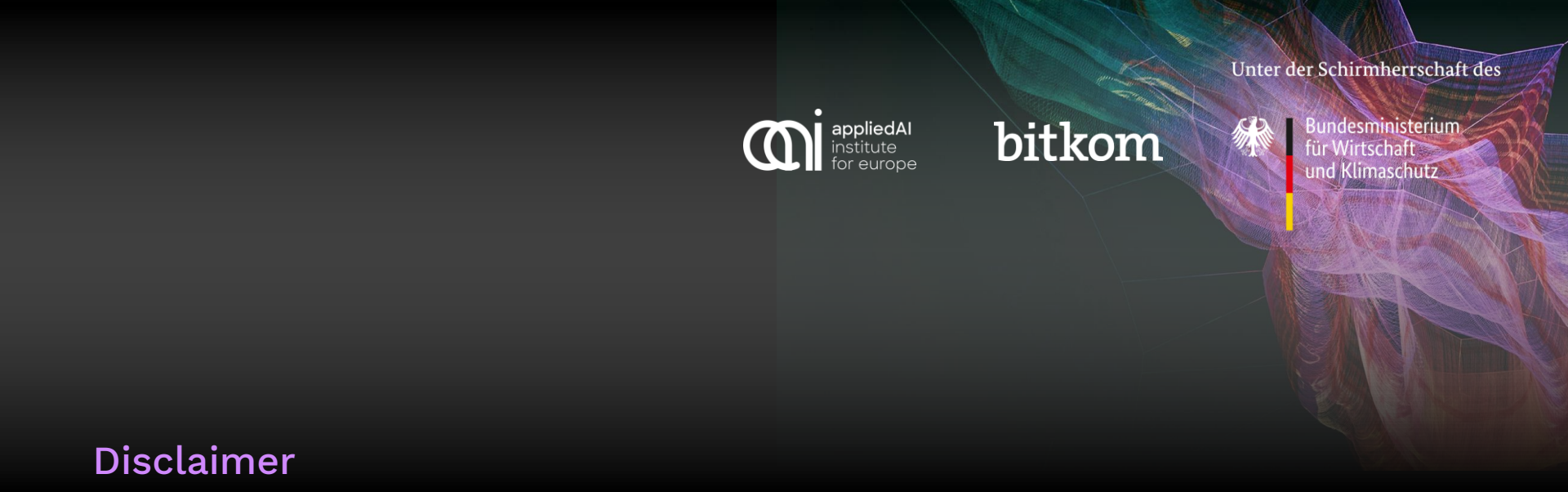
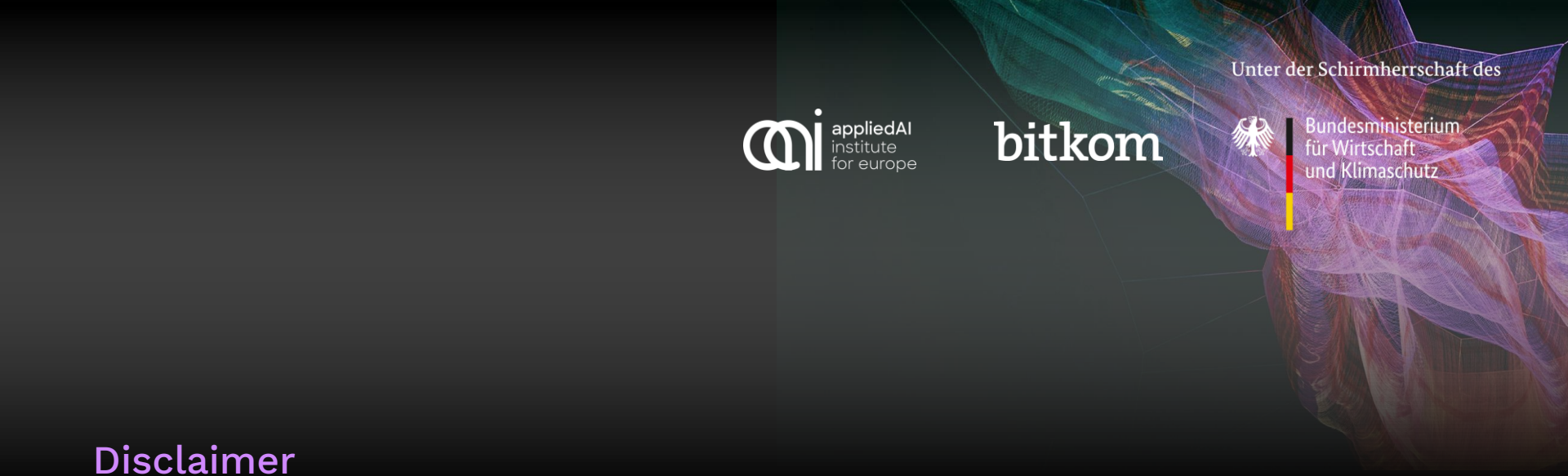

Unter der Schirmherrschaft des
appliedAI
institute
for europe
bitkom
Bundesministerium
für Wirtschaft
und Klimaschutz
AI Act Implementation Day
13. February 2025 - Munich



Disclaimer

By taking part in this event today you grant the event organizers full rights to use the images resulting from the photography/video filming, and any reproductions or adaptations of the images for publicity.

This might include (but is not limited to) the right to use them in their printed and online publicity, social media and press releases. Please contact us with any questions.



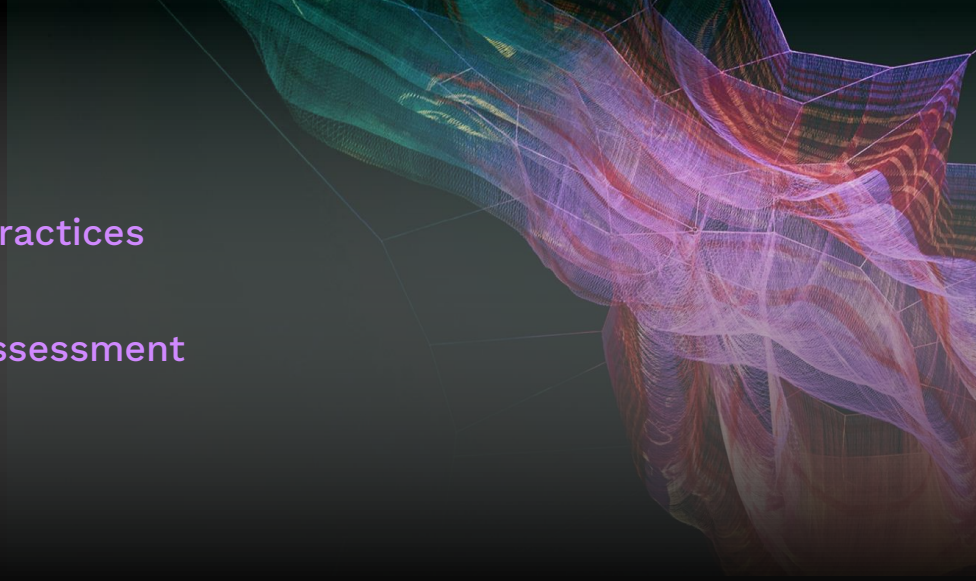
Disclaimer

A prerequisite for participation is **compliance with antitrust law**:
Section 1 of the German Act Against Restraints of Competition (GWB):
"Agreements between undertakings, decisions by associations of undertakings, and concerted practices that have as their object or effect the prevention, restriction, or distortion of competition are prohibited."

Program

08:30 am	Arrival & Registration
09:15 am	**Welcome & Opening** Susanne Dehmel - Bitkom Dr. Frauke Goll - appliedAI Institute for Europe Rebekka Weiß - Microsoft Deutschland
09:30 am	**Opening Keynote** Dr. Christoph Peylo - Robert Bosch GmbH
09:45 am	**Talk: Update on AI Act implementation streams** Sabrina Küspert - AI Office Evelyn Graß - German Federal Ministry for Economic Affairs and Climate Amelie Buss - DIN
10:45 am	**Coffee Break**

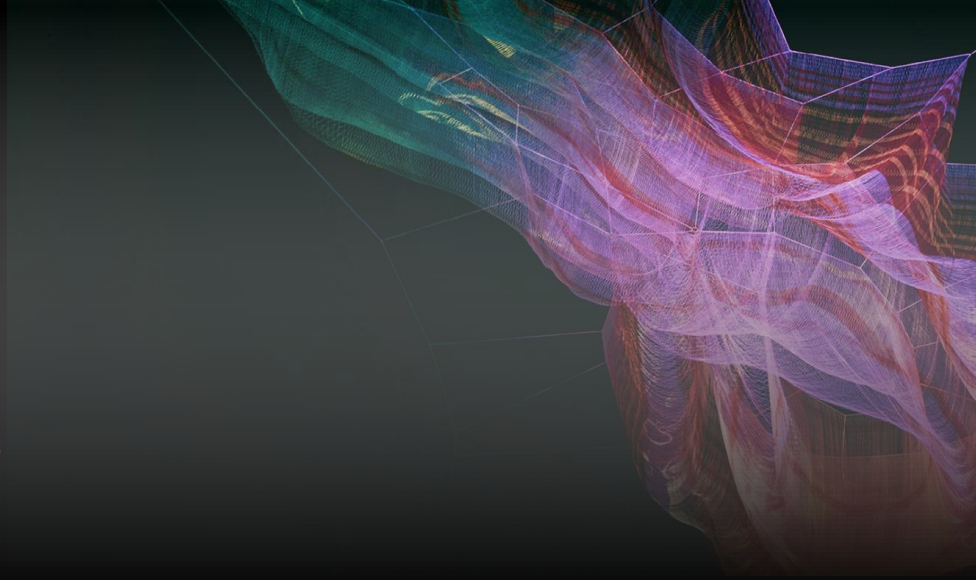
Program



11:00 am	**Talk: Insights into Prohibited Practices** Gabriele Mazzini - MIT Media Lab
11:30 am	**Panel: High-Risk Conformity Assessment** Maria Frantzi - European Central Bank Dr. Christoph Poetsch - TÜV AI.Lab Dr. Wolfgang Hildesheim - IBM
12:30 pm	**Lunch Break**
01:30 pm	**Panel: AI Value Chain & Responsibilities** Sebastian Dürdoth - Microsoft Deutschland GmbH Dr. Mathis Börner - SAP SE Prof. Boris Bauke - TH Aschaffenburg
02:30 pm	**Panel: Integration of AI Act Requirements in sectoral regulation** Prof. Dr. Sonja Zillner - Siemens AG Araceli Alcala - Carl Zeiss Dr. Florian Jell - Allianz

Program

03:30 pm	**Coffee Break**
03:45 pm	**Talk: GPAI Model Fine-tuning** Maximilian Kufner - BMW
04:05 pm	**Talk: Transparency Obligations** Tobias Kellner - Google Germany
04:25 pm	**Talk: AI Literacy** Paula Cippiere - Ada Learning
04:45 pm	**Closing Remarks** Susanne Dehmel - Bitkom Dr Till Klein - appliedAI Institute for Europe
05:00 pm	**Networking & Drinks (until 7pm)**



So many questions, So little time!

Share your questions
For networking and follow up activities.

menti.com
ID: 6332 3733

11:00 - 11:30 am

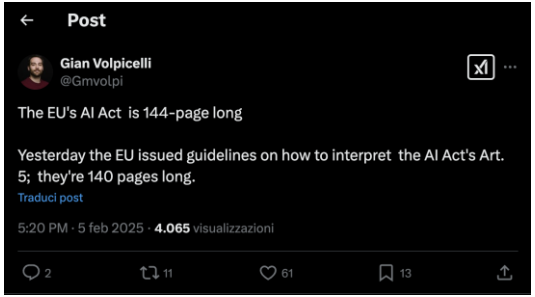
Insights into Prohibited Practices

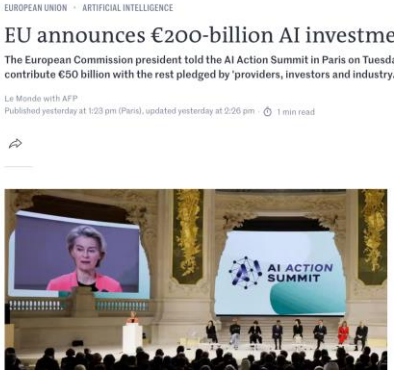
Gabriele Mazzini
MIT Media Lab, Lead author of the AI Act

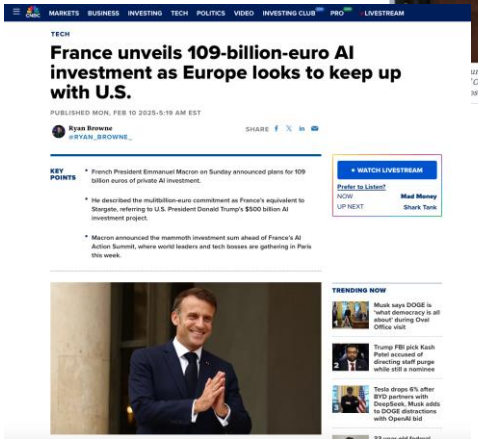
Prohibited AI Practices of the AI Act: origin and evolution

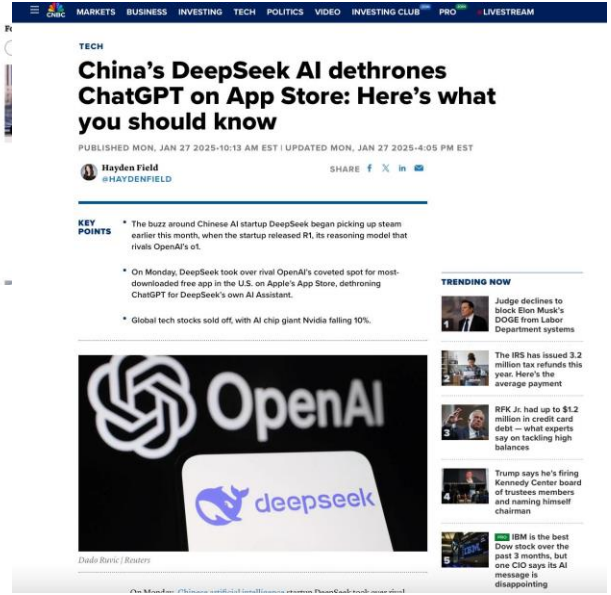
Gabriele Mazzini
Architect & Lead Author AI Act
MIT Media Lab Research Affiliate & MIT Connection Science Fellow

AI Act Implementation Day by bitkom & appliedAI
February 13, 2025
Munich









Introduction

Origins

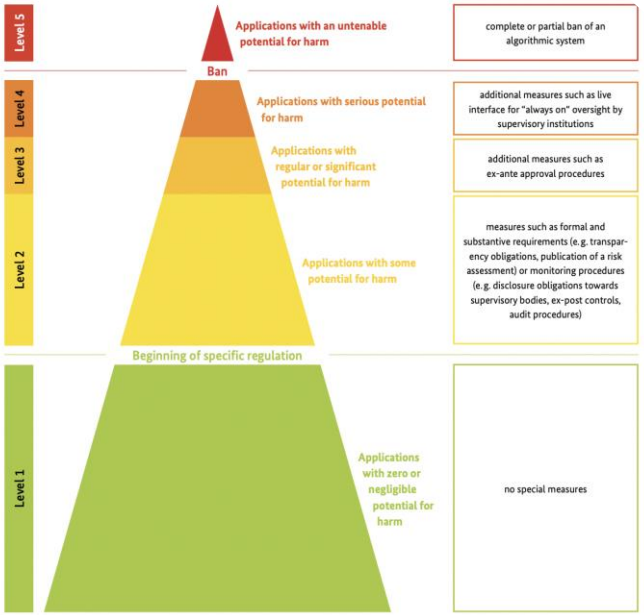


Figure 8:
Criticality pyramid and risk-adapted regulatory system for the use of algorithmic systems

Opinion of the Data Ethics Commission, December 2019, p. 177

LAW - algorithm-determined killings

HLEG ethics guidelines for trustworthy AI, April 2019, p. 33

Critical concerns

- Identifying and tracking individuals with AI
- Covert AI systems
- AI enabled citizens scoring
- LAW
- Potential long term concerns

Context and thinking behind initial draft

- Fits well into risk-based approach
- Most restrictive & impactful legal approach - need to be very specific & ‘surgical’ – thread carefully!
- Safety net for ‘extreme undesired behavior’ that has no societal value, exceptional situations
- ‘AI practices’ rather than ‘AI systems’ – Unfair Commercial Practices Directive
- In practice likely already prohibited under EU and/or national law

Prohibited AI Practices

Subliminal techniques **& manipulative/deceptive** techniques resulting in significant harm

Exploitation of vulnerabilities resulting in significant harm

'Social scoring' by public & private authorities

'Real-time' remote biometric identification for law enforcement purposes in publicly accessible spaces (with exceptions)

Biometric categorisation (race, political opinions, trade union membership, religion/philosophical beliefs, sex life, sexual orientation)

Individual criminal risk assessment

Emotion recognition in workplace and education except medical or safety reasons

Untargeted scraping of internet or CCTV for facial images to build-up or expand databases

Initial Prohibited AI practices

Harmful subliminal manipulation – Art. 5(1)(a)

Commission AI Act proposal

(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness ~~in order to materially distort~~ a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

Final AI Act

(a) the placing on the market, **the** putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness **or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken** in a manner that causes or **is reasonably** likely to cause that person, another person **or group of persons significant harm**;

Harmful exploitation of vulnerabilities – Art.5(1)(b)

Commission AI Act proposal

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, ~~in order to materially distort~~ the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

Final AI Act

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities **of a natural person or** a specific group of persons due to their age**,** disability **or a specific social or economic situation, with the objective, or the effect, of** materially **distorting** the behaviour of that person **or a person belonging to that group** in a manner that causes or is **reasonably** likely to cause that person or another person **significant** harm;

‘Social scoring’ – art. 5(1)(c)

Commission AI Act proposal

the placing on the market, putting into service or use of AI systems ~~by public authorities or on their behalf~~ for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;

Final AI Act

the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, **inferred** or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups **of persons** in social contexts **that** are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups **of persons** that is unjustified or disproportionate to their social behaviour or its gravity;

Real-time remote biometric identification - Art. 5(1)(h)

Prohibition with three exceptions

- **Searching for victims** of abduction, trafficking, or sexual exploitation, and locating **missing persons**
- Preventing a specific, serious, and immediate **threat to the life or physical safety** of individuals, or addressing a real and imminent or likely **terrorist threat**
- Locating or identifying a **person suspected of committing a criminal offense**, in order to carry out a criminal investigation, prosecution, or enforce a criminal penalty for certain offenses (listed in Annex II) that are **punishable in the Member State** by a custodial sentence or detention order for at least four years

Procedural requirements

- **National law** authorising the use
  - establish **safeguards and conditions** in relation to the use, in particular as regards the temporal, geographic and personal limitations, **specifically state objectives** and **criminal offences** (Annex II) for which use is authorized
  - MS may introduce **more restrictive laws** on use
- **prior authorisation** for each use by judicial authority or independent administrative authority
- **prior FRIA** & **registration of system** in EU database
- **each use notified** to DPA and MSA
- **DPA and MSA to submit annual reports** to COM on use, incl. # of authorisations & **COM to publish annual reports**

New Prohibitions

Criminal risk assessment – Art. 5(1)(d)

The placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, **based solely on the profiling of a natural person or on assessing their personality traits and characteristics**; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity

Untarget scraping to develop facial recognition databases - Art. 5(1)(e)

The placing on the market, the putting into service for this specific purpose, or the use of **AI systems that create or expand facial recognition databases** through the **untargeted scraping of facial images from the internet or CCTV footage**

Emotion Recognition - Art. 5 (1) (f)

The placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person **in the areas of workplace and education institutions**, except where the use of the AI system is intended to be put in place or into the market for **medical or safety reasons**

Biometric Categorization - Art. 5(1)(g)

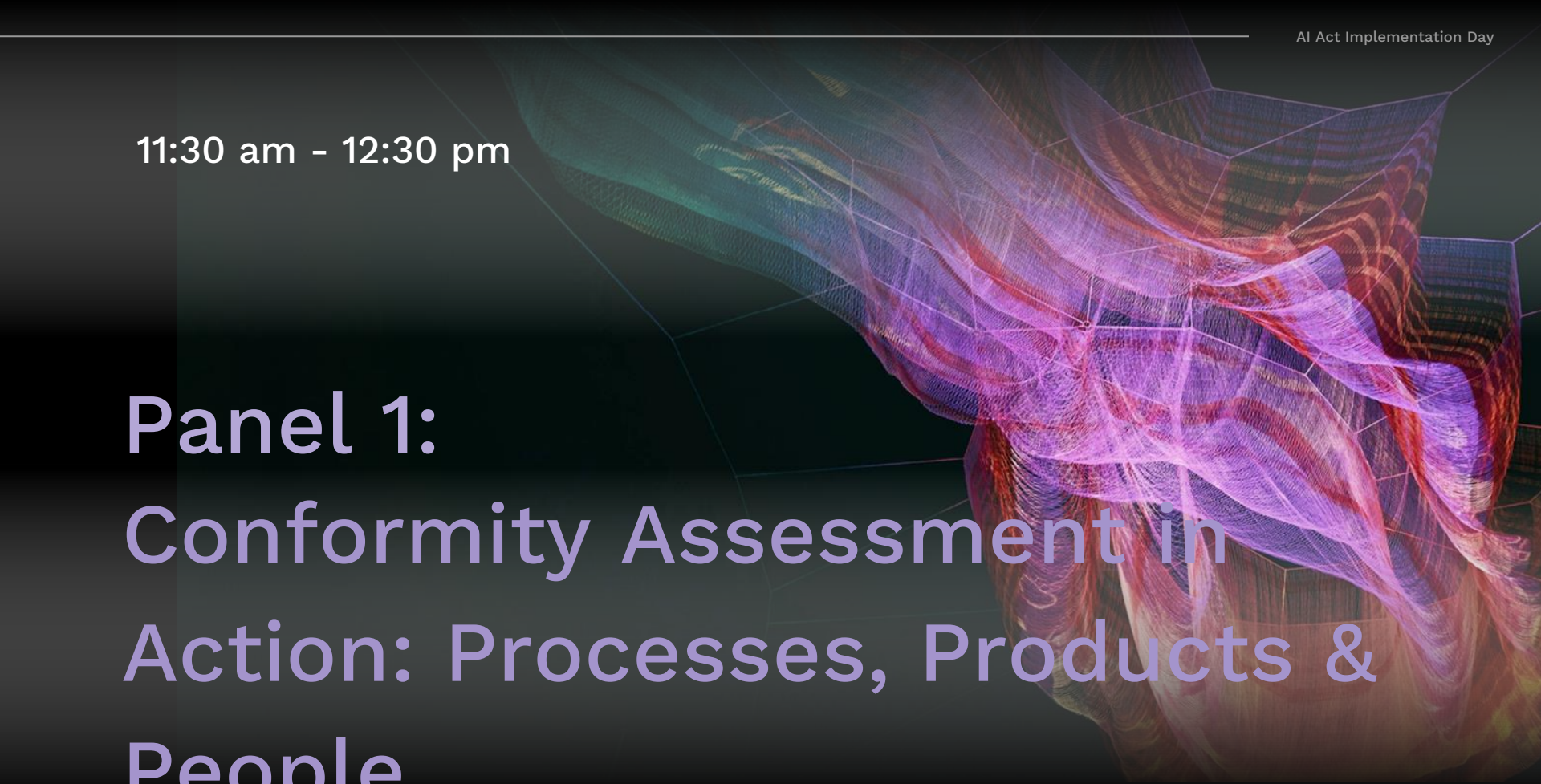
The placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to **deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation**; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement

Thank you!

gmazzini@llm10.law.harvard.edu

mazzini@mit.edu

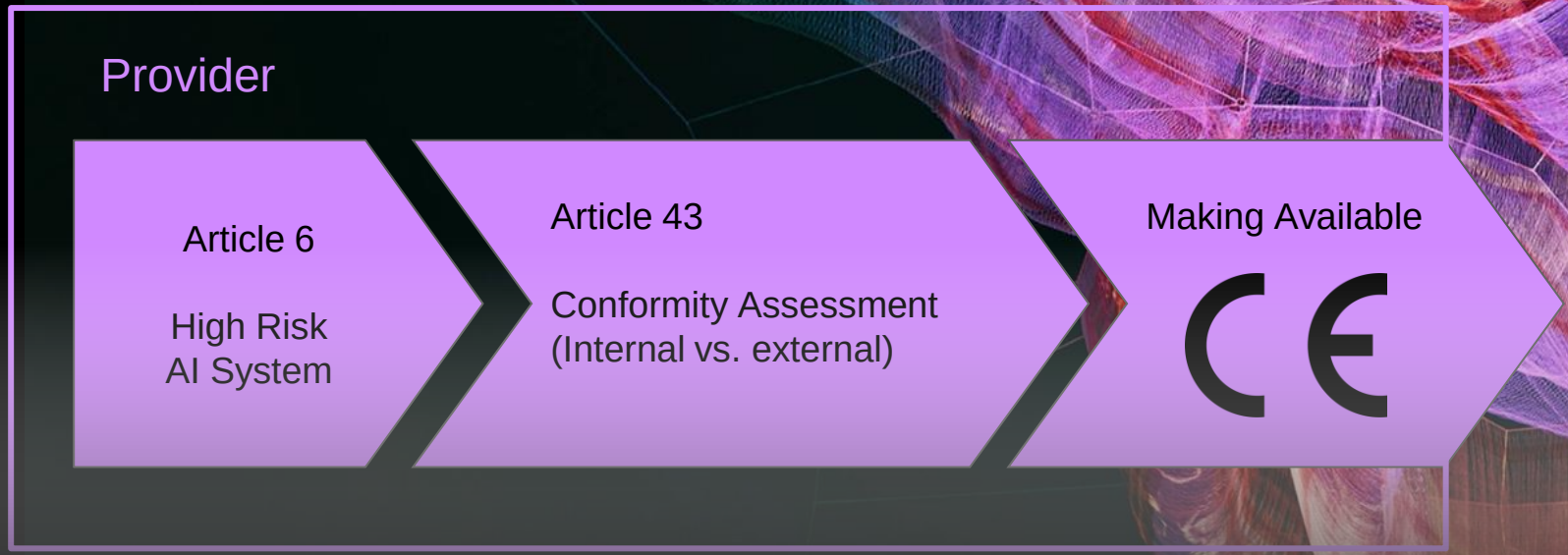
11:30 am - 12:30 pm



Panel 1: Conformity Assessment in Action: Processes, Products & People

11:30 am - 12:30 pm

Panel: High-Risk Conformity Assessment



11:30 am - 12:30 pm

Conformity Assessment in Action: Processes, Products & People

Dr. Christoph Poetsch
Head of AI Quality and Ethics, TÜV AI.LAB

Pillars to effectively implement the AI Act

Dr. Christoph Poetsch

Head of AI Quality and Ethics @ TÜV AI.Lab

Keep calm & carry on, but …

Instead of “all regulation off”, we should stick to Europe’s USP “safety & innovation” — but: Europe needs to do its homework, we have to regu-late better & more efficiently

Standards and Guidelines

Standards and guidelines need to be timely and concrete enough to plan, to develop and to test, that means w.r.t. all relevant do-mains and AI technologies

Efficient implementation

Concise structures w.r.t. relevant public authorities, equal implementation across Europe (no “gold-plating”), and efficient certification pipelines

Innovative Potentials

Assessments and high standards as advantage on the market — but: compre-hensive and strict enforce-ment to have a level playing field for all stakeholders

TÜV AI.LAB

11:30 am - 12:30 pm

Conformity Assessment in Action: Processes, Products & People

Dr. Wolfgang Hildesheim
Head of Watson, Data Science & AI, IBM Deutschland

EU AI Act – 1-pager for Executives ?!?

1. Which AI systems do we have?

2. Do we have a homogeneous risk assessment “a la EU AI Act”?

3. Which AI systems are “high risk” ? (5-15% of systems)
   - Option 1: Conformity assessment by third party, f.i. TÜV, Phönix Labs…
   - Option 2. Self-conformity using the 8-10 European harmonized AI-standards

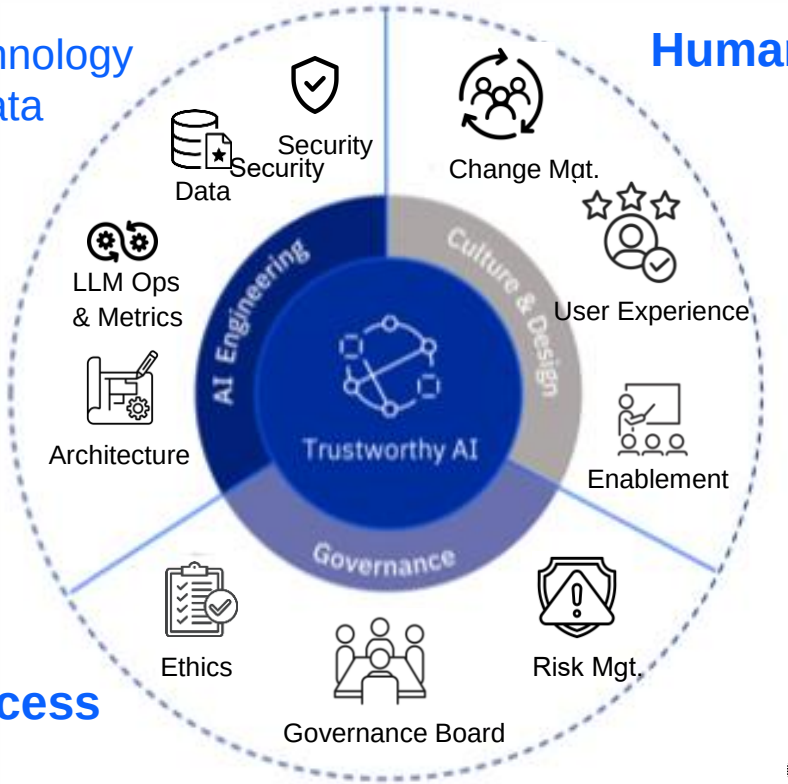
4. Which AI systems are “not high risk” ? (85-95% of systems)
   - No conformity tests needed
   - Transparency need related to the GPAI-models
   - System tests needed in the “usual sectors”, f.i. automotive, medical, telco…

AI - What keeps a company Executive awake at night ?

Do I have a good AI strategy? Are the 6 success factors of AI covered?

1. **AI People** = Talent with AI expertise
2. **AI Data** = Collections- & Data-Management
3. **AI SW** = Access & Knowledge about AI SW
4. **AI Innovation Culture** = „use case focus“, „step-by-step“ & „fail fast“ approach
5. **AI eco-system** = business-& tech-partners
6. **AI governance** = Trustworthiness & Compliance with EU AI Act

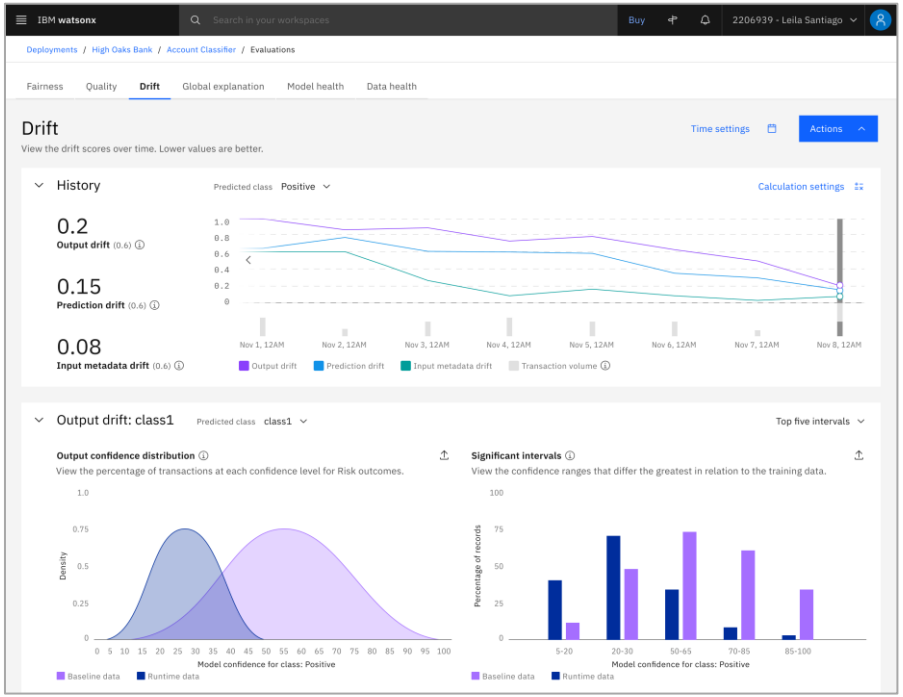
Do I have the elements of a Trustworthy AI?



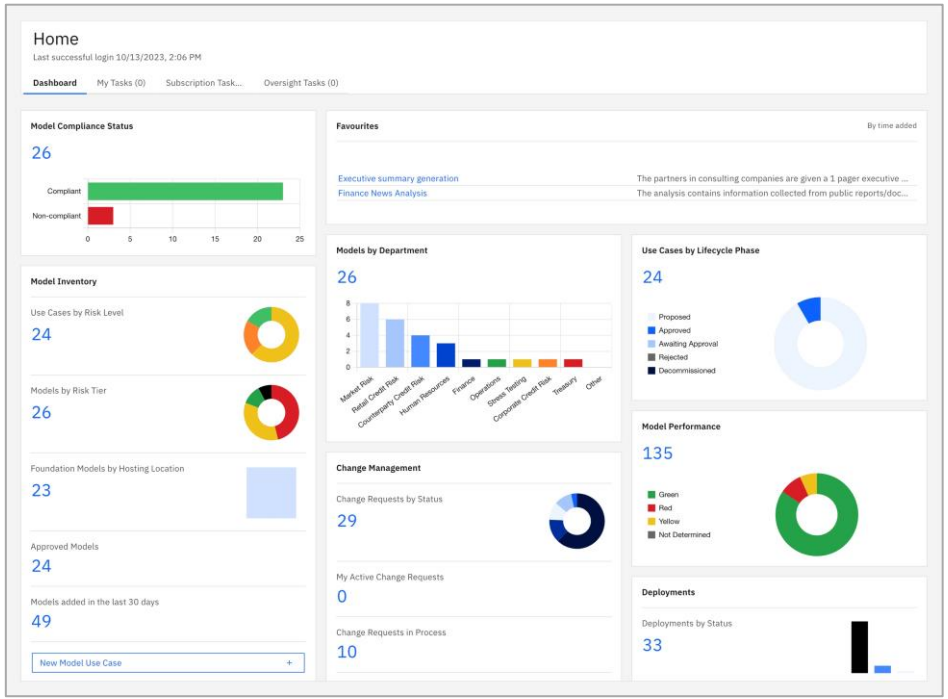
Watsonx.governance

Monitor the performance of your models and AI governance via dashboards

Evaluation and Monitoring



Risk Management and “best practices”



Example

AI Recognition of buildings and outlines

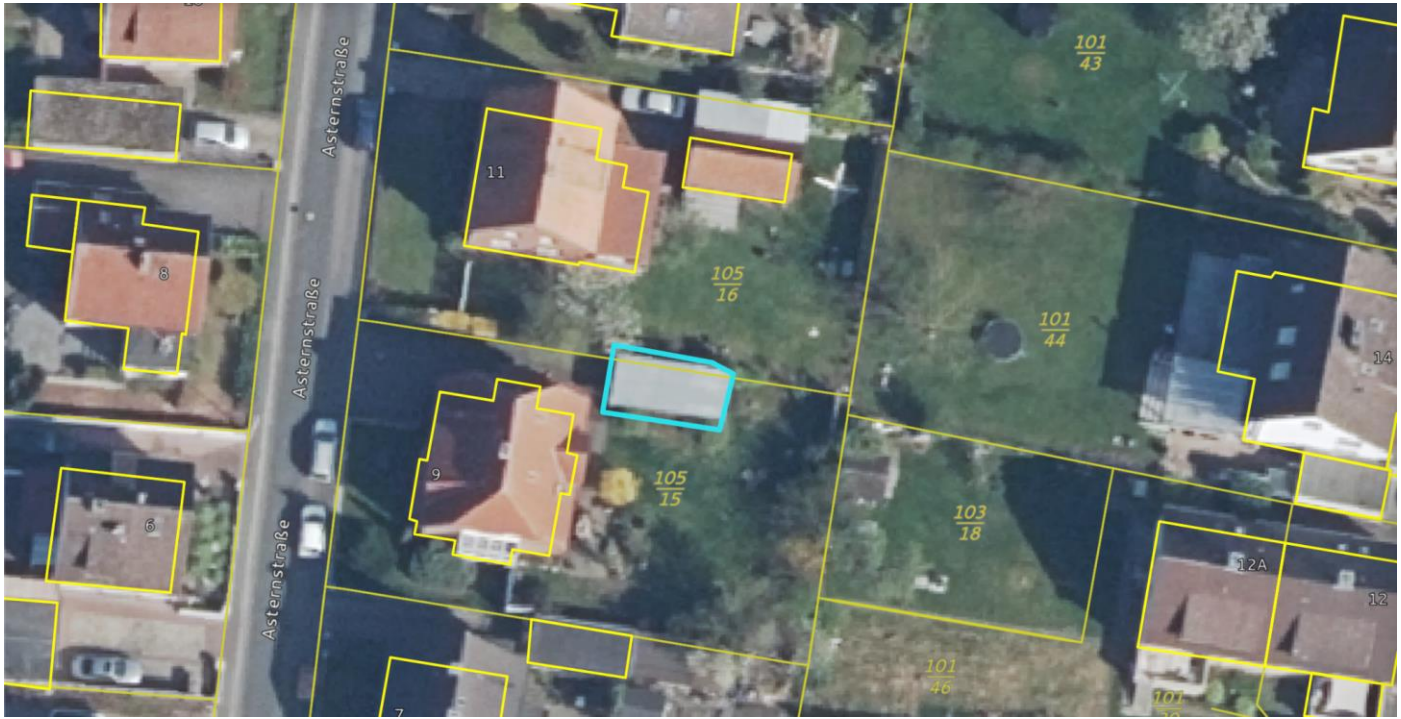


Figure 11.1: Use case for AI: Find the few missing buildings (here a garage in blue) in thebuildings (here garage in blue) in the mass data of the real estate cadastre(buildings and parcels in yellow)
https://www.amazon.de/K%C3%BCnstliche-Intelligenz-managen-verstehen-book/dp/341031458X.

v0.18.3

DEUTSCHE VERWALTUNGSCLOUD

EIN PROJEKT DES IT-PLANUNGSRATS

Cloud-Services

Filter

Anbieter (1)

Portfoliokategorie

Serviceart

Servicekategorie

Alle zurücksetzen

Landesamt für Geoinformat... ×

Suchbegriff eingeben ...

Name A-Z

KI-Gebäudeerkennung

Mit der KI-Gebäudeerkennung können Nutzende Gebäude in Luftbilddaten automatisch erfassen lassen, um damit z.B. den Gebäudebestand eines Liegenschaftskatasters zu aktualisieren.

Mehr

SaaS

AI Trustworthiness Label to support the GTM

https://www.amazon.de/K%C3%BCnstliche-Intelligenz-managen-verstehen-book/dp/341031458X

Artificial Intelligence

The AI model recognises objects on satellite images. The model is trained on building locations, building outlines, building types and other building properties.The satellite images are composed of different sensor data: optical images, lidar images.

Manufacturer: LGLN
Model version: V2.3 aus 2022

Application: Object recognition on aerial photographs

Capability	Method	Data
Percept >External >>See	Machine Learning >Supervised Learning >>Neural Network	Training input: known quality-checked satellite images (optical, infrared) and lidar data Operational data: unknown images
Process >Facts >>Select >>Verify	Machine Learning >Supervised Learning >>Neural Network	Building location ,+-xx cm, Building outline ,+- yy cm
Act		
Communicate		

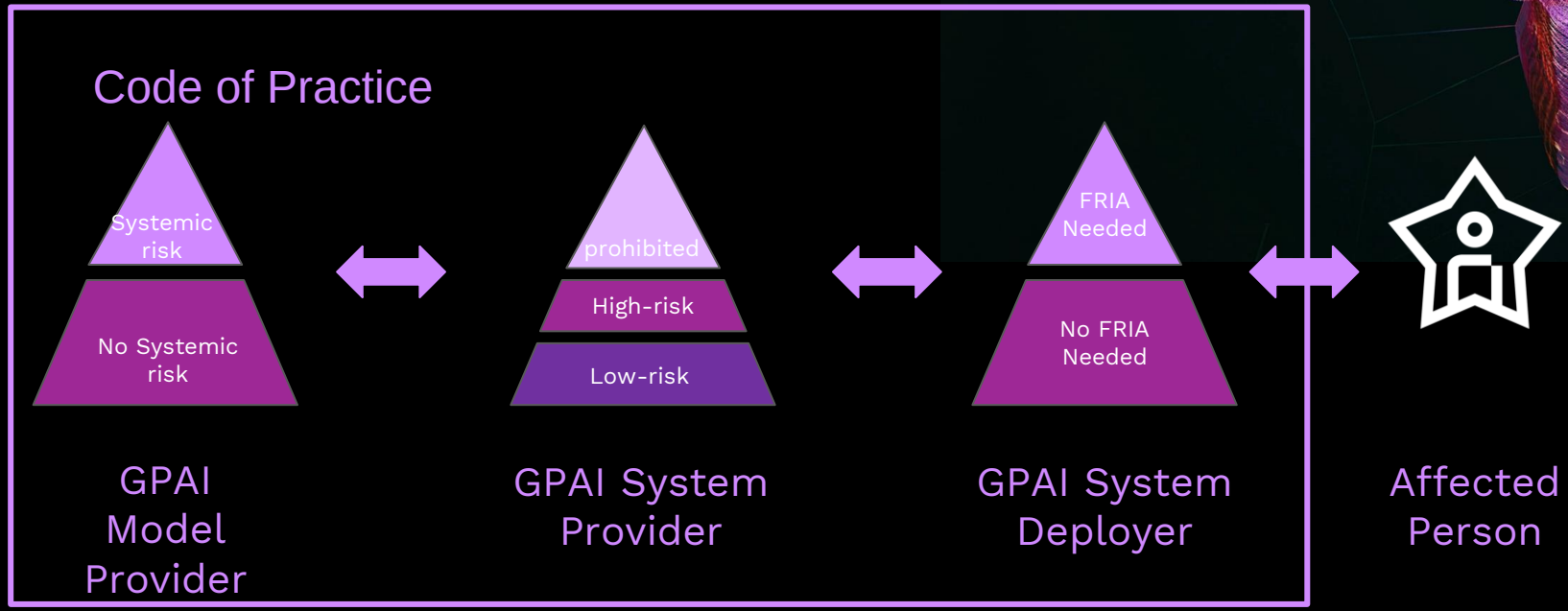
Risk very low

01:30 - 02:30 pm

Panel 2: AI Value Chain & Responsibilities

01:30 - 02:30 pm

Panel 2: AI Value Chain & Responsibilities



01:30 - 02:30 pm

AI Value Chain & Responsibilities

Sebastian Dürdoth,
Senior Corporate Counsel, Microsoft Deutschland

Pillars to effectively implement the AI Act

Dr. Christoph Poetsch

Head of AI Quality and Ethics @ TÜV AI.Lab

Keep calm & carry on, but …

Instead of “all regulation off”, we should stick to Europe’s USP “safety & innovation” — but: Europe needs to do its homework, we have to regu-late better & more efficiently

Standards and Guidelines

Standards and guidelines need to be timely and concrete enough to plan, to develop and to test, that means w.r.t. all relevant do-mains and AI technologies

Efficient implementation

Concise structures w.r.t. relevant public authorities, equal implementation across Europe (no “gold-plating”), and efficient certification pipelines

Innovative Potentials

Assessments and high standards as advantage on the market — but: compre-hensive and strict enforce-ment to have a level playing field for all

TÜV AI.LAB

Microsoft

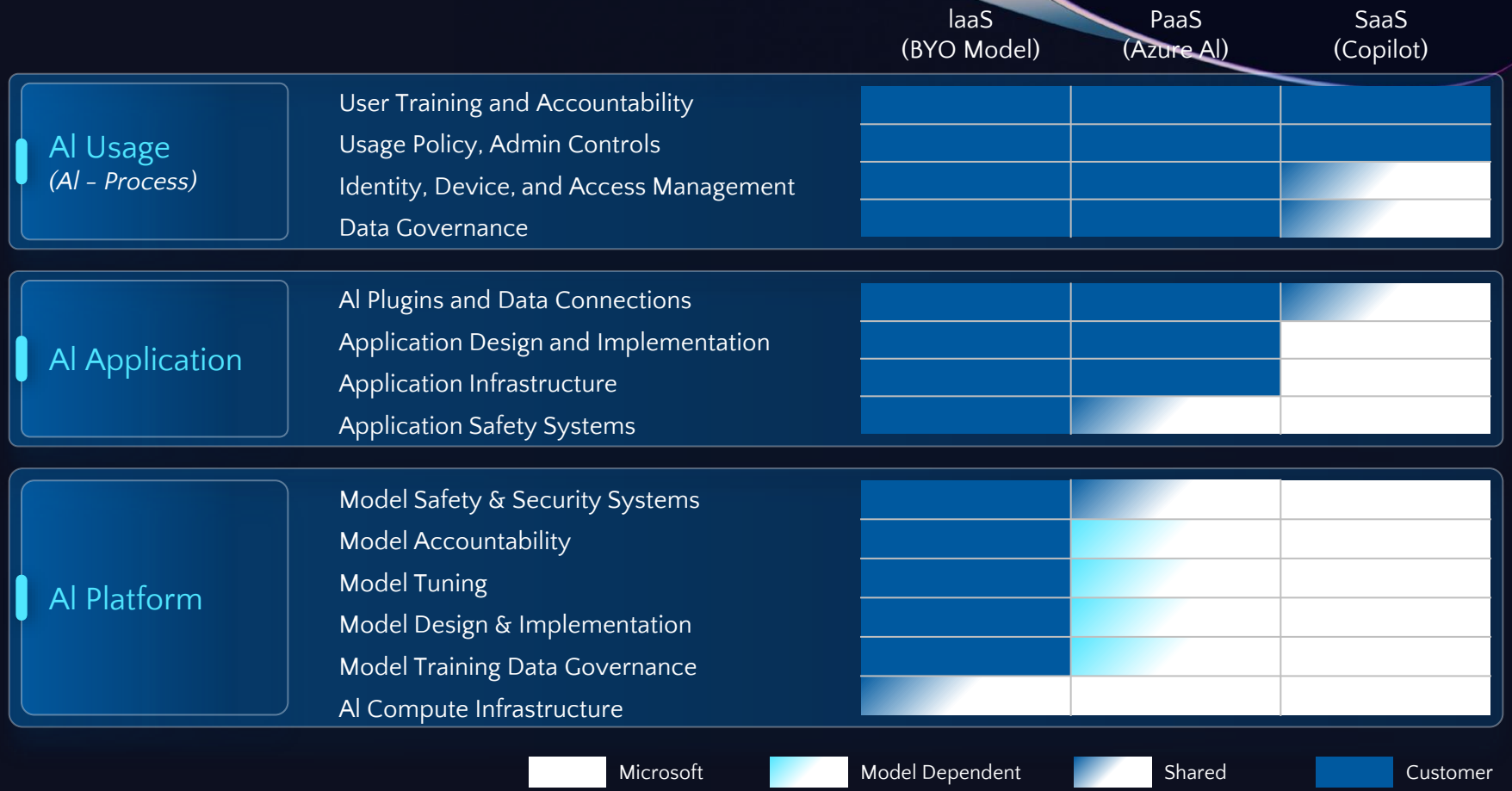
The AI value chain

Supporting customers on their AI compliance journey

Sebastian Dürdoth
Senior Corporate Counsel

CELA
Customer &
Partner Solutions

Just like cloud, AI is a shared responsibility



How Microsoft supports customers on their AI compliance journey

Mitigate AI risks

Provide transparency

Share RAI learnings

Support AI skilling

http://aka.ms/rai

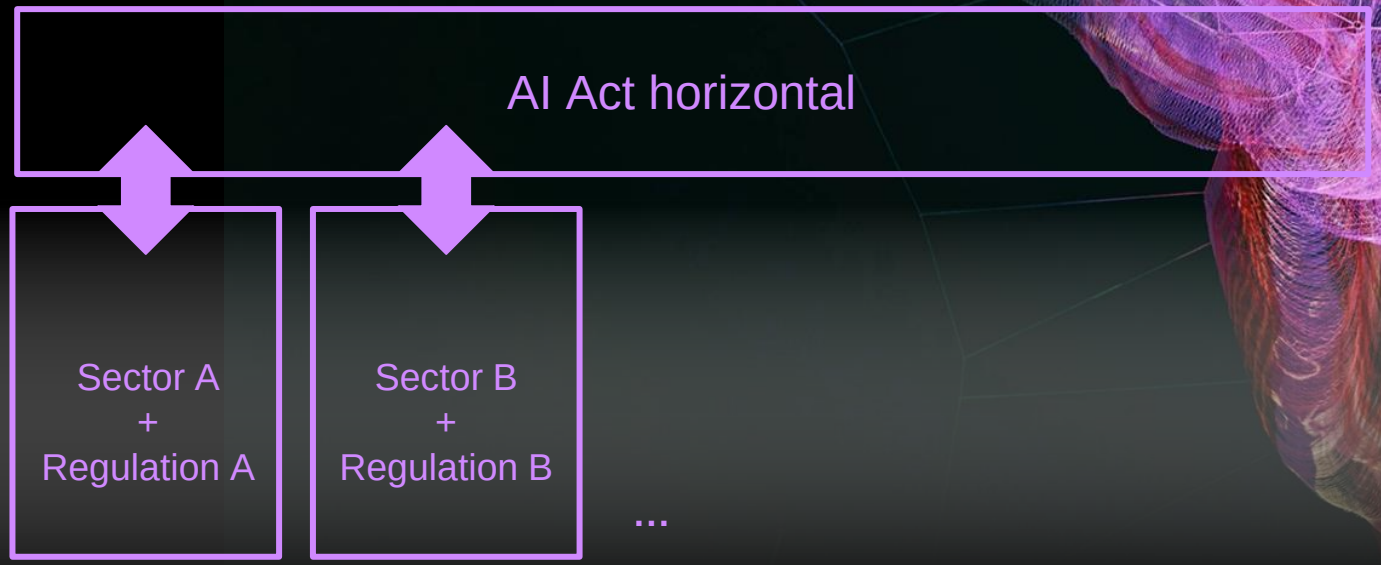
https://aka.ms/EUAIAct
(AI Literacy Starting Guide)

02:30 - 03:30 pm

Panel 3: High Risk & Sectoral Regulation

02:30 - 03:30 pm

Panel 3: High Risk & Sectoral Regulation



How Siemens is getting prepared for the upcoming AI regulations, such as the AI Act?

13th February 2025

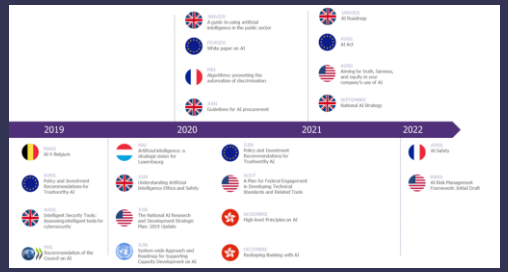
AI Act Implementation Day

Prof. Dr. Sonja Zillner

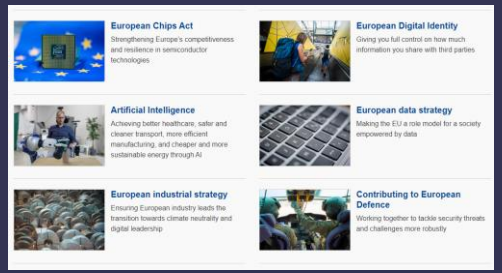
SIEMENS

Emerging regulatory landscape for Data & AI …….

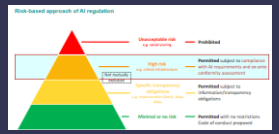
…….requires a consistent and comprehensive framework across the organization



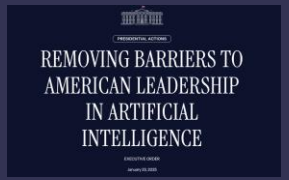
On international level…….



….covering various digital and data related aspects



Risk based approach of the EU AI ACT



Removing Barriers to American Leadership in AI- Trumps Executive Order

China Global AI Governance released AI governance regulation

Guiding principles & codes of conduct for AI (G7 Hiroshima AI process)

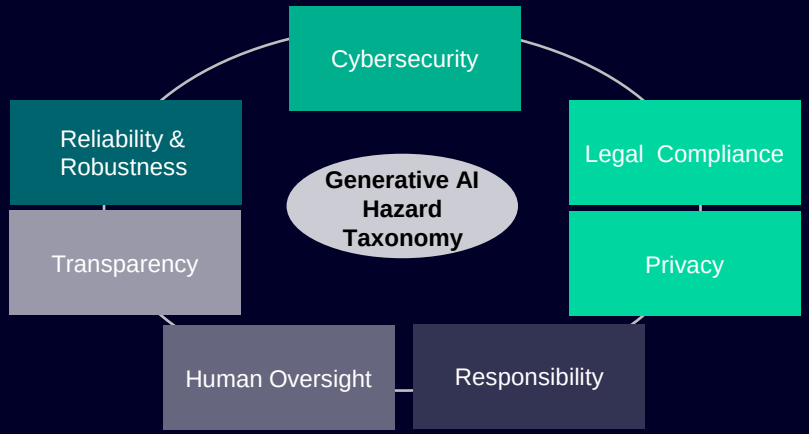
SIEMENS

The Siemens Generative AI Governance approach is risk-based

Siemens Generative AI Risk Management Framework

Generative AI Risk & Hazard Methodology….

- **Risk Profiling and Classification** to determine the criticality of Generative AI applications
- **Generative AI Risk/Hazard Taxonomy** to guide the risk identification
- **Mitigation Guideline** to assess and mitigate Generative AI triggered risks
- **Process Description** defining roles, responsibilities, milestones, quality gates and decision points
- **Best Practices of Pre-approved architectural** Patterns to speed up the evaluation process



….enabling the **systematic** identification of **risk sources**

while developing & deploying GenAI applications

….is mapped to the related organisational processes

by defining roles, responsibilities, milestones, quality gates & decision points

Product Lifecycle Management | Project Management | Cybersecurity processes | Data Privacy | Other….

SIEMENS

Generative AI Risk Management Framework
Embedding into the Product Lifecycle Management Process

Trigger:
Are you planning to use a Generative AI model to offer a service, product, or solution to a customer?

Yes → **Portfolio Evaluation**

Classify new product
AI Act High Risk Classification

I_Trigger

Define scope of new product
GenAI Risk **Profile**

I_Trigger

Approval for Implementation
GenAI Risk **Assessment**

I_Trigger

Approval for Sales
GenAI Risk **Mitigation**

"Are you high-risk in accordance to the AI Act?"

"Describe the intended purpose of the GenAI and the data flow?"

"Check Generative AI risk list & define risk mitigation measures"

"Implement the defined mitigation measures e.g., robust AI, explainable AI"

Supported by **Generative AI Risk Methodology**

AI Risk Classification Methodology to determine the criticality of the AI Product

Intended purpose description to define the scope of the GenAI risk assessment

Generative AI Risk List to guide the risk identification and scope mitigations

Mitigation Guideline to assess and mitigate Generative AI triggered risks

SIEMENS

Generative AI Risk Management Framework
Embedding into the Product Lifecycle Management Process

Trigger:
Are you planning to use a Generative AI model to offer a service, product, or solution to a customer?

Yes → **Portfolio Evaluation**

Classify new product
AI Act High Risk Classification

I_Trigger

Define scope of new product
GenAI Risk **Profile**

I_Trigger

Approval for Implementation
GenAI Risk **Assessment**

I_Trigger

Approval for Sales
GenAI Risk **Mitigation**

“Are you high-risk in accordance to the AI Act?”

“Describe the intended purpose of the GenAI and the data flow?”

“Check Generative AI risk list & define risk mitigation measures”

“Implement the defined mitigation measures e.g., robust AI, explainable AI”

Supported by **Generative AI Risk Methodology**

AI Risk Classification Methodology to determine the criticality of the AI Product

Intended purpose description to define the scope of the GenAI risk assessment

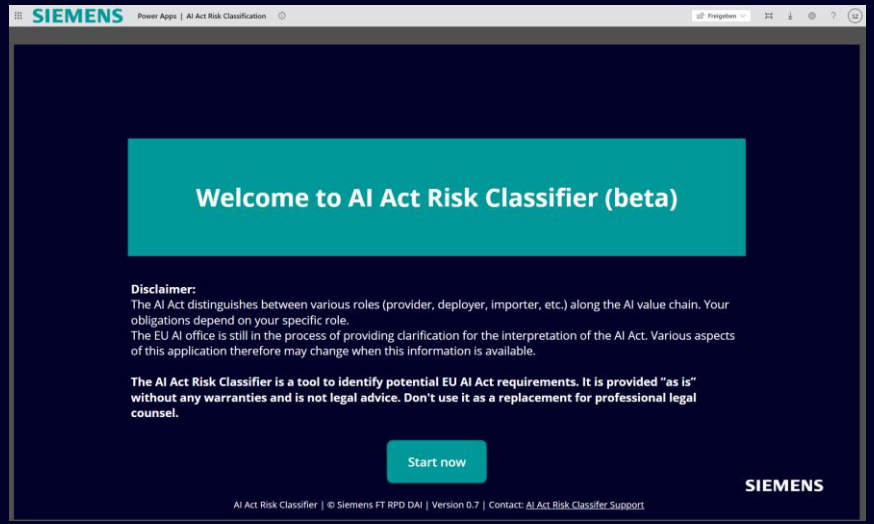
Generative AI Risk List to guide the risk identification and scope mitigations

Mitigation Guideline to assess and mitigate Generative AI triggered risks

SIEMENS

EU AI Act Risk Classification (Compliance to AI Act)

The **AI Act Risk Classification** helps to determine the risk class/category of your AI system in accordance with the AI Act.



EU AI Act Risk Classification

AI Act Risk classification to determine the criticality of the GenAI product.

In case of

- **Low risk:** Continue the product development
- Transparency obligations: Additional transparency obligations (Article §50) need to be fulfilled
- **High risk:** request expert consultancy to ensure presumption of AI Act conformity while product development
- **Unacceptable risk:** stop product development

SIEMENS

EU AI Act Risk Classification (Compliance to AI Act)
Example RAG-based Q&A System

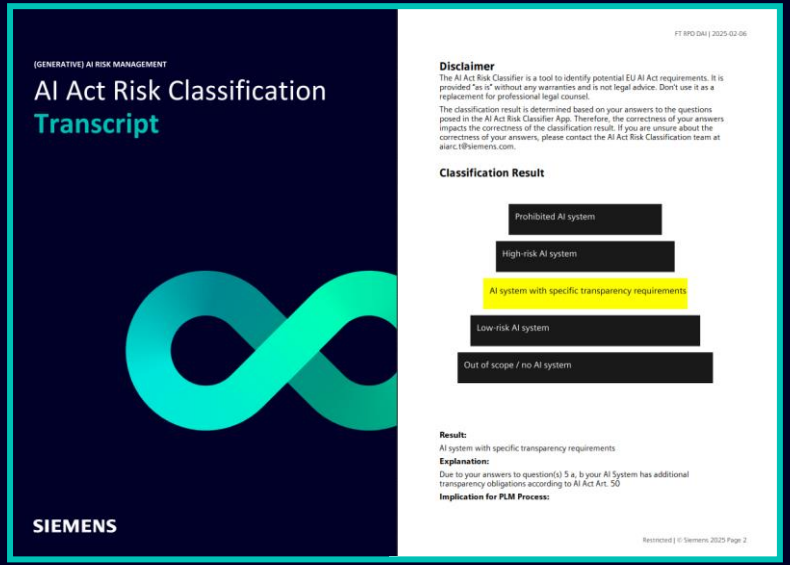
The classification services is a self-service enabling the access to legal, standardization and AI experts in case of questions

Product Manager, Team Architect

Individually or in a short session

< 30 min

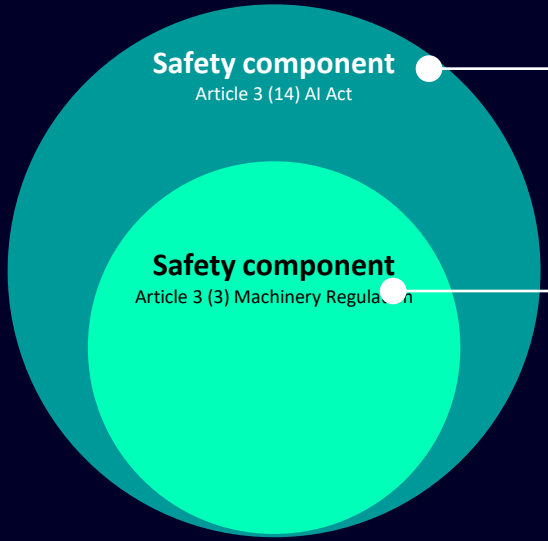
Transcript is stored in the respective product development repository



SIEMENS

Interplay AI Act x Machinery Regulation*: Safety Components

The definition of safety components under the AI Act **is much broader** than in the Machinery Regulation



AI Act

- ….fulfils a **safety function…..**

OR

- …failure / malfunctioning endangers the health or safety or **property**….
- not necessary to be placed on the market separately

Machinery Regulation

- designed or intended to fulfil a **safety function**

AND

- placed on the market **separately**
- additional safety device, no impact on machine function
- Machine is fully operational without the safety component

The same component that falls under both the AI Act and the Machinery Regulation may now be classified differently depending on the regulatory context.

SIEMENS

Implementation of the AI Act

Our Learnings & Upcoming Challenges in a nutshell

Embedding AI Governance into existing organizational process is beneficial

People require explanations and/or guidance from experts

Inconsistency of legal definitions needs to be addressed!!

Harmonized AI Standards are still missing

SIEMENS

02:30 - 03:30 pm

High Risk & Sectoral Regulation

Araceli Alcala Espinosa
Regulatory Affairs Manager, Carl Zeiss Medical

Guiding EU AI Act Adoption with MDR Insights

Araceli Alcala

February 13th, 2025

Disclosure

Carl Zeiss Meditec AG

Medical Device Regulation
Our North Star for navigating the AI Act

Are companies compliant with EU legislative frameworks, like MDR, better prepared for the AI Act?

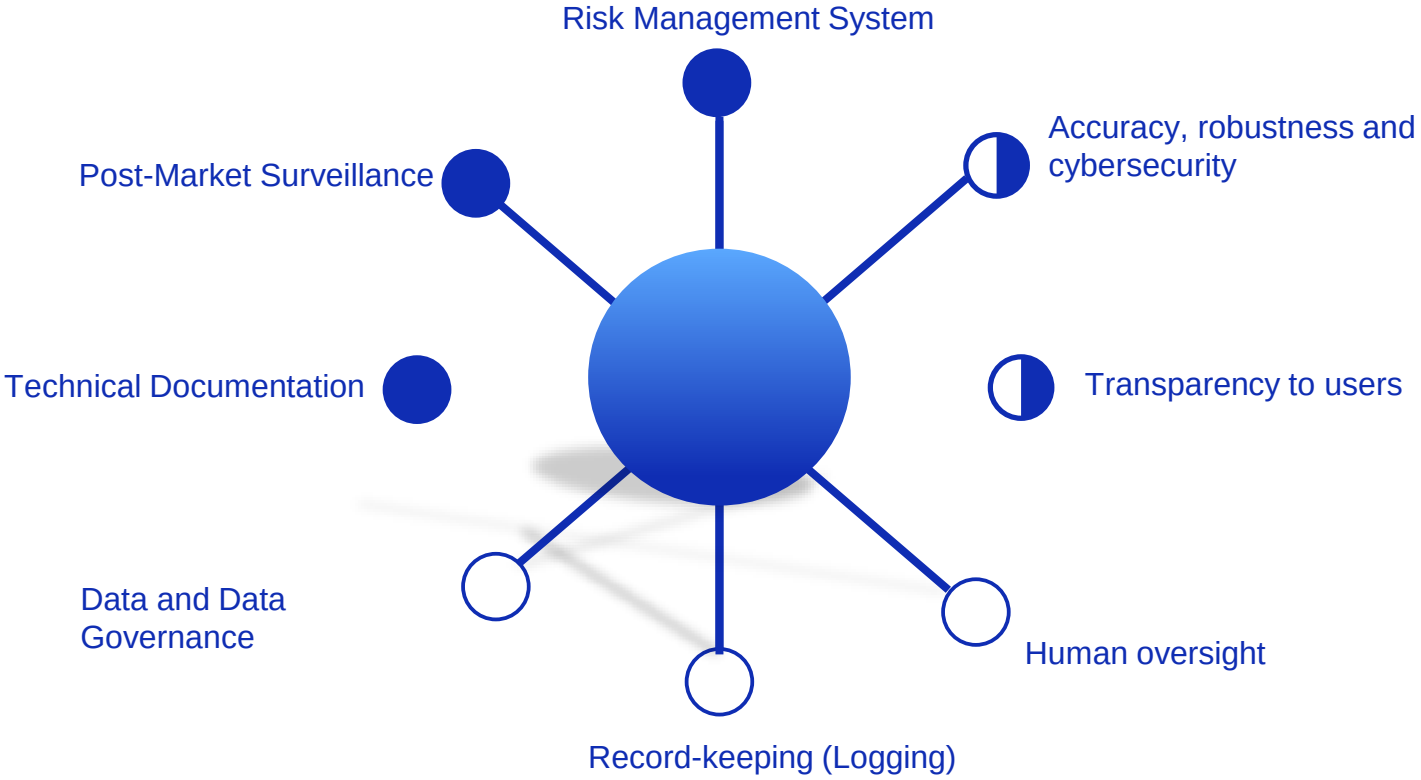
Source: Botond Horvath / Shutterstock.com

A comparative overview of shared principles

MDR (EU) 2017/745	AI ACT (EU) 2024/1689
Comprehensive regulatory framework for medical devices	Comprehensive regulatory framework for artificial intelligence
Applies to all medical devices, including software	Applicable requirements commensurate to the risk AI systems can pose
Primary goal: Protect patients and users	Primary goal: Foster trustworthy AI and ethical considerations
Ensures high safety standards during total product lifecycle	Ensures high safety standards during total product lifecycle

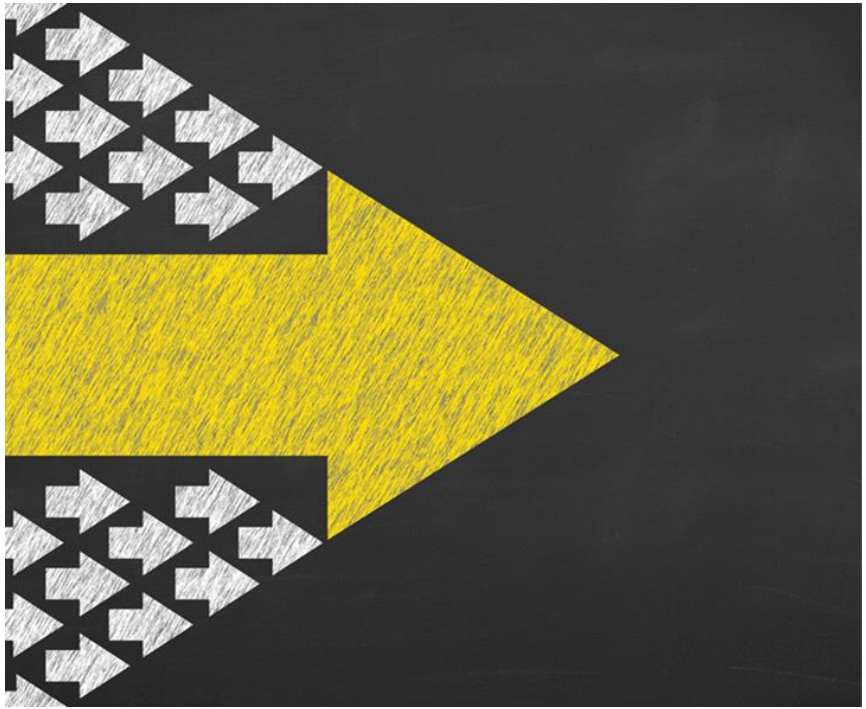
MDR provides a strong foundation for navigating the complexities of the AI Act

MDR and EU AI Act
Partial alignment of provisions for high-risk AI Systems



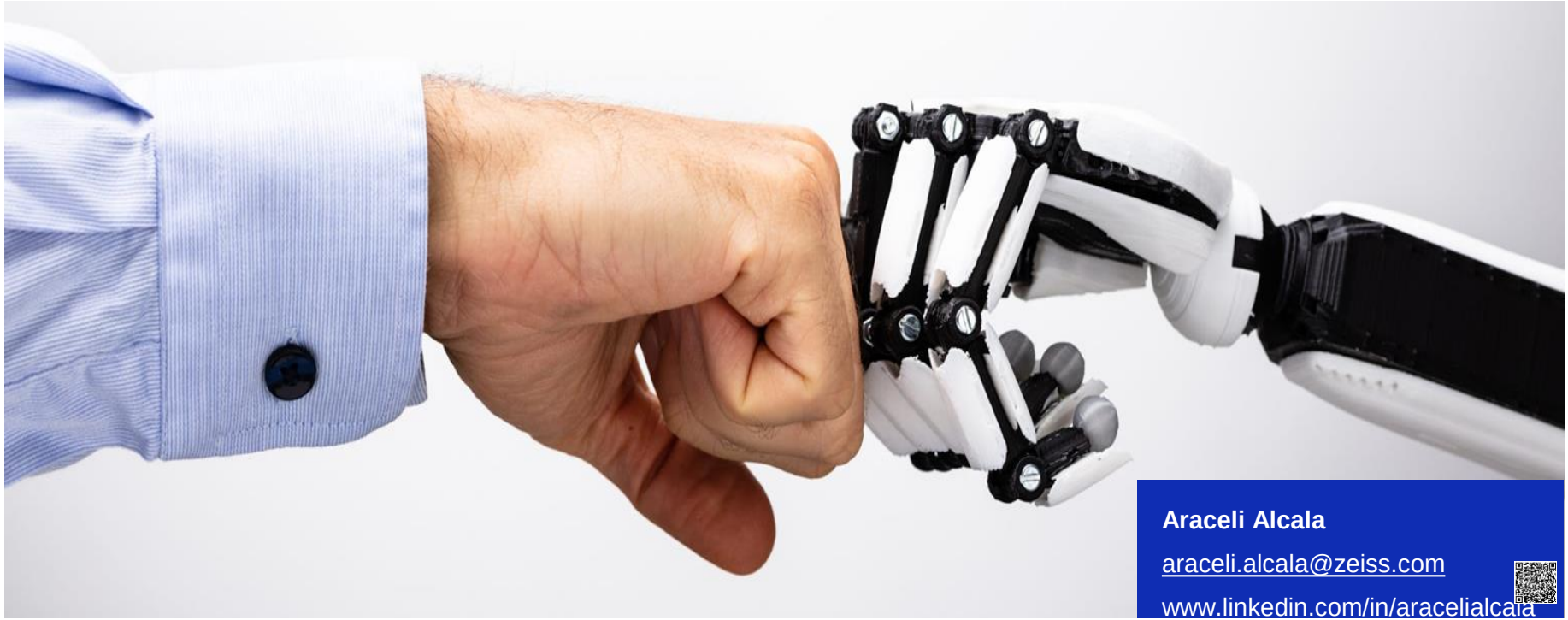
Fully covered
Partially covered
Not covered

Reflecting on MDR Learnings for AI Act Success



1. Early preparation is crucial
2. Stronger clinical evidence is essential
3. Post-market surveillance (PMS) is a continuous journey
4. Proper resource allocation
5. Compliance is a cross-functional effort
6. Tailor the QMS

Thank you



Araceli Alcala

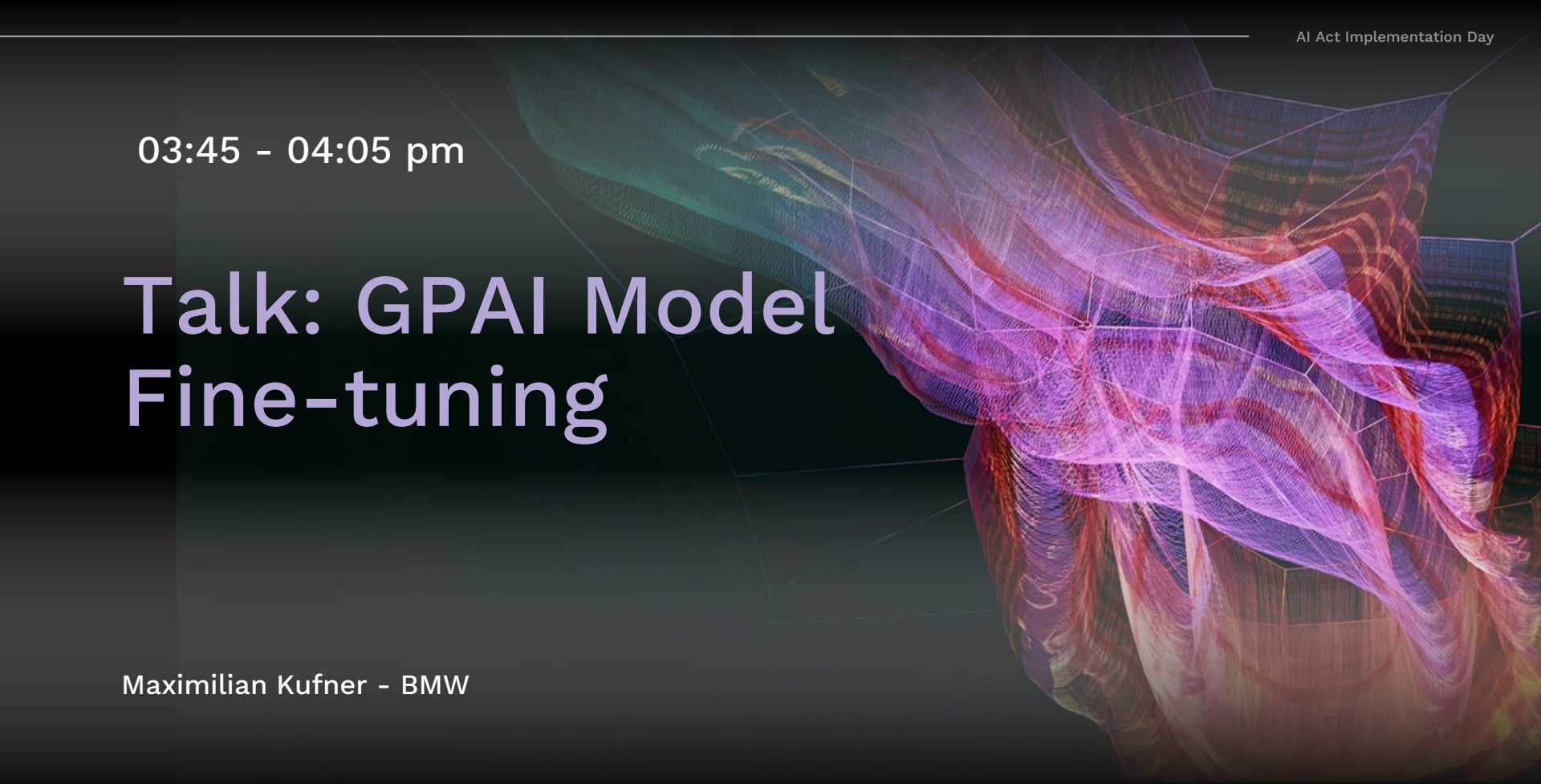
araceli.alcala@zeiss.com

www.linkedin.com/in/aracelialcala

Seeing beyond

03:45 - 04:05 pm

Talk: GPAI Model Fine-tuning



Maximilian Kufner - BMW

04:05 - 04:25 pm

Talk: Transparency Obligations: AI Use Cases

Sebastian Grantz
Global Data & Privacy Manager, Industry Relations, Google Germany

REGULATORY RESPONSIBILITIES IN THE CASE OF GPAI MODEL FINE TUNING

MAXIMILIAN KUFNER, BMW GROUP

THERE ARE DIFFERENT REQUIREMENTS **FOR PROVIDERS OF GPAI MODELS WITH** AND **WITHOUT SYSTEMIC RISK.**

10^{25} FLOPS or **less** used for the training

Requirements for GPAI models **without** systemic risk

Article 53: Obligations for providers of GPAI models, esp.:

- Technical documentation (s. Annex XI (1) for minimum requirements)
- Copyright compliance strategy
- Information and documentation for providers of AI systems (s. Annex XII for minimum requirements).
- Training data

› **"Documentation Obligations"**

Additional requirements for AI models with systemic risk:

More than 10^{25} FLOPS used for the training

Requirements for GPAI models **with** systemic risk

Art. 53 (1), Annex XI (2): Additional information to be provided by providers of GPAI models with systemic risk, esp.:

- **Evaluation strategies**
- **Adversarial testing**
- **System architecture**

Article 55: Obligations of providers of GPAI models with systemic risk, esp.:

- **Model evaluation, risk assessment and mitigation**
- **Incident tracking, documentation and reporting**
- **Cybersecurity protection**

› **"Integrity Obligations"**

There are **"Documentation Obligations"** and **"Integrity Obligations"** for GPAI models.

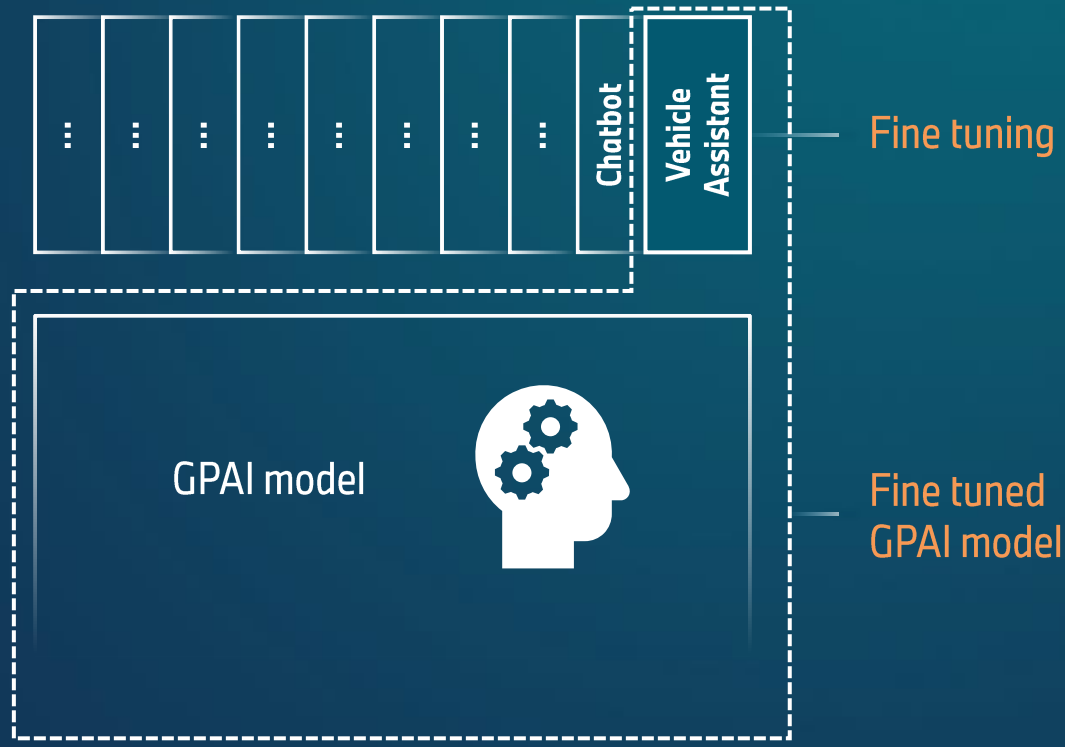
THE EU AI ACT DEFINES **GPAI MODELS AS MONOLYTIC.** IN REALITY **INDUSTRIAL APPLICATIONS** WILL APPLY **FINE TUNING.**

GPAI models as described by the EU AI Act

GPAI models **without** systemic risk

GPAI models **with** systemic risk

Assumed use of GPAI models by the industry

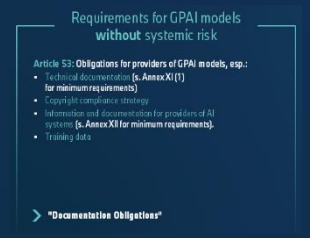


Obligations for GPAI models mentioned in the EU AI Act do **not consider fine tuning** and are **hardly applicable** for the industry.

THERE ARE **MULTIPLE OPTIONS** REGARDING RESPONSIBILITIES FOR FINE TUNED GPAI MODELS. ONLY **SHARED RESPONSIBILITY** SEEMS APPLICABLE.

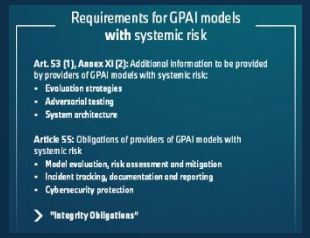
Req. for the **GPAI model** part

- Requirements GPAI models without systemic risk



› **"Documentation Obligations"**

- Requirements GPAI models with systemic risk

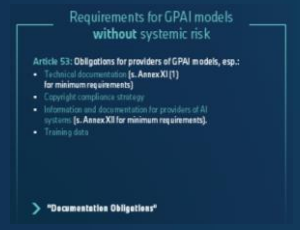


› **"Integrity Obligations"**

› **To be fulfilled by the GPAI model provider**

Req. for **the fine tuning** part

- Requirements GPAI models without systemic risk

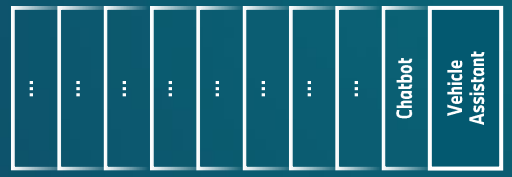


› **"Documentation Obligations"**

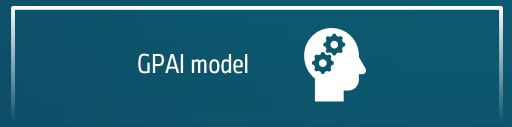
› **To be fulfilled by the fine tuning provider**

»

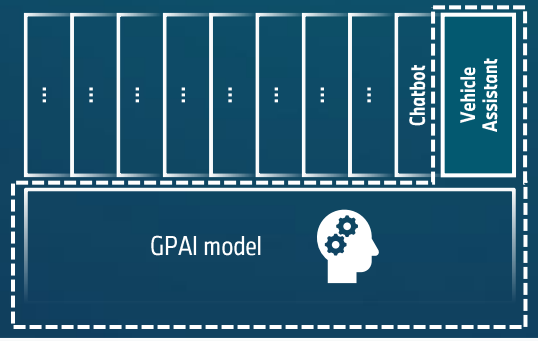
Req. for the **fine tuning** part



\+ Req. for the **GPAI model** part

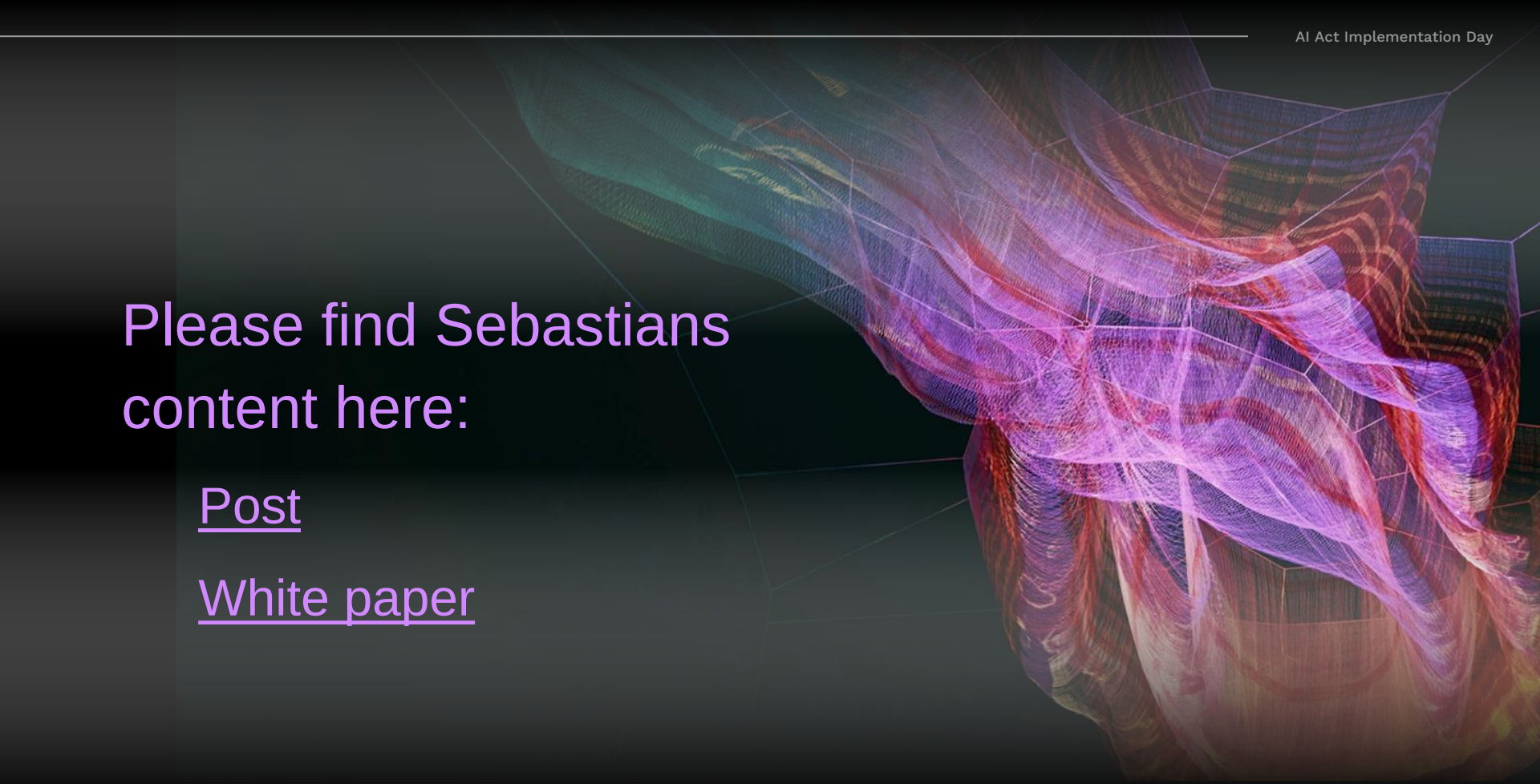


= Req. for the **fine tuned GPAI model**



Proposal: The requirements for fine tuned GPAI models are **solely the sum** of the **requirements for the GPAI model** and the **requirements for fine tuning.**

THANK YOU FOR YOUR ATTENTION!



Please find Sebastians content here:

- Post
- White paper

04:25 - 04:45 pm

Talk: AI Literacy requirements and how to meet them

Paula Cipierre
Director of Data Ethics & Innovation, ada Learning

AI Act Implementation Day

13.02.2025

AI Literacy As Defined By Art. 4 AI Act

Core Requirements & Best Practices for Implementation

Paula Cipierre
Director of Data Ethics & Innovation
ada Learning GmbH

Introduction

Introduction (1/2)

🗓️ In February 2025, Art. 4 AI Literacy became applicable as one of the first requirements of the EU AI Act.

❗ Art. 4 AI Act requires that all organizations developing or deploying AI in the EU take reasonable measures to ensure a sufficient level of AI literacy of their staff and other persons handling AI systems on their behalf.

💡 The AI Act defines AI literacy as the ability to make an informed deployment of AI systems, and to gain awareness about their opportunities, risks, and possible harms.

✅ In so doing, organizations have to take into account their employees' background and role, the context in which the AI systems are to be used, and the perspective of affected persons.

Introduction (2/2)

💡 In other words, Art. 4 AI Literacy encompasses the following three components:

1️⃣ Legal knowledge (a sufficient level of AI literacy).

2️⃣ Technical knowledge (the ability to make an informed deployment of AI systems).

3️⃣ Role- and context-specific knowledge (taking into account the background and role of employees, the context the AI systems are to be used in, and the perspective of affected persons).

Core Requirements

Legal knowledge

1 Employees should be able to recognize when they are interacting with an AI system as defined by the AI Act.

2 Employees should understand the role their organization plays with regards to the AI system and in particular if it operates as a provider or deployer.

3 Employees should be able to evaluate the opportunities, risks, and possible harms of AI systems.

4 Employees should have basic familiarity with the concept of high-risk AI systems.

Technical knowledge

💡 Employees need to be able to make an informed deployment of AI systems.

➡️ In other words, organizations should ensure that their employees know how to use the AI systems that are made available to them.

✅ Note that this is not only a compliance requirement, but also a business advantage.

Role- and context-specific knowledge

💡 When implementing AI literacy, organizations have to take into account their employees' background and role, the context in which the AI systems are to be used, and the perspective of affected persons.

❗ Beyond foundational knowledge, companies may thus have to invest in additional trainings for specific groups of employees.

➡️ What additional trainings to offer could depend on the role the organization is playing with regards to its AI systems (provider or deployer) and the type of AI systems it operates (high-risk or not).

Best Practices for Implementation

Best practices for implementation

✅ Legal knowledge: Familiarize your employees with relevant concepts of the AI Act.

➡️ Definition of AI systems
➡️ Roles and responsibilities along the lifecycle of AI
➡️ Opportunities, risks, and possible harms of AI
➡️ High-risk AI systems

✅ Technical knowledge: Create an inventory of AI systems, including who has access to which system, and train your employees how to use them accordingly.

✅ Role- and context-specific knowledge: Invest in further AI literacy measures depending on the organization's role (provider or deployer) and the nature of the AI systems (high-risk or not).

Frequently Asked Questions (FAQs)

FAQs

➡️ What fines are associated with non-compliance?
✅ There are no direct fines associated with non-compliance with Art. 4 AI Act.

➡️ Why should I bother implementing Art. 4 AI Act in that case?
✅ First, because it is a legal requirement regardless. Second, because you don't want to be in the awkward position where your AI systems cause harm, and it then turns out you did not train your employees appropriately. Third, the likelihood that your AI systems do cause harm is inevitably lower if your employees know how to use them effectively and ethically.

➡️ I have not yet started implementing Art. 4 AI Act. Am I in trouble?
✅ Not yet. In an AI Pact workshop on AI literacy in December 2024, the European AI Office suggested enforcement of AI literacy would not begin before August 2025.

➡️ I still have questions. Where can I find out more?
✅ The European AI Office will be hosting a webinar on AI literacy on February 20th from 10am-12pm.

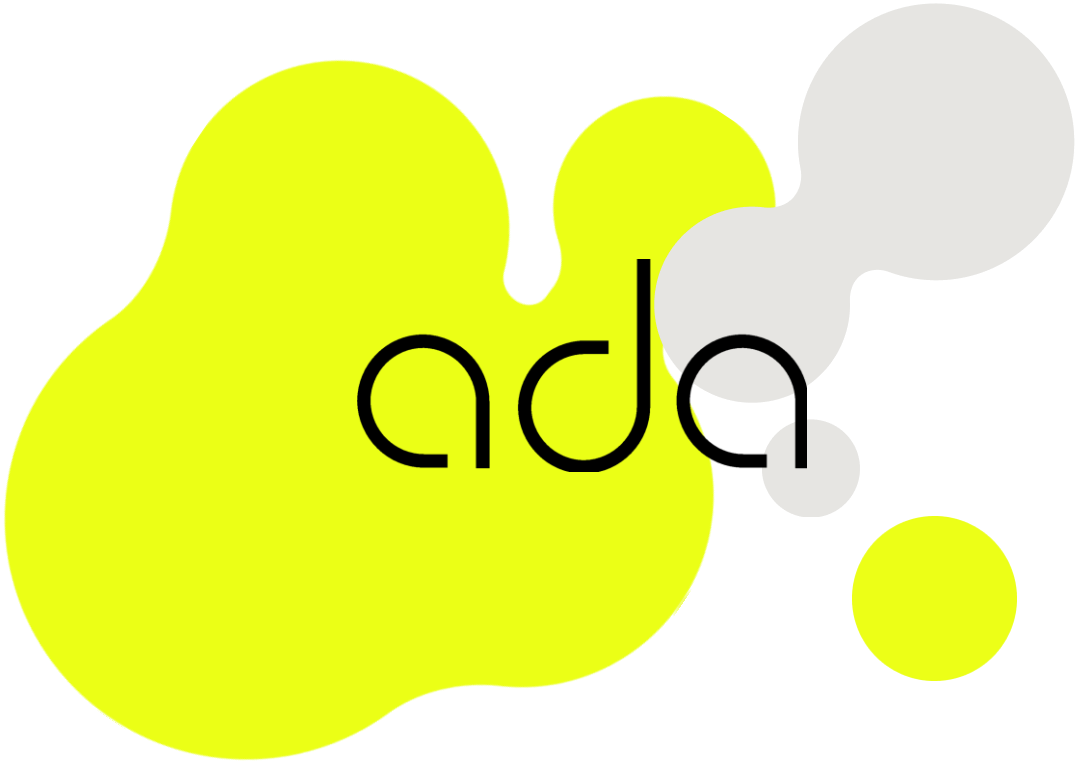
Thank you

Paula Cipierre
Director of Data Ethics & Innovation


+49 151 55152480


paula.cipierre@join-ada.com

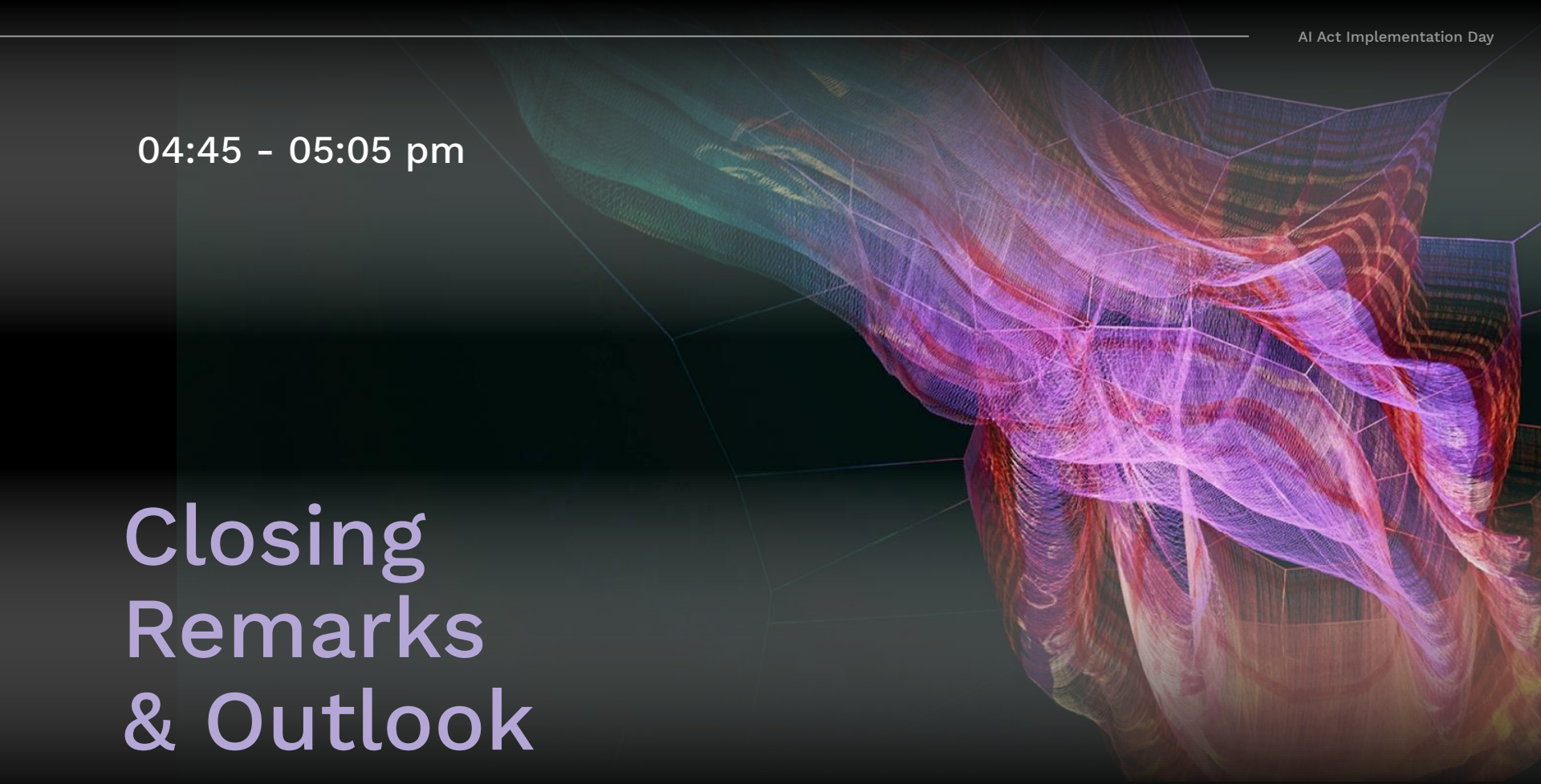

ada Learning GmbH
Graf-Adolf-Platz 15
40213 Düsseldorf



GROWTH RARELY HAPPENS ALONE.

04:45 - 05:05 pm

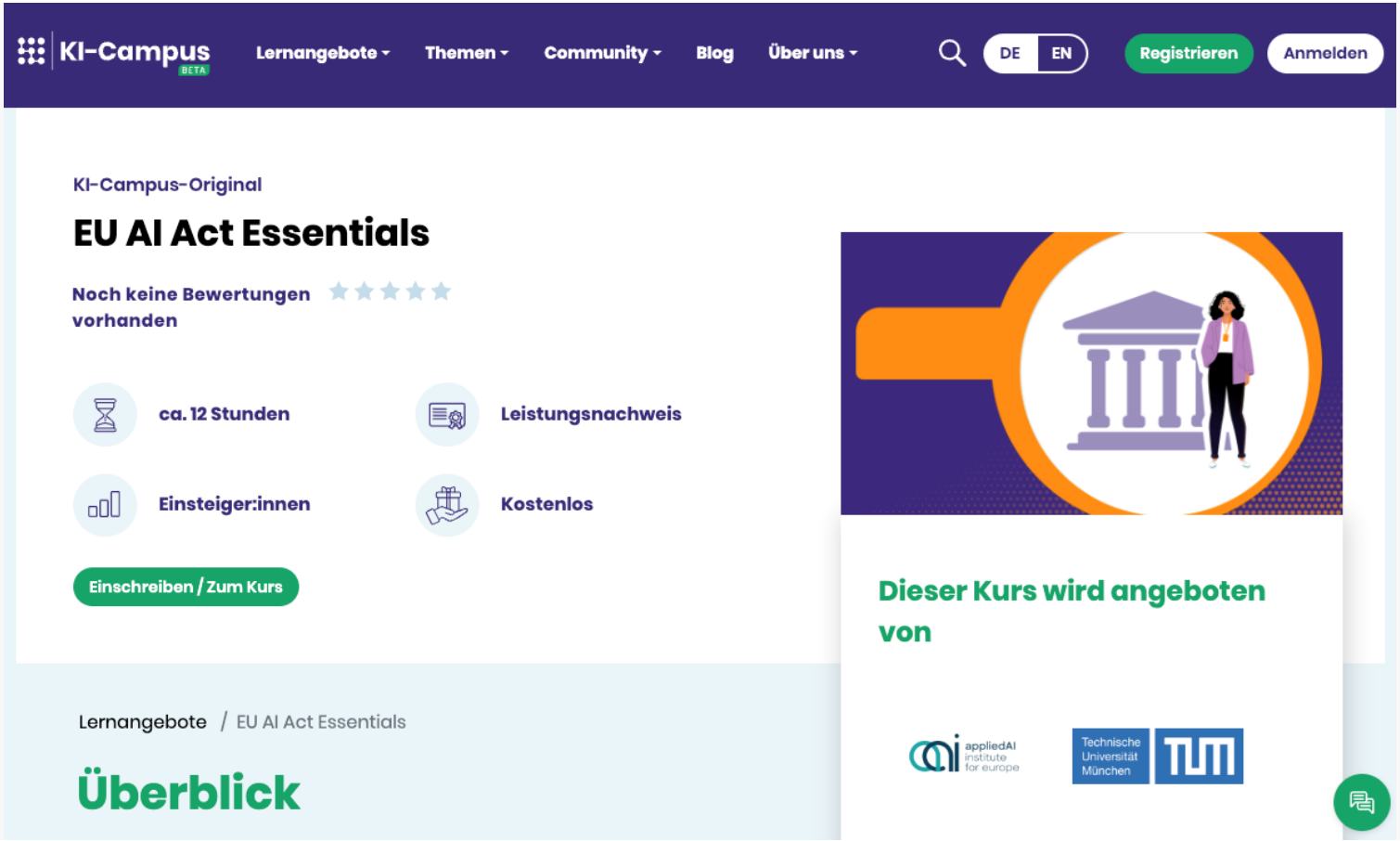
Closing Remarks & Outlook



Dr. Till Klein

Head of AI Regulation
appliedAI Institute for Europe

Launching soon: AI Act Essentials Online Course
A collaboration with KI-Campus and TUM



The Bavarian AI Act Accelerator is speeding up compliance with the AI Act while fostering AI Innovation

Mission

Accelerating the process of **AI Act compliance** by **linking research and practice** through the systematic identification of the **biggest challenges** facing businesses and public bodies and addressing them through new and existing services.

Objectives

1. Reduce compliance cost
2. Shortening time to compliance
3. Strengthening AI Innovation

Target groups

1. Startups
2. Small and medium sized enterprises
3. Public sector

Bayerisches Staatsministerium für Digitales

This project is funded by the Bavarian Ministry for Digital Affairs.

Thank you!