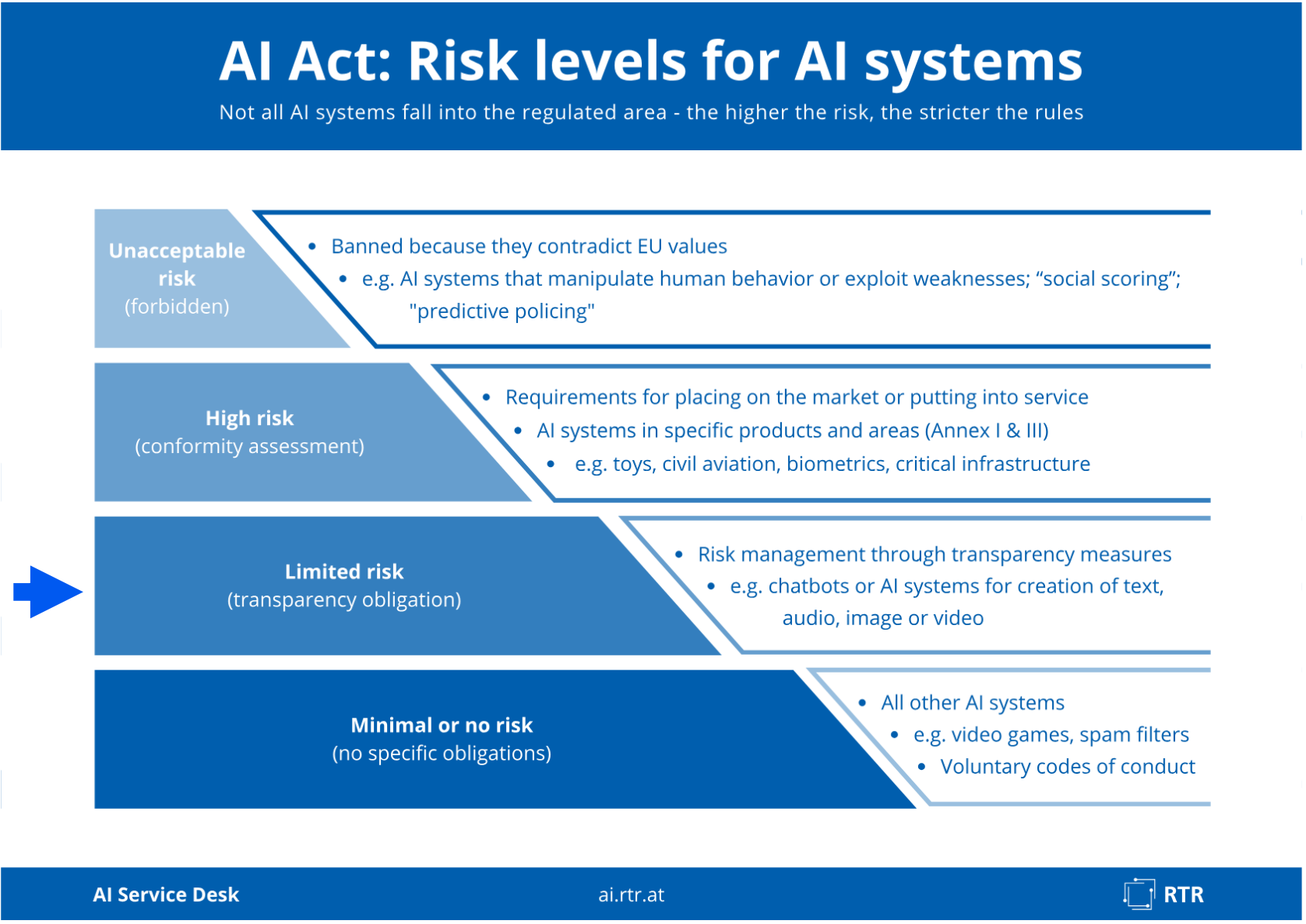
High-risk AI systems



Decision Scheme High-Risk AI System (Art 6 AI Act)

Art 6 AI-Act.

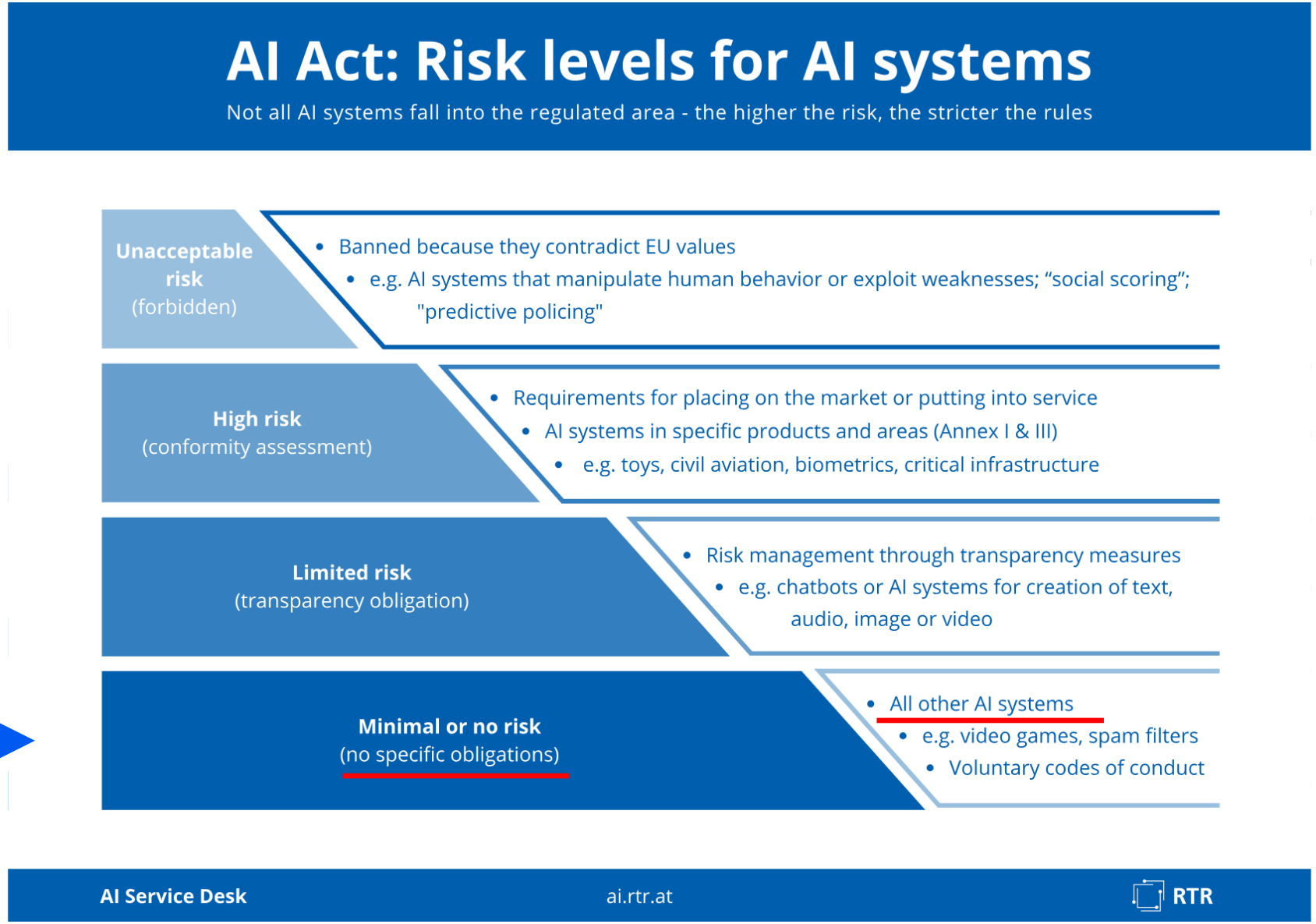
AI-Act Risk Levels



- AI Systems designed for direct interaction with natural persons
- AI Systems generating synthetic content/deep fakes
- Emotion recognition systems / biometric categorisation systems

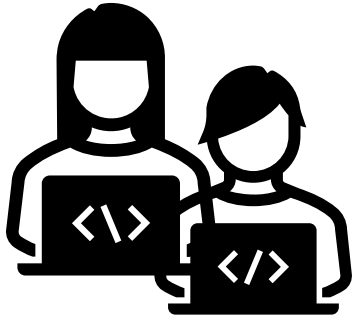
Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Risk levels of AI systems, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.en.html>.

AI-Act Risk Levels



Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Risk levels of AI systems, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.en.html>.

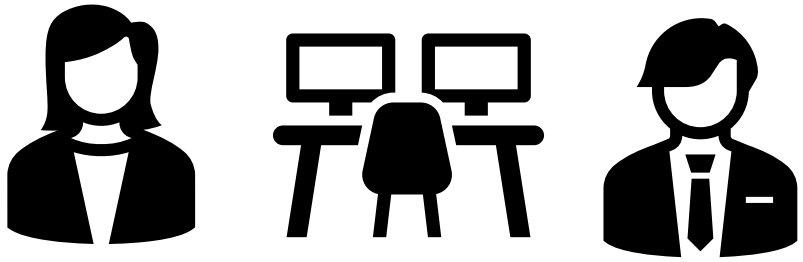
AI-Act Operators



Provider
develops an AI system (general-purpose AI model) **and**
places it on the market / puts the AI system into service

Art 3 Sec 3 AI-Act.

AI-Act Operators



Deployer
using an AI system under its authority

Art 3 Sec 4 AI-Act.

AI Act: Provider obligations

The scope of obligations decreases according to the risk classification of the AI system/AI model

	High risk AI system	GPAI model systemic risk	GPAI model	AI system limited risk	AI system minimal risk
AI literacy	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 13	Art. 55 (1)	Art. 53 (1) b	Art. 50 (1), (2)	
Data requirements	Art. 10	Art. 55 (1)	Art. 53 (1) c, d		
Technical documentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Cooperation with authorities	Art. 21	Art. 55 (1)	Art. 53 (3)		
Appointment of authorized representative (if third country)	Art. 22	Art. 55 (1)	Art. 54		
Risk management	Art. 9	Art. 55 (1) a, b			
Accuracy, robustness and cybersecurity	Art. 15	Art. 55 (1) d			
Registration resp. notification obligations	Art. 49	Art. 52 (1)			
Reporting obligations to authorities	Art. 73	Art. 55 (1) c			
Record-keeping	Art. 12				
Implementation of human oversight tools	Art. 14				
Labelling requirements	Art. 16 b				
Ensuring accessibility requirements	Art. 16 l				
Quality management	Art. 17				
Documentation and log-keeping	Art. 18, 19				
Corrective actions	Art. 20				
Conformity assessment procedure, -declaration, -marking	Art. 43, 47, 48				

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Provider obligations in the AI Act, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html>.

AI Act: Deployer obligations

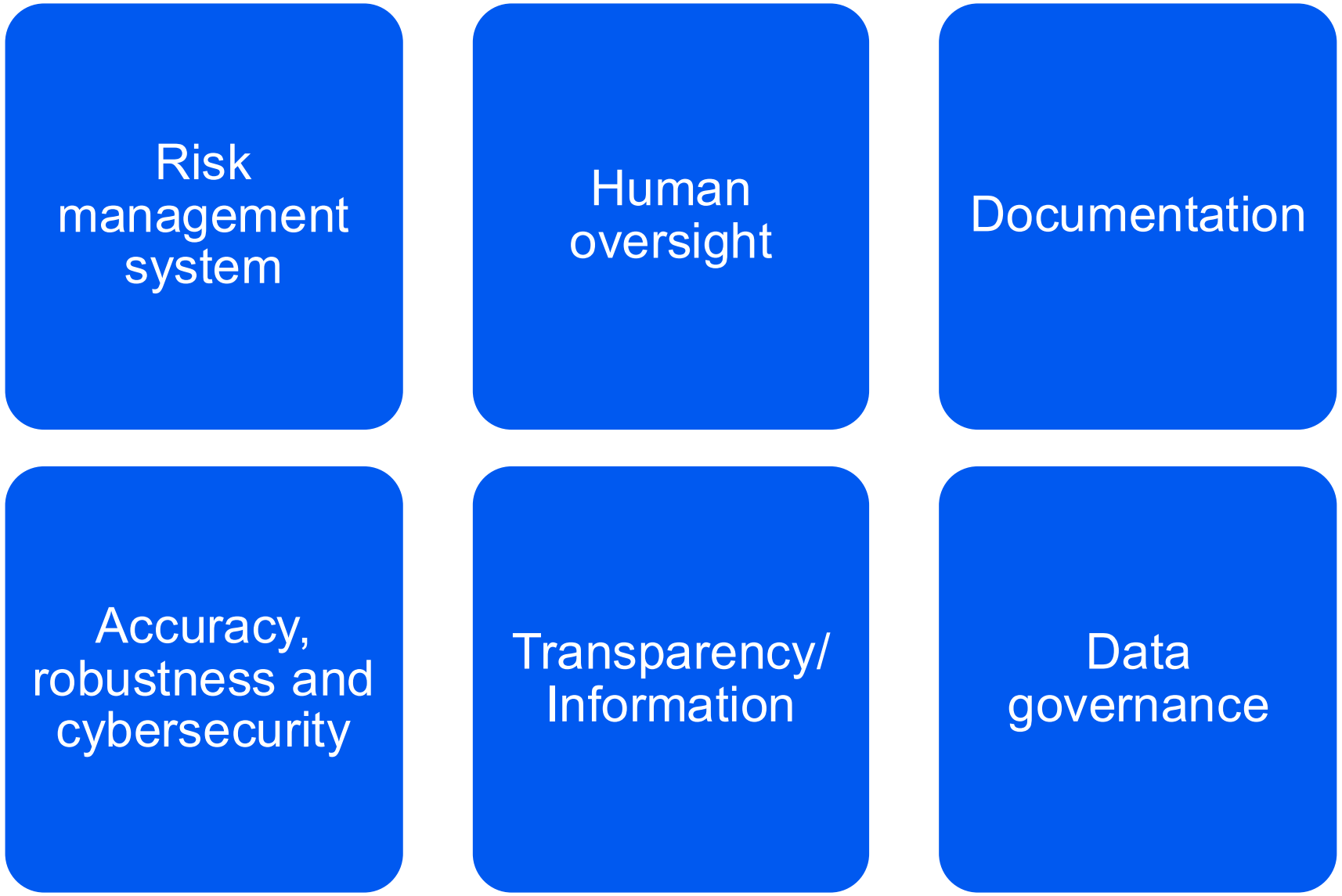
The scope of obligations decreases according to the risk classification of the AI system

	High risk AI system	AI system limited risk	AI System minimal risk
AI literacy	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 26 (11)	Art. 50 (3), (4)	
Use of the AI system according to the instructions for use	Art. 26 (1), (3), (4)		
Human oversight	Art. 26 (2)		
Monitoring of the AI system	Art. 26 (5)		
Reporting of serious incidents	Art. 26 (5), 73		
Record-keeping	Art. 26 (6)		
Where relevant, data protection impact assessment	Art. 26 (9)		
Cooperation with competent national authorities	Art. 26 (12)		
Right to explanation of individual decision-making	Art. 86 (1)		
Information towards employee representatives *if employer uses high-risk AI systems in the workplace*	Art. 26 (7)		
Registration obligations *if EU institutions, EU bodies and other EU agencies*	Art. 26 (8), 49		
Authorisation by a judicial or administrative authorithy *if AI-system is used for post-remote biometric identification*	Art. 26 (10)		
Fundamental rights impact assessment *if i.a. public bodies and private entities provide public services*	Art. 27		

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), AI Act: Deployer Obligations, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Deployer_obligations.en.html>.

Requirements for high-risk AI systems



Art 8 - 15 AI-Act.

AI Act: Provider obligations

The scope of obligations decreases according to the risk classification of the AI system/AI model

	High risk AI system	GPAI model systemic risk	GPAI model	AI system limited risk	AI system minimal risk
AI literacy	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 13	Art. 55 (1)	Art. 53 (1) b	Art. 50 (1), (2)	
Data requirements	Art. 10	Art. 55 (1)	Art. 53 (1) c, d		
Technical documentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Cooperation with authorities	Art. 21	Art. 55 (1)	Art. 53 (3)		
Appointment of authorized representative (if third country)	Art. 22	Art. 55 (1)	Art. 54		
Risk management	Art. 9	Art. 55 (1) a, b			
Accuracy, robustness and cybersecurity	Art. 15	Art. 55 (1) d			
Registration resp. notification obligations	Art. 49	Art. 52 (1)			
Reporting obligations to authorities	Art. 73	Art. 55 (1) c			
Record-keeping	Art. 12				
Implementation of human oversight tools	Art. 14				
Labelling requirements	Art. 16 b				
Ensuring accessibility requirements	Art. 16 l				
Quality management	Art. 17				
Documentation and log-keeping	Art. 18, 19				
Corrective actions	Art. 20				
Conformity assessment procedure, -declaration, -marking	Art. 43, 47, 48				

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Provider obligations in the AI Act, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html>.

AI Act: Deployer obligations

The scope of obligations decreases according to the risk classification of the AI system

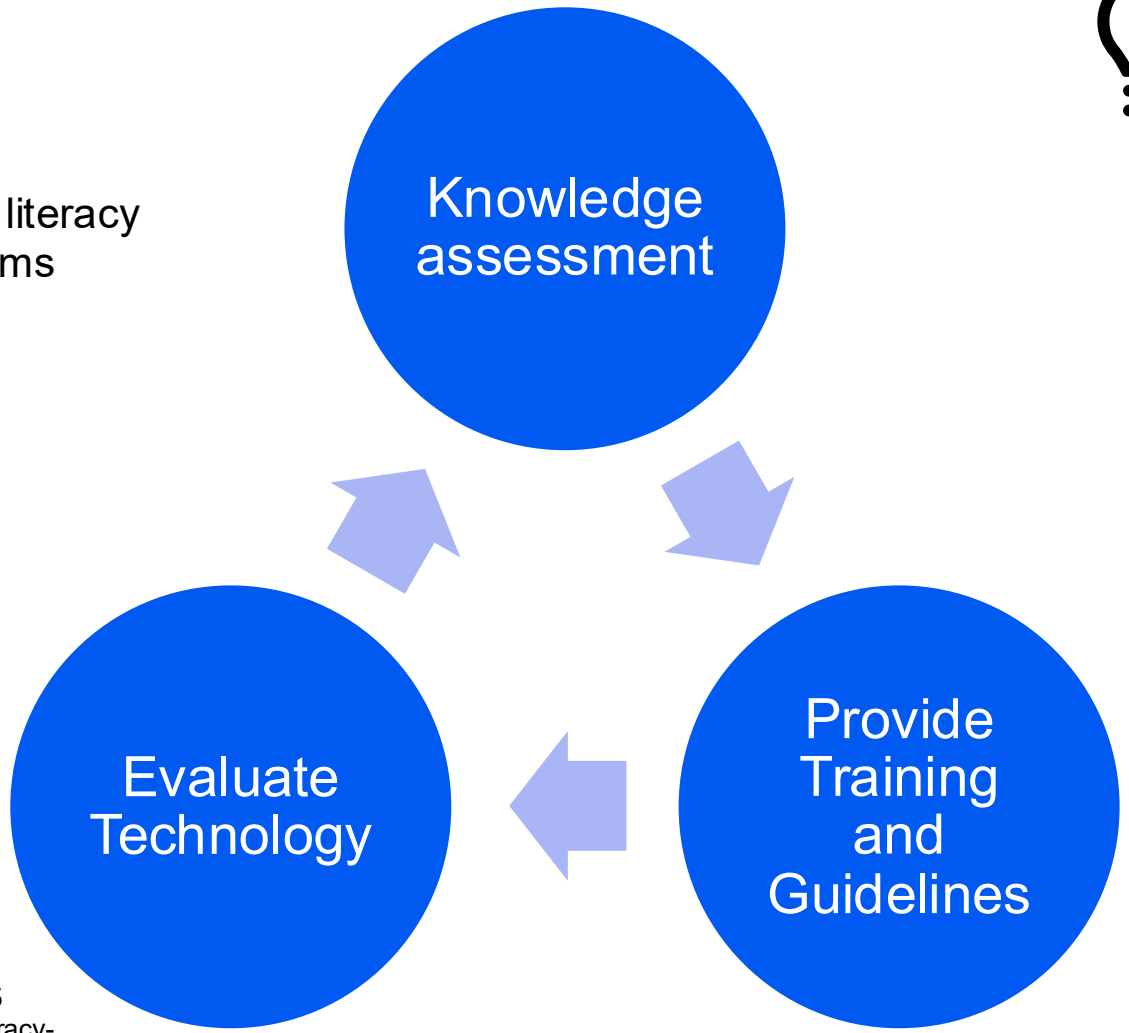
	High risk AI system	AI system limited risk	AI System minimal risk
AI literacy	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 26 (11)	Art. 50 (3), (4)	
Use of the AI system according to the instructions for use	Art. 26 (1), (3), (4)		
Human oversight	Art. 26 (2)		
Monitoring of the AI system	Art. 26 (5)		
Reporting of serious incidents	Art. 26 (5), 73		
Record-keeping	Art. 26 (6)		
Where relevant, data protection impact assessment	Art. 26 (9)		
Cooperation with competent national authorities	Art. 26 (12)		
Right to explanation of individual decision-making	Art. 86 (1)		
Information towards employee representatives *if employer uses high-risk AI systems in the workplace*	Art. 26 (7)		
Registration obligations *if EU institutions, EU bodies and other EU agencies*	Art. 26 (8), 49		
Authorisation by a judicial or administrative authority *if AI-system is used for post-remote biometric identification*	Art. 26 (10)		
Fundamental rights impact assessment *if i.a. public bodies and private entities provide public services*	Art. 27		

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), AI Act: Deployer Obligations, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Deployer_obligations.en.html>.

AI literacy – Providers and Deployers

- Ensure a sufficient level of AI literacy of persons operating AI systems
- Consider
  - technical knowledge,
  - experience,
  - education and
  - training.



See:
Living Repository of
AI Literacy Practices for examples[1]

- Purpose and limitations of the System;
- How to use it (how to prompt);
- Do's and Dont's;
- Ethics
- awareness about risks / possible harm

EC, AI Literacy - Questions & Answers, 18.08.2025 <https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>.

1: *EC*, Living repository to foster learning and exchange on AI literacy, <https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy>.

Rappenglück/Vonthien, RDi 2025, 398.

Art 3 Num 56 , Art 4 AI-Act.

AI Act: Provider obligations

The scope of obligations decreases according to the risk classification of the AI system/AI model

	High risk AI system	GPAI model systemic risk	GPAI model	AI system limited risk	AI system minimal risk
AI literacy	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 13	Art. 55 (1)	Art. 53 (1) b	Art. 50 (1), (2)	
Data requirements	Art. 10	Art. 55 (1)	Art. 53 (1) c		
Technical documentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Cooperation with authorities	Art. 21	Art. 55 (1)	Art. 53 (3)		
Appointment of authorized representative (if third country)	Art. 22	Art. 55 (1)	Art. 54		
Risk management	Art. 9	Art. 55 (1) a, b			
Accuracy, robustness and cybersecurity	Art. 15	Art. 55 (1) d			
Registration resp. notification obligations	Art. 49	Art. 52 (1)			
Reporting obligations to authorities	Art. 73	Art. 55 (1) c			
Record-keeping	Art. 12				
Implementation of human oversight tools	Art. 14				
Labelling requirements	Art. 16 b				
Ensuring accessibility requirements	Art. 16 l				
Quality management	Art. 17				
Documentation and log-keeping	Art. 18, 19				
Corrective actions	Art. 20				
Conformity assessment procedure, -declaration, -marking	Art. 43, 47, 48				

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Provider obligations in the AI Act, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html>.

AI Act: Deployer obligations

The scope of obligations decreases according to the risk classification of the AI system

	High risk AI system	AI system limited risk	AI System minimal risk
AI literacy	Art. 4		Art. 4
Transparency towards downstream actors	Art. 26 (11)	Art. 50 (3), (4)	
Use of the system according to the instructions for use	Art. 26 (1) (3) (4)		
Human oversight	Art. 26 (2)		
Monitoring of the AI system	Art. 26 (5)		
Reporting of serious incidents	Art. 26 (5), 73		
Record-keeping	Art. 26 (6)		
Where relevant, data protection impact assessment	Art. 26 (9)		
Cooperation with competent national authorities	Art. 26 (12)		
Right to explanation of individual decision-making	Art. 86 (1)		
Information towards employee representatives *if employer uses high-risk AI systems in the workplace*	Art. 26 (7)		
Registration obligations *if EU institutions, EU bodies and other EU agencies*	Art. 26 (8), 49		
Authorisation by a judicial or administrative authorithy *if AI-system is used for post-remote biometric identification*	Art. 26 (10)		
Fundamental rights impact assessment *if i.a. public bodies and private entities provide public services*	Art. 27		

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), AI Act: Deployer Obligations, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Deployer_obligations.en.html>.

Transparency – Providers and Deployers

Guidelines and Code of Practice on transparent AI systems

Providers:

- **Inform** about interaction with AI
- Generated audio, image, video or text must be **marked** as generated by AI

Deployers:

- **inform** about operation of emotion recognition system / biometric categorisation system
- **disclose** deep fakes
- **disclose** if text is generated by AI if it shall inform the public about matters of public interest

Art 50 AI-Act.

European Commission (EC), Guidelines and Code of Practice on transparent AI systems, <https://digital-strategy.ec.europa.eu/en/faqs/guidelines-and-code-practice-transparent-ai-systems>.

AI Act: Provider obligations

The scope of obligations decreases according to the risk classification of the AI system/AI model

	High risk AI system	GPAI model systemic risk	GPAI model	AI system limited risk	AI system minimal risk
AI literacy	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 13	Art. 55 (1)	Art. 53 (1) b	Art. 50 (1), (2)	
Data requirements	Art. 10	Art. 55 (1)	Art. 53 (1) c, d		
Technical documentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Cooperation with authorities	Art. 21	Art. 55 (1)	Art. 53 (3)		
Appointment of authorized representative (if third country)	Art. 22	Art. 55 (1)	Art. 54		
Risk management	Art. 9	Art. 55 (1) a, b			
Accuracy, robustness and cybersecurity	Art. 15	Art. 55 (1) d			
Registration resp. notification obligations	Art. 49	Art. 52 (1)			
Reporting obligations to authorities	Art. 73	Art. 55 (1) c			
Record-keeping					
Implementation of human oversight tools	Art. 14				
Labelling requirements					
Ensuring accessibility requirements	Art. 16 l				
Quality management	Art. 17				
Documentation and log-keeping	Art. 18, 19				
Corrective actions	Art. 20				
Conformity assessment procedure, -declaration, -marking	Art. 43, 47, 48				

AI Service Desk ai.rtr.at RTR

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Provider obligations in the AI Act, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html>.

AI Act: Deployer obligations

The scope of obligations decreases according to the risk classification of the AI system

	High risk AI system	AI system limited risk	AI System minimal risk
AI literacy	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 26 (11)	Art. 50 (3), (4)	
Use of the AI ... according to the instructions for use	...		
Human oversight	Art. 26 (2)		
... of the AI system	Art. 26 (5)		
Reporting of serious incidents	Art. 26 (5), 73		
Record-keeping	Art. 26 (6)		
Where relevant, data protection impact assessment	Art. 26 (9)		
Cooperation with competent national authorities	Art. 26 (12)		
Right to explanation of individual decision-making	Art. 86 (1)		
Information towards employee representatives *if employer uses high-risk AI systems in the workplace*	Art. 26 (7)		
Registration obligations *if EU institutions, EU bodies and other EU agencies*	Art. 26 (8), 49		
Authorisation by a judicial or administrative authorithy *if AI-system is used for post-remote biometric identification*	Art. 26 (10)		
Fundamental rights impact assessment *if i.a. public bodies and private entities provide public services*	Art. 27		

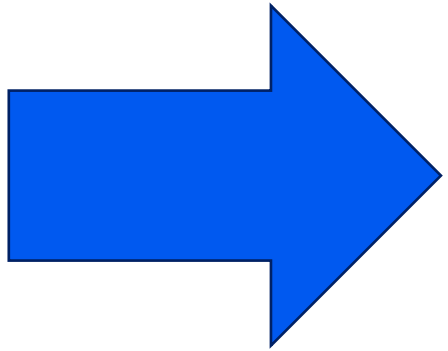
AI Service Desk ai.rtr.at RTR

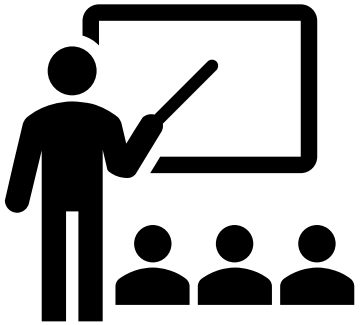
Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), AI Act: Deployer Obligations, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Deployer_obligations.en.html>.

Human oversight – Providers and Deployers (high-risk)

Humans:

- are aware of **automation bias**,
- correctly **interpret output,**
- **can decide** not to use AI System,
- interviene with/**stop** the AI System.

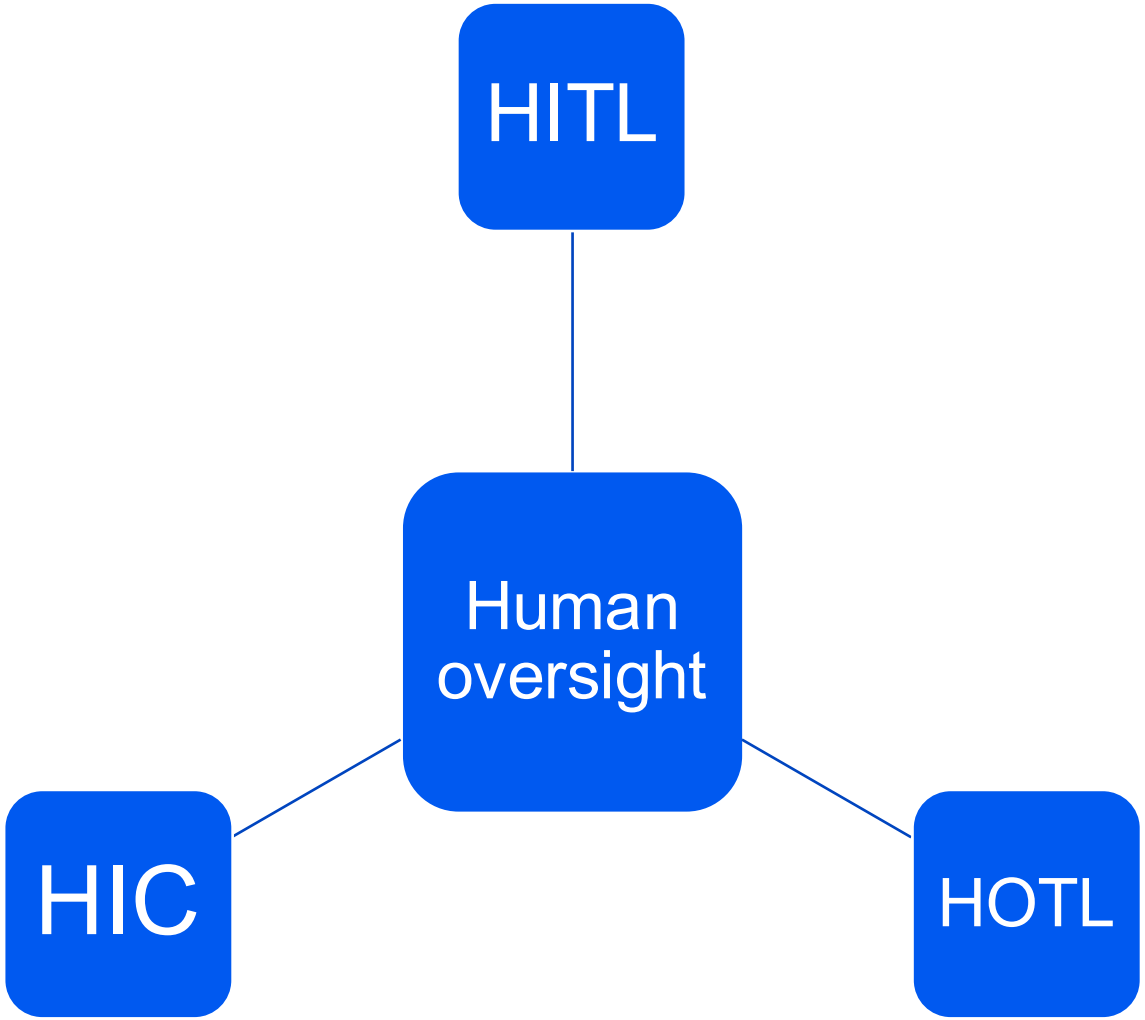




AI Literacy!

Art 14, 26 AI-Act.

Human oversight – Providers and Deployers (high-risk)



- Human-in-the-loop (**HITL**): capability for human intervention in every decision cycle of the system
- human-on-the-loop (**HOTL**): capability for human intervention during the design cycle of the system and monitoring the system's operation
- human-in-command (**HIC**): capability to oversee the overall activity of the AI system and the ability to decide when and how to use the system in any situation

High-Level Expert Group on Artificial Intelligence (HLEG), Ethics guidelines for trustworthy AI, 08.04.2019.

AI Act: Provider obligations

The scope of obligations decreases according to the risk classification of the AI system/AI model

	High risk AI system	**GPAI model** systemic risk	**GPAI model**	**AI system** limited risk	**AI system** minimal risk
AI literacy	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparency to downstream actors	Art. 13		Art. 53 (1) b	Art. 50 (1), (2)	
Data requirements	Art. 10	Art. 55 (1)	Art. 53 (1) c, d		
Technical documentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Cooperation with authorities	Art. 21	Art. 55 (1)	Art. 53 (3)		
Appointment of authorized representative (if third country)	Art. 22	Art. 55 (1)	Art. 54		
Risk management	Art. 9	Art. 55 (1) a, b			
Accuracy, robustness and cybersecurity	Art. 15	Art. 55 (1) d			
Registration resp. notification obligations	Art. 49	Art. 52 (1)			
Reporting obligations to authorities	Art. 73	Art. 55 (1) c			
Record-keeping	Art. 12				
Implementation of human oversight tools	Art. 14				
Labelling requirements	Art. 16 b				
Ensuring accessibility requirements	Art. 16 l				
Quality management	Art. 17				
Documentation and log-keeping	Art. 18, 19				
Corrective actions	Art. 20				
Conformity assessment procedure, -declaration, -marking	Art. 43, 47, 48				

AI Service Desk ai.rtr.at **RTR**

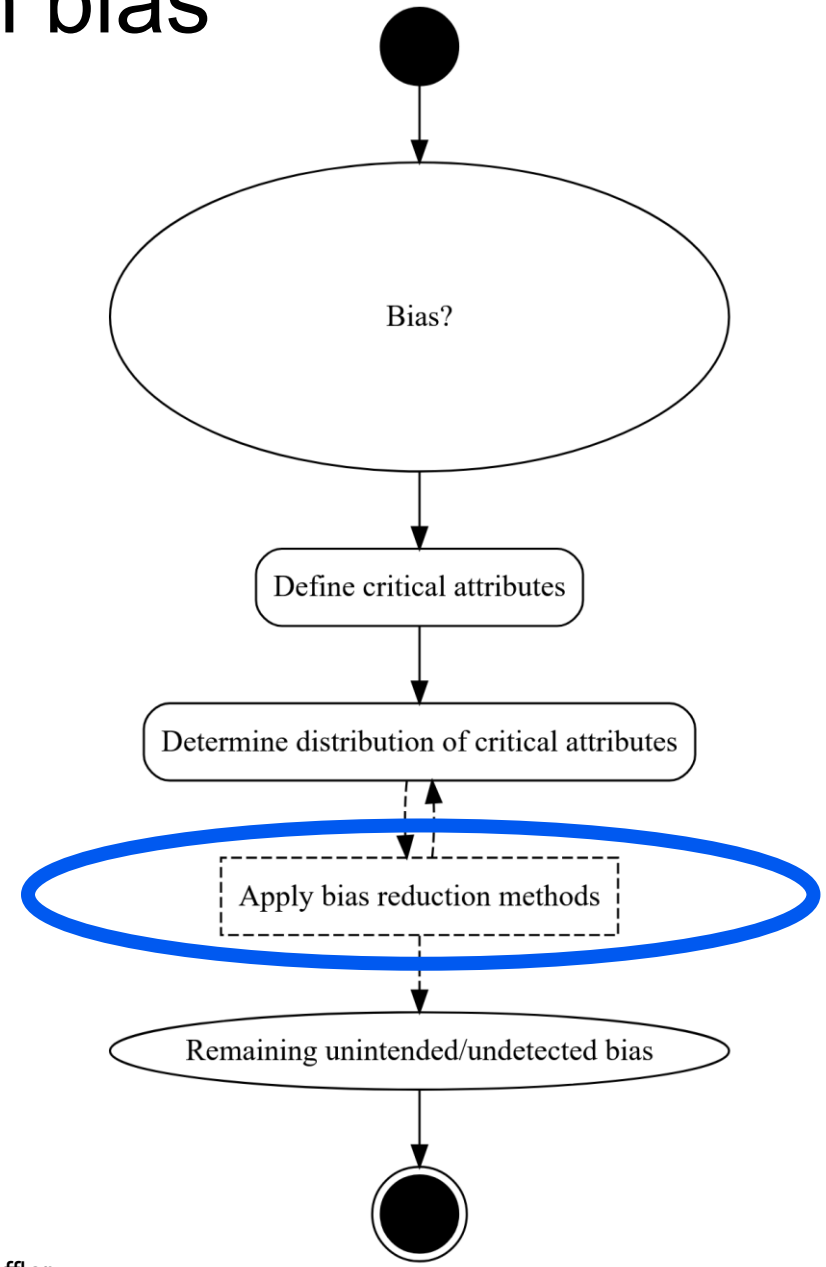
Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Provider obligations in the AI Act, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html>.

Data and data governance (Excerpt)

– Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used.

 Atari et al, Which Humans?, 22.09.2023.

The problem with bias



Identification and Reduction of Bias

Technical Documentation and documentation keeping (Excerpt)

- The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date. It must be clear and comprehensive!

- The details of the technical documentation are governed in Annex IV.
  - […]
  - A description of relevant changes made by the provider to the system through its lifecycle;
  - […]

- The provider shall, for a period ending 10 years after the high-risk AI system has been placed on the market or put into service, keep [i.a. the documentation] at the disposal of the national competent authorities.

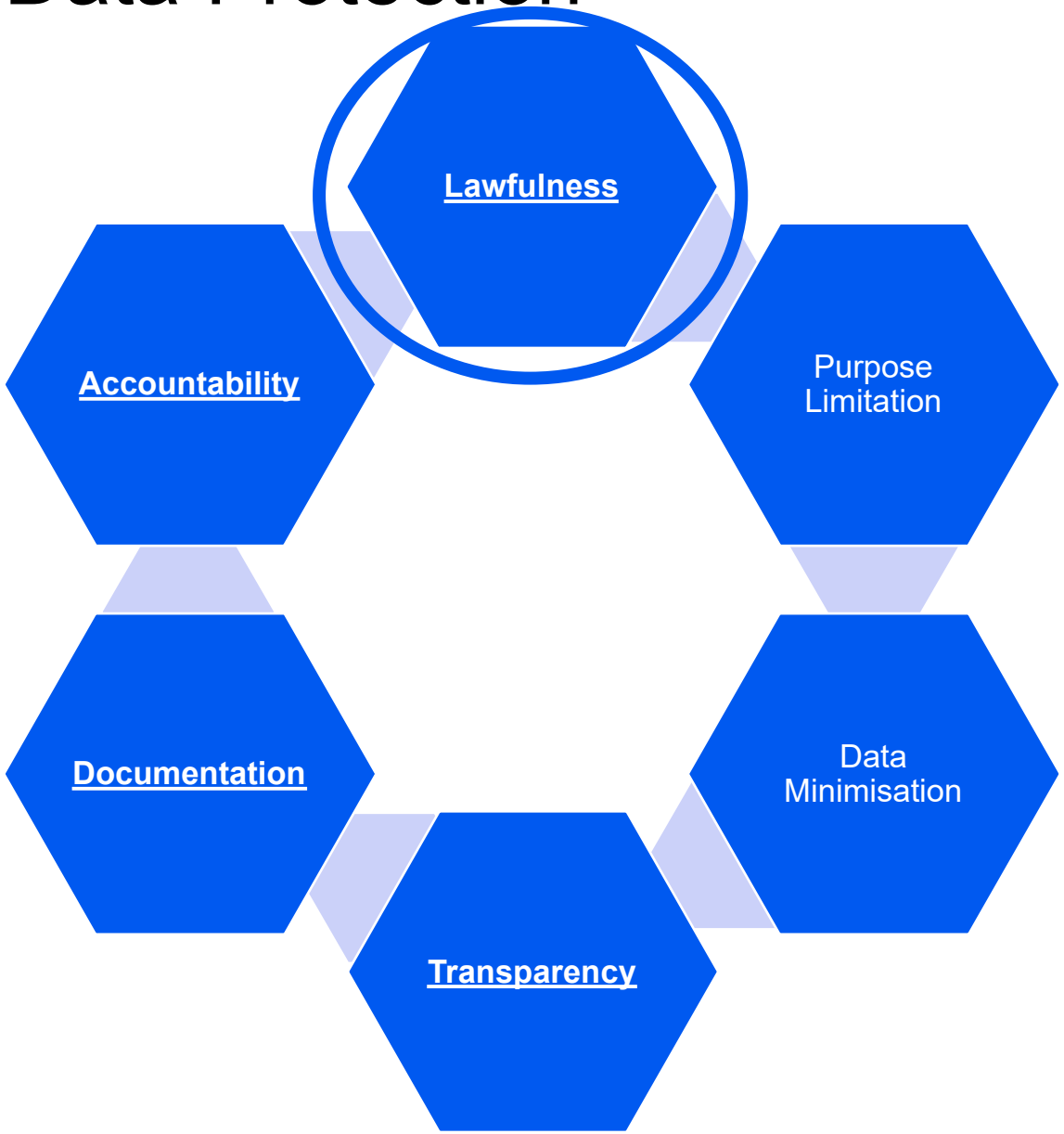
Technical Documentation GPAI (Excerpt)

Model Documentation Form	
How data was obtained and selected:	A description of the methods used to obtain and select training, testing, and validation data, including methods and resources used to annotate data, and models and methods used to generate synthetic data where applicable. For data previously obtained from third parties, a description of how the provider obtained the rights to the data if not already disclosed in the public summary of training data published in accordance with Article 53(1), point (d). *[Recommended 300 words]*
Measures to detect unsuitability of data sources:	A description of any methods implemented in data acquisition or processing, if any, to detect the presence of unsuitable data sources considering the model's intended uses, including but not limited to illegal content, child sexual abuse material (CSAM), non-consensual intimate imagery (NCII), and personal data leading to its unlawful processing. *[Recommended 400 words]*

 Oliver/Bommasani, Code of Practice for General-Purpose AI Models: Transparency Chapter, 10.07.2025.

Legal Landscape

Data Protection



Data protection law is characterized by the prohibition principle!

“Everything is forbidden unless it is exceptionally permitted.”

AI and Privacy

Processing shall be **lawful only** if:

- consent is provided

- processing is necessary for :
  - performance of a contract,
  - compliance with a legal obligation,
  - protect vital interests,
  - performance of a task carried out in the public interest/exercise of official authority,

- based on legitimate interests

Legitimate interests are **not** eligible, if special categories of data (e.g. health data) are processed!

In that case ?

- data made public by data subject (how to validate?),
- scientific research – if there is an Union or Member State law.

Facilitated AI training?

… in discussion!

Commission proposal (Digital Omnibus):

- Permission to use special categories of data (under certain conditions) for the development and operation of AI systems or the training of an AI model.
- The development of AI systems or the training of AI models should represent a legitimate interest (with certain restrictions) and be thus permitted.

What about AI Models that were (already) trained with personal data?

- As of now there is no prevailing opinion on the “lawfullnes” of such AI Models.[1]

1: *Specht-Riemenschneider/Bortnikov/Steffens*, Keine „Fruit of the poisonous KI “-Doktrin im Datenschutzrecht, KIR 2025, 213. *Datenschutzkonferenz*, Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode, 10.2025.

AI and Privacy

General Data Protection Regulation **applies** to personal data processed in connection with AI!

AI-Act:	Data governance	Documentation	Transparency/ Information	Human oversight	[…]
GDPR:	Processing principles	Documentation	Transparency/ Information	Data protection officer	[…]

Bausewein, Synergiepotenziale zwischen DSGVO und KI-VO für KI-System-Betreiber, Datenschutz und Datensicherheit - DuD 2025, 293–296.

Data Protection Guide

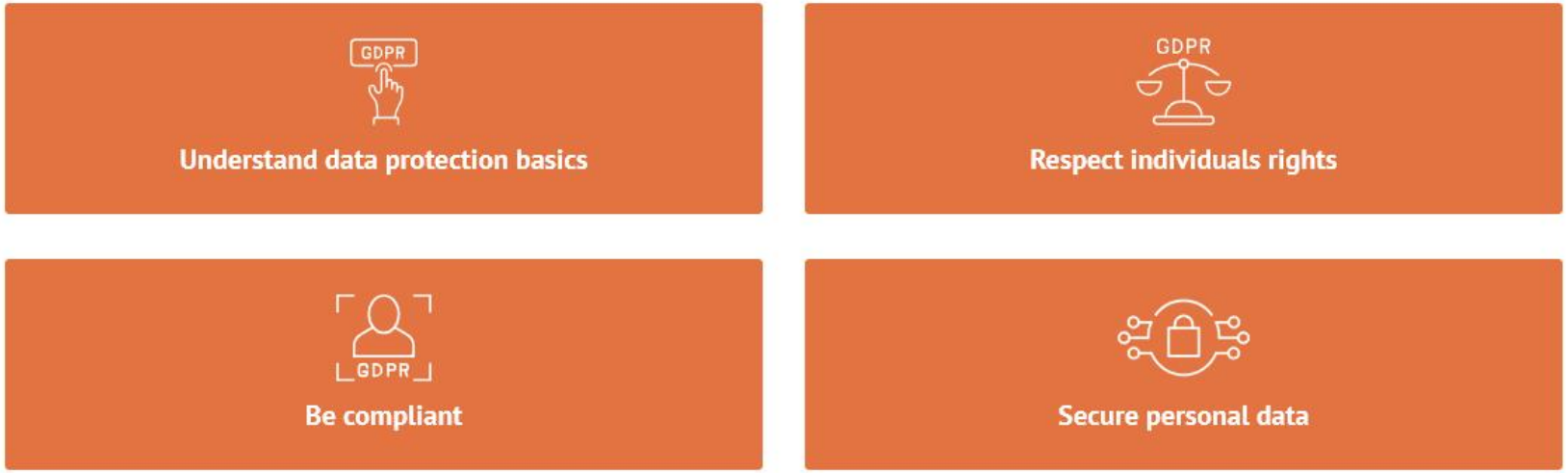
Luckily, there is extensive guidance available how to comply with the GDPR!

The EDPB data protection guide for small business

Are you unsure how to comply with GDPR?

Do you process personal data about your staff, consumers, and business partners?

Do you want to understand data protection rights?



European Data Protection Board, The EDPB data protection guide for small business, <https://www.edpb.europa.eu/sme-data-protection-guide/home_en>.

Data Protection Guide

Luckily, there is extensive guidance available how to comply with the GDPR!

Datenschutzbehörde, Ihre Pflichten als Verantwortliche:r, <https://dsb.gv.at/rechte-pflichten/ihre-pflichten-als-verantwortlicher>.

Stiftung Datenschutz, Datenschutz für Kleinunternehmen, <https://ds-kleinunternehmen.de/startseite>.

Legal Landscape

Intellectual Property Rights - Basic concepts

- IPR typically refer to ©, patents, trademarks, industrial designs and geographical indications
- ‘property’
  - ownership
  - utilization – economic value
- subject of IPR is the ‘work’, the ‘creation’
- entitlement to the ‘author’, to the ‘creator’

Expression vs. Ideas

- © protects
- not the ideas,
- nor their style,
- nor their content, but
- ***form of expression***

Common Law - © Vs civil law - authors' rights

- Authors' rights - part of copyright law (French term droit d'auteur, German Urheberrecht)
- XVIII. century – both copyright (common law systems) and authors' rights (civil law systems) aimed to address the inequality in relations between authors and publishers, thus provide for a monopoly right granted to the author for a limited term
- both systems require certain level of creativity (US Feist v. Rural case; French and German copyright laws protect "works of the mind" („oeuvres de l'esprit"; „geistige Schöpfungen")
- civil law: strong link between the rights and the person of the author (but: software, advertisements) while protecting the moral rights of authors as an integral part of their personality
- common law jurisdictions: accept corporate ownership of copyright; the employer owns the copyright in work created by employees (while in civil law – employer was only granted an exclusive licence to the economic rights in work created by employees)

Relevance: AI providers typically NOT under civil law jurisdiction

‚Work' under © protection

"literary and artistic works" including *every production* in the literary, scientific and artistic domain, *whatever may be the mode or form of its expression* (Berne Convention Article 2 (1))

All literary, scientific and artistic creations that are

- **of individual and original nature**
- **derived from the intellectual activity of the author**

no regard for their quantitative, qualitative, or aesthetic characteristics or any judgment regarding the standard of creation.

Not protected are typically official texts of a legislative, administrative and legal nature and official translations of such texts.

Certain © protection is provided for diligence during the creation of a work - e.g. database rights – (neither creativity, nor originality is required – limited protection)

Copyright protection is obtained automatically without the need for registration or other formalities (voluntary registration of works – in many countries, these systems can help solve disputes over ownership or the creation of registration certificates

What kind of ‘rights’ does © provide?

Economic rights

- to authorize or prevent uses of the work
  - reproduction;
  - public performance;
  - recording;
  - broadcasting;
  - communication to the public (i.e. transmission via broadband networks);
  - translation; and
  - adaptation
- to receive remuneration for the use of the work

Moral rights - the non-economic interests of the author

- the right to claim authorship of a work – the right of paternity
- the right to oppose changes to a work that could harm the creator's reputation – the right integrity

The term of copyright protection

- Copyright
  - Economic rights: > 50 years after the creator's death – EU, US, etc.: 70 years
  - Moral rights: in Europe perpetual - not possible for authors to assign or waive their moral rights
- Related rights
  - 50 years after the performer's death
  - limited scope

International Legal Context: Copyright Treaties

WIPO World Intellectual Property Organization of the UN) administers 26 treaties including the WIPO Convention (1967)

- Paris Convention (1883)
- Berne Convention (1886)
- Brussels Convention
- Madrid Agreement (Indications of Source)
- Marrakesh VIP Treaty
- Nairobi Treaty
- Beijing Treaty on Audiovisual Performances
- Patent Law Treaty
- Phonograms Convention
- Rome Convention
- Singapore Treaty on the Law of Trademarks
- Trademark Law Treaty
- Washington Treaty
- WIPO Copyright Treaty (WCT)
- WIPO Performances and Phonograms Treaty (WPPT)

The EU copyright legislation

AI Factory Austria AI:AT - PUBLIC – Krisztina Rozgonyi

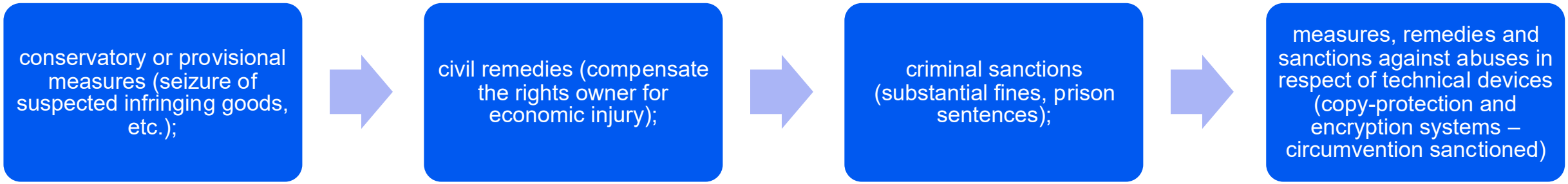
The EU copyright law consists of 13 directives and 2 regulations, harmonising the essential rights of authors, performers, producers and broadcasters

1. **Copyright in the Digital Single Market (DSM Directive) (2019)**
2. Directive on television and radio programmes (2019)
3. Regulation on cross-border portability of online content services (2017)
4. Management of Copyright and Related Rights (2014)
5. Orphan works (2012)
6. Rental and lending rights (2006)
7. Term of Protection (2011)
8. **Infosoc Directive (2011)**
9. Satellite and Cable (1993)
10. Resale right (2001)
11. Protection of Computer Programs (2009)
12. Protection of Databases (1966)
13. **E-Commerce** (2000)
14. Enforcement (2004)
15. Conditional Access Directive (1998)

Copyright Enforcement - Collective Management Organizations (CMOs)

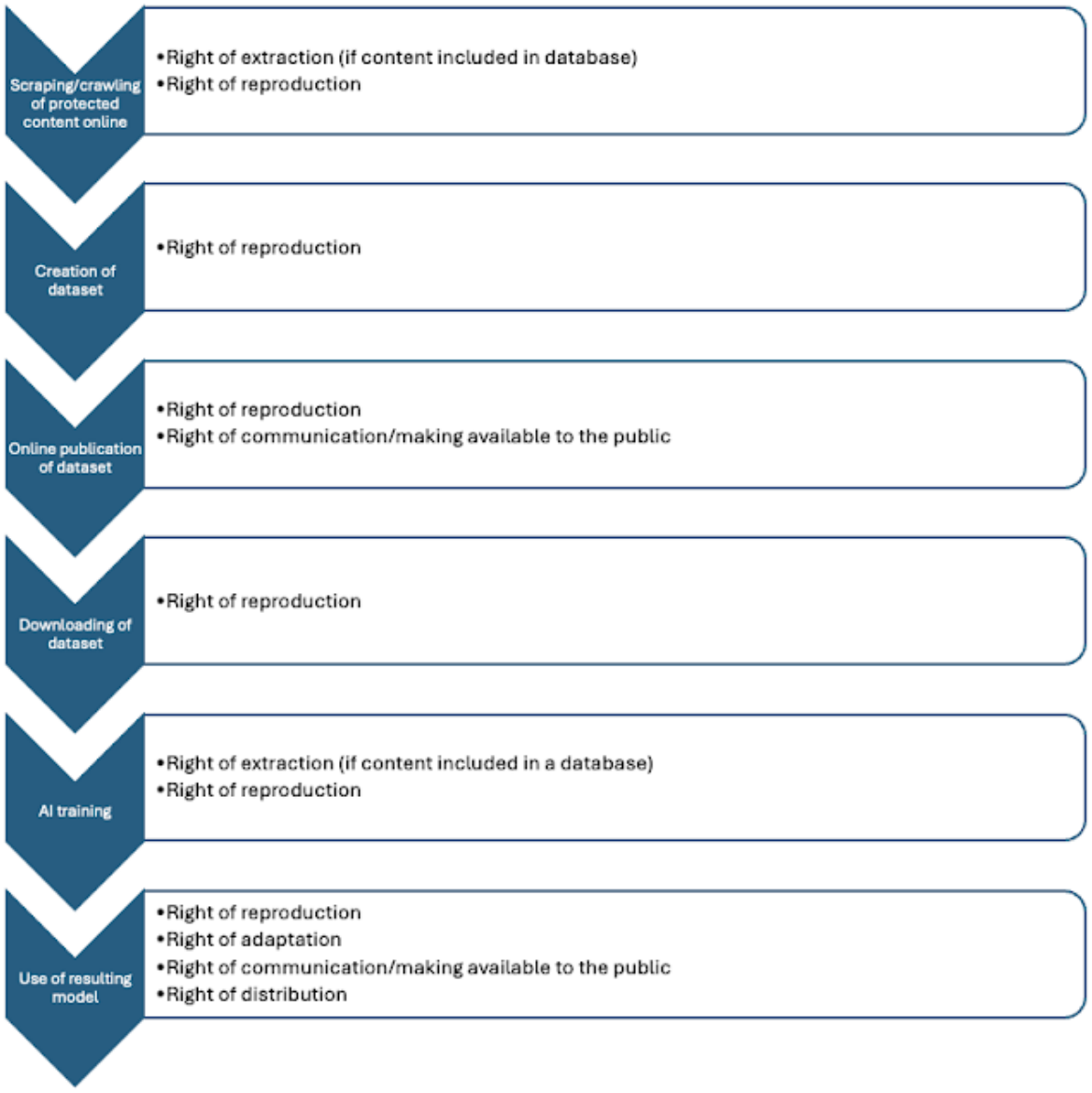
CMOs (on behalf of authors and other rightsholders) monitor uses of works+negotiating licenses +collecting remuneration+distributing to creators/copyright holders (typical: musical and literary works

Enforcement measures and sanctions



AI & Copyright – acts of use

(Rosati 2025)



AI & Copyright: Main issues under EU law

USING COPYRIGHT-PROTECTED WORKS TO TRAIN GENERATIVE AI (INPUT SIDE): Training of general-purpose AI

GenAI developers copy and store vast datasets

CDSM Directive's text and data mining (TDM) exceptions are misaligned with GenAI

Rightsholders received no compensation

LEGAL STATUS OF AI-GENERATED OUTPUTS (OUTPUT SIDE)

Human Authorship

AI-Assisted vs. AI-Generated

Creative Control Is the Threshold

AI & Input data

"Utilizing data for training purposes encompasses a comprehensive procedure of assimilating various forms of information, such as texts, images, and additional content, sourced from accessible platforms."

"This process may involve copying content, potentially violating copyright law’s exclusive reproduction rights."

(Lucchi 2024)

Data Mining

Data mining is the process, whereby software algorithms and statistical methods are utilized to spot trends and patterns within vast amounts of data, going beyond simple analysis.

„any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations”
(Art. 2 Directive on Copyright in the Digital Single Market [**DSM**] (2019/790)

- very broad definition
- covers all sorts of Natural Language Processing (NLP) applications

DSM includes 2 provisions allowing for **text and data mining (TDM) exceptions**

- **TDM for research (art. 3)**
- **TDM for other purposes (art. 4)**

TDM for scientific research (mandatory exception) - Art. 3 DSM

Beneficiaries

- research organisations
- cultural heritage institutions
- NO → institutions controlled by commercial undertakings

Purposes

- research on a non-profit basis
- public-interest mission
- public-private research partnerships

Permitted acts of use

- reproductions of copyright-protected works
- reproductions of subject matter of related rights
- extractions from databases

Requirement: "lawful access" to data source material

General TDM Exception (mandatory exception) – Art. 4 DSM

Beneficiaries: everyone (without restrictions)

Permitted acts:

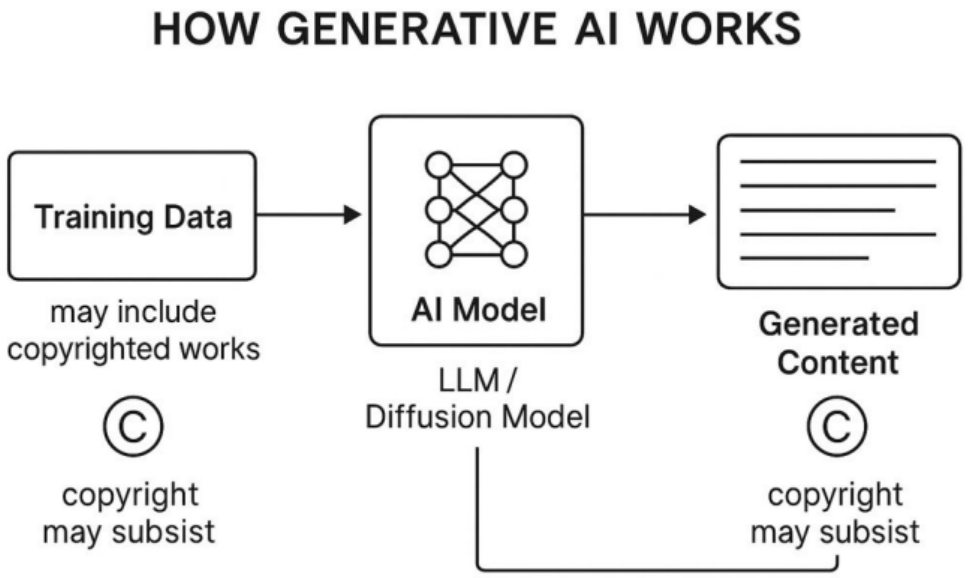
- reproductions of copyright-protected works
- reproductions of subject matter of related rights
- extractions from databases

Purpose: for any kind of purpose

Requirement: lawful access

Condition: *Mining allowed unless explicitly denied by rights holders (opt-out)*

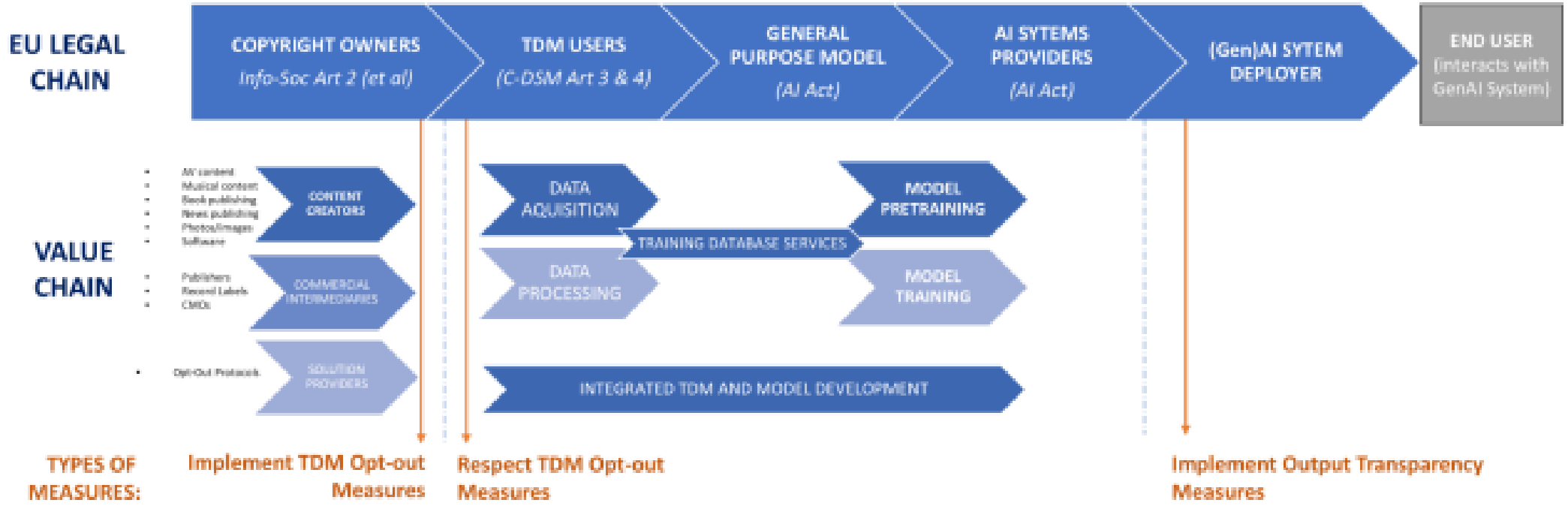
Generative AI & Copyright



(EP Study 2025, p. 20)

EU Legal Chain

(European Union Intellectual Property Office, 2025)

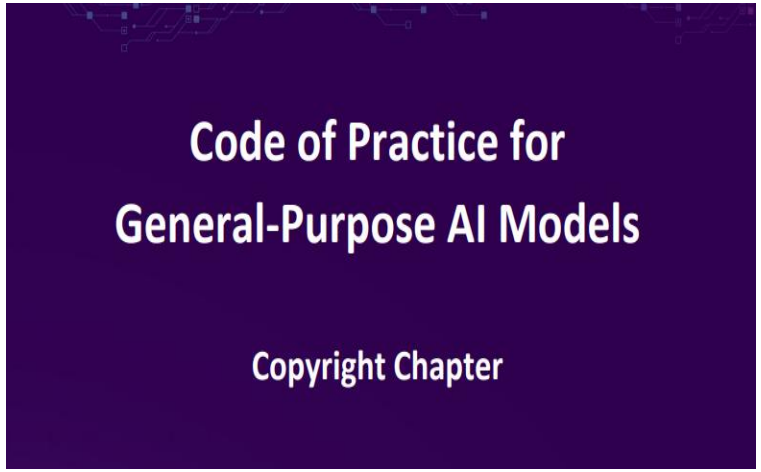


AI ACT & TDM

Obligations for providers of general-purpose AI models (Art. 53 1. (c), (d) AIA)

(c) put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790;

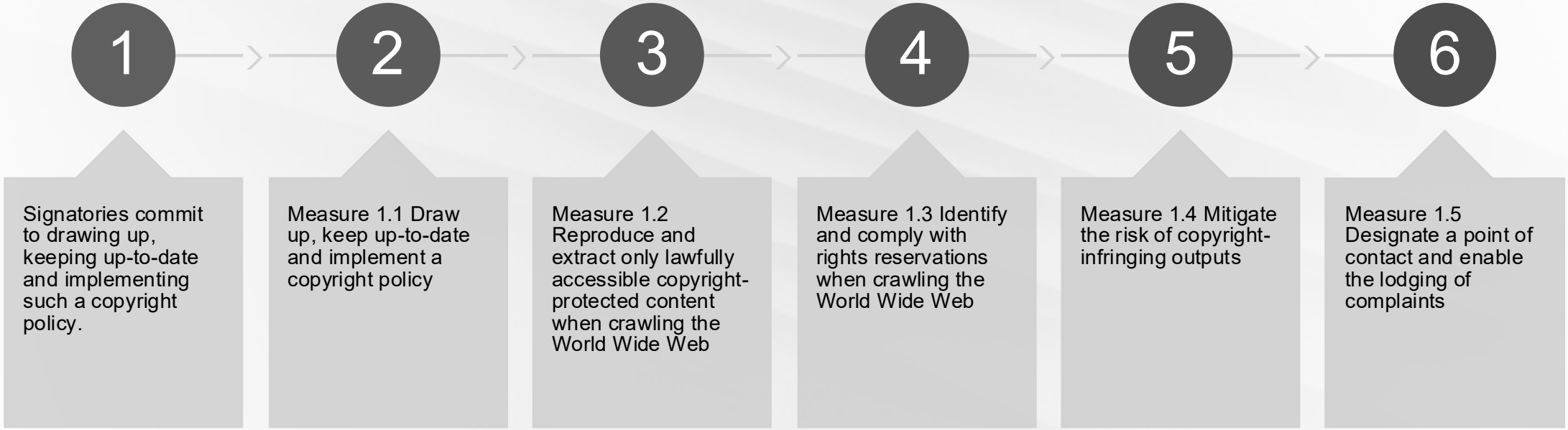
(d) draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.



Signatories of Code of Practice

- Accexible
- AI Alignment Solutions
- Aleph Alpha
- Almawave
- Amazon
- Anthropic
- Bria AI
- Cohere
- Cyber Institute
- Domyn
- Dweve
- Euc Inovação Portugal
- Fastweb
- Google
- Humane Technology
- IBM
- Lawise
- LINAGORA
- Microsoft
- Mistral AI
- Open Hippo
- OpenAI
- Pleias
- re-inventa
- ServiceNow
- Virtuo Turing
- WRITER

Commitment 1 Copyright policy



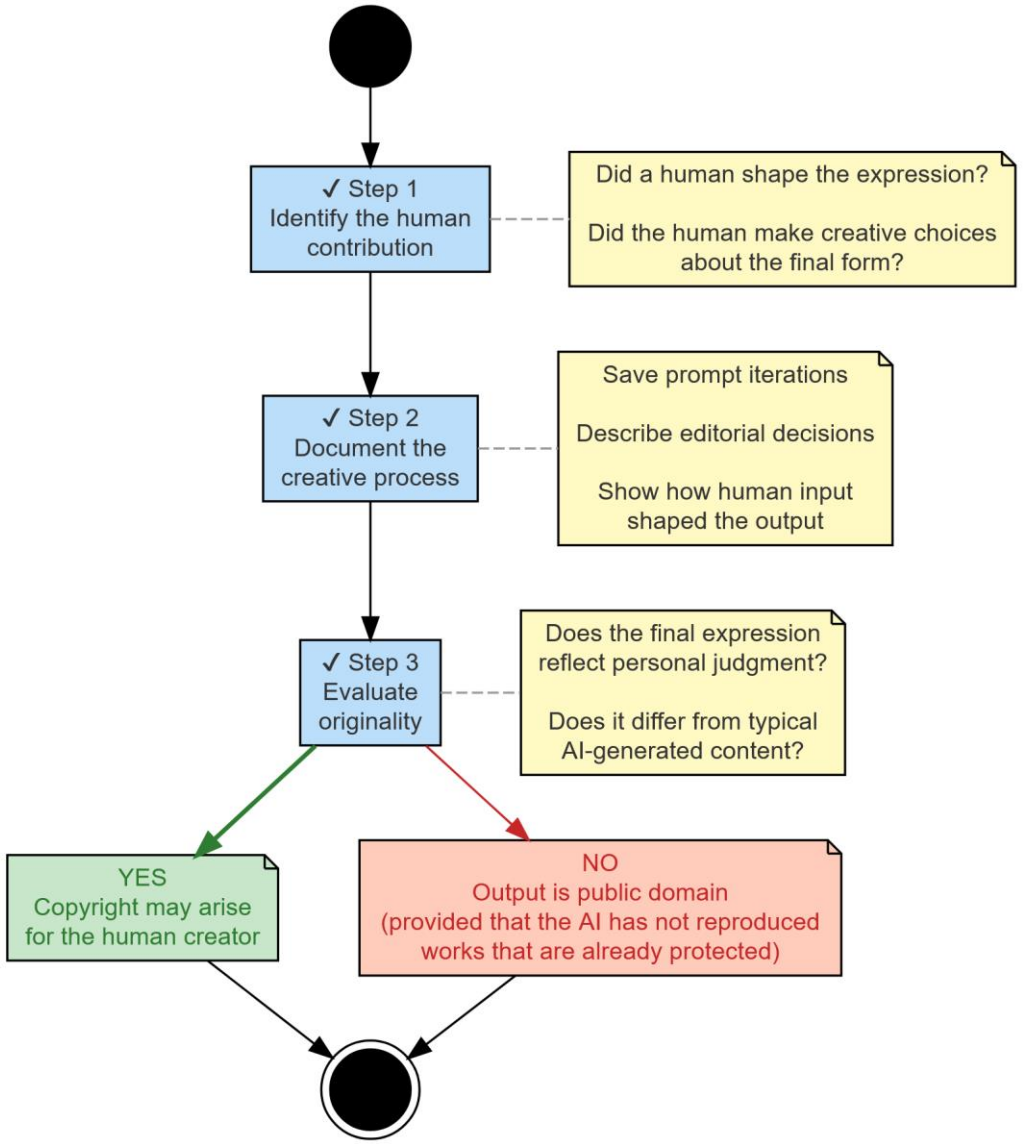
Opt-out from AI training use

- **Technical means:** e.g. Robots Exclusion Protocol (REP), TDMRep, digital watermarks, metadata standards such as C2PA or ISCC
- **Legal measures:** e.g. explicit terms of use on websites or license models with AI developers
- **Combination solutions:** Many rely on a mixture of technical and legal protection strategies

Evolving market for opt-out solutions

(See: European Commission Call for tenders EC-CNECT/2025/OP/0002 - Study to assess the feasibility of a central registry of Text and Data Mining opt-out expressed by rightsholders (2025))

Workflow: Determining Whether AI-Assisted Outputs Are Copyrightable



Generative Artificial Intelligence Output

- Human Authorship is Central
- AI-Assisted vs. AI-Generated
- No Copyright for Prompts Alone
- No Legal Recognition of AI as Author
- Creative Control Is the Threshold
- Style Is Not Protected, But Risks Remain
- No General Exception for AI Outputs infridgements

(Lucchi 2025)

The Human Element as the Legal Bedrock

- the extent of human control over generation;
- the presence of creative choices in editing, structuring, or curation;
- the use of judgment in selecting or combining generated material;
- the degree of revision or refinement applied

Legal disputes & Litigations (ongoing)

- GEMA v. OpenAI (Germany 2025)
- Like Company v. Google Ireland (CJEU Case C-250/25)
- Disney and Universal v. Midjourney (US District Court for the Central District of California)
- Warner Bros. Discovery v. Midjourney
- US Copyright class action against OpenAI (2023) (Tremblay P. and Awad M Tremblay P. and Awad M. v. . v. OpenAI INC. et al OpenAI INC. et al,, No. 3:23-cv-03223) No. 3:23-cv-03223

Conclusion

EU TDM Rules Limitations

- Less freedom than anticipated
- For-profit TDM activities require content owner permission due to Article 4's opt-out clause

Impact on European Innovators

- Puts EU AI creators, journalists, and researchers at a disadvantage if not mitigated i.e. new remuneration regimes

Need for Reevaluation

- Potential reconsideration of TDM rules to foster innovation and competitiveness in the EU?

(EP Study 2025)

AI Coypright & Ethics – cross-cutting issues

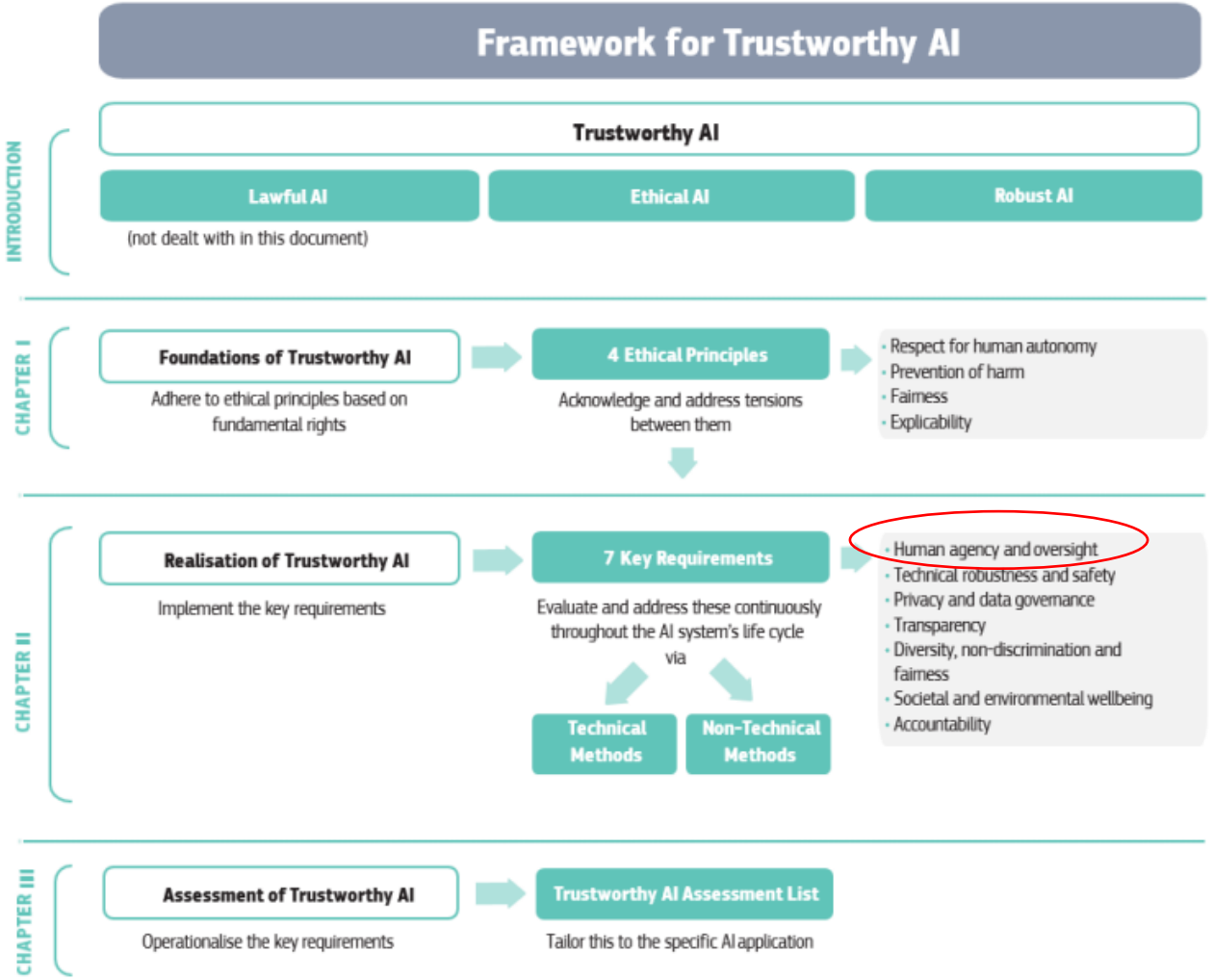


Figure 1: The Guidelines as a framework for Trustworthy AI

Contact

Michael Löffler

Lead Legal, Regulatory and Ethics
AI Factory Austria AI:AT

+43 664 88390692
michael.loeffler@ai-at.eu

Krisztina Rozgonyi DDr.

Senior Scientist, Legal and Policy
AI Factory Austria AI:AT

+43 664 78042372
krisztina.rozgonyi@ai-at.eu

AI Factory Austria AI:AT
Schwarzenbergplatz 2
1010 Wien, Austria

training@ai-at.eu
info@ai-at.eu

ai-at.eu

@ai-factory-austria

Funded by

under discussion with

EuroHPC
Joint Undertaking

Funded by
the European Union

Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

FFG
Promoting Innovation.

AI Factory Austria AI:AT has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101253078. The JU receives support from the Horizon Europe Programm of the European Union and Austria (BMIMI / FFG).