



UNIVERSITÄT  
DES  
SAARLANDES

INSTITUTE OF  
LEGAL INFORMATICS

# Law and Product Development: The Case of the EU AI Act

Engineering Process Days 2026 | Darmstadt, 18 May, 2026

# Prof. Dr. Georg Borges



- Chair of Civil Law, Legal Informatics, German and International Business Law and Legal Theory, Saarland University
- Director of Institute of Legal Informatics, Saarland University
- Judge, Oberlandesgericht Hamm [higher regional court] (2012-2015)
- Member of the Hörst-Görtz Institute for IT Security (HGI) (2005–2015)
- Member of the Board, EDV-Gerichtstag e.V. [German Association for eJustice]
- Member of the Board, Stiftung Datenschutz [Data Protection Foundation]
- Member, EU Commission Expert Group on “Liability and new technologies, New technologies formation” (2018-2020)
- Member, EU Commission „Expert Group on B2B Data Sharing” (2022-2025)
- Distinguished Visiting Professor, University of Johannesburg (since 2023)
- Visiting Professor, Keio University, Tokyo (since 2024)



# Institute of Legal Informatics – Fields of Research

- AI / Autonomous Systems
- Data Protection
- IT-Security
- Industry 4.0 / Cloud Computing
- Legal Informatics / Legal Tech
- Big Data
- eJustice / eGovernment
- [www.rechtsinformatik.saarland](http://www.rechtsinformatik.saarland)



**Amtsgericht 4.0**



**A-DigiKomp**



**MONTAGSPOST**



# Institute of Legal Informatics – Education and outreach

## ▪ Education

- Master's degree „IT and Law“ (LL.M.)
- Focus area „IT Law and Legal Informatics“
- Summer School „IT Law and Legal Informatics“
- Certificate „IT Law and Legal Informatics“

## ▪ Events

- Symposia/Workshops/Seminars
- E.g. GDPR! Data protection in practice.

## ▪ Services for the public

- GesetzMobil [collections of laws]
- JuraPush, BGH-Push [law and Federal Court of Justice newsletter]
- IT-Recht.Karriere [career portal]



# Master's degree (LL.M.) „Informationstechnologie und Recht“ [IT and Law]

- Interdisciplinary teaching
- 14 modules
- Part time studies possible
- Professors as mentors
- Study period: 1 year (~ 2 terms)





# SUMMER SCHOOL 2026

IT Law and Legal Informatics

INSTITUTE OF  
LEGAL INFORMATICS  
SAARLAND UNIVERSITY

Home

Topic Areas

Programme

How to apply

Support

FAQ

Information for Participants

Previous

Weitere Informationen unter  
[www.summerschool-itlaw.org](http://www.summerschool-itlaw.org)



# Agenda

## I. The EU AI Act at a glance

1. Overview
2. Addressees and obligations
3. General-purpose AI models (GPAI)
4. Transparency obligations and individual rights protection
5. Interim result

## II. The regulation of for high-risk AI systems

1. The concept of a high-risk AI system
2. The obligations of high-risk AI system providers
3. Role switch in high-risk AI systems

## III. AI Act - Strategies for Production Companies

## IV. Conclusion





# The EU AI Act at a glance



The EU AI Act at a glance



**Overview**

# AI regulation – the need and concept

## The current debate on AI regulation

PRESS RELEASE | Aug 1, 2024 | Brussels | 4 min read

### European Artificial Intelligence Act comes into force

**Key messages**  
The European Artificial Intelligence Act (AI Act), the world's first comprehensive regulation on artificial intelligence, enters into force. The AI Act is designed to ensure that AI developed and used in the EU is trustworthy, with safeguards to protect people's fundamental rights. The regulation aims to establish a harmonised internal market for AI in the EU, encouraging the uptake of this technology and creating a supportive environment for innovation and investment.

"The regulation aims to establish a harmonised internal market for AI in the EU, encouraging the **uptake of this technology** and creating a **supportive environment for innovation and investment.**"

regulations, including non-regulatory systems, high quality of data sets, logging of activity, detailed documentation, clear user information, human oversight, and a high level of robustness, accuracy, and cybersecurity. Regulatory sandboxes will facilitate responsible innovation and the development of compliant AI systems. Such high-risk AI systems include for example AI systems used for recruitment, or to assess whether somebody is entitled to get a loan, or to rate autonomous vehicles.

Press release, 1 August 2024



*Thierry Breton,  
Commissioner for  
Internal Market*

"With the entry into force of the AI Act, European democracy has delivered an **effective, proportionate** and **world-first framework** for AI, tackling risks and serving as a **launchpad for European AI startups.**"

# AI regulation – the need and concept

## The current debate on AI regulation

*Zurück auf den Boden der Tatsachen in der KI-Regulierung*

Von Robert Mayr

D  
Gescheitert ist die Utopie, die EU könnte zum regulatorischen Weltgewissen werden.

**Frankfurter Allgemeine**  
ZEITUNG FÜR DEUTSCHLAND

**BUSINESS**

**JD Vance warns 'massive' European regulation may kill AI, rips 'authoritarian censorship'**



"We believe that excessive regulation of the AI sector could kill a transformative industry just as it's taking off [...]"

# The EU AI Act at a glance

## The Digital Omnibus on AI

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

- Postponement of the temporal scope part of the Regulation
- Correction of errors / Minor amendments

➔ no fundamental change



# The EU AI Act at a glance

## Regulatory framework and contents

- **Exceptionally broad area of application ('AI systems')**
- **Four regulatory concepts of AI with different protection concepts**
  - (1) Prohibition of certain AI practices (Art. 5)

*Examples: Subliminal techniques, harmful and detrimental social scoring, biometric identification procedures in public spaces*
  - (2) Protection against high-risk AI systems (Chapter III, Art. 6–49)
    - » Obligation of the provider for risk and quality management
  - (3) Transparency obligations for certain AI systems (Art. 50)

*Examples: labelling of AI systems as such, disclosure of deep fakes*
  - (4) No requirements for other AI systems/ Infrastructure for AI development
- **Differentiation: AI systems, high-risk AI systems, GPAI models**

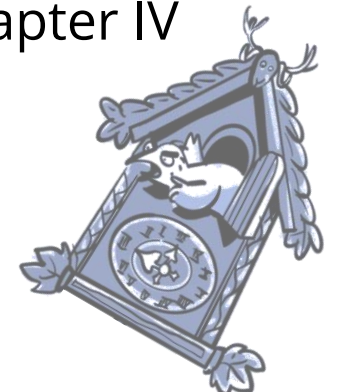
# The EU AI Act at a glance

## The scope of application over time



### ■ Application over time in four steps, Art. 113

- Chapters I and II (Prohibitions, Art. 5)
  - » February 2025
- Chapter III Section 4 (notifying authorities, notified bodies), Chapter V (General purpose AI models), Chapter VII (Governance), Chapter XII (Penalties), Article 78 (Confidentiality)
  - » August 2025
- Chapter III Art. 6 para. 2 (High-risk AI systems referred to in Annex III), Chapter IV (Transparency obligations), VI (Measures in support of innovation)
  - » *current AI Act*: August 2026 » *AI-Omnibus-R*: Dezember 2027
- Chapter III, Art. 6 para. 1 (High-risk AI systems according to Annex I)
  - » » *current AI Act*: August 2027 » *AI-Omnibus-R*: Dezember 2028



# The EU AI Act at a glance

## Material scope of application

- **AI systems**
  - Definition 'AI system' (Art. 3 no. 1): software, based on machine learning
- **General-purpose AI models** (Art. 3 no. 63): content of neural networks
- **Important exceptions and restrictions:**
  - Research and development, Art. 2 para. 6
  - Data protection, Art. 2 para. 7 (GDPR has priority)
  - Consumer protection, product safety, Art. 2 para. 9
  - Use of AI systems in the course of a purely personal non-professional activity, Art. 2 para. 10



# The EU AI Act at a glance

## The territorial scope of application

- **Broad extraterritorial scope of application, Art. 2 para. 1**
  - 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, lit. a)
  - Deployers of AI systems that have their place of establishment or are located within the Union, lit. b)
  - Providers and deployers of AI systems that have their place of establishment or are **located in a third country**, where the **output** produced by the AI system is **used in the Union**, lit. c)



# The EU AI Act at a glance

## Regulatory framework and contents

<b>Content of the AI Act at a glance</b> 113 articles in 13 chapters and 13 annexes	
<b>Chapter I</b>	General provisions (Art. 1- 4)
<b>Chapter II</b>	Prohibited AI practices (Art. 5)
<b>Chapter III</b>	High-risk AI systems (Art. 6 – 49)
<b>Chapter IV</b>	Transparency obligations for providers and deployers of certain AI systems (Art. 50)
<b>Chapter V</b>	General-purpose AI models (Art 51 - 56)
<b>Chapter VI</b>	Measures in support of innovation (Art. 57 – 63)
<b>Chapter VII</b>	Governance (Art. 64 – 70)
<b>Chapter VIII</b>	EU database for high-risk AI systems (Art. 71)
<b>Chapter IX</b>	Post-market monitoring, information sharing and market surveillance (Art. 72 – 94)
<b>Chapter X</b>	Codes of conduct and guidelines (Art. 95 - 96)
<b>Chapter XI</b>	Delegation of power and committee procedure (Art. 97 - 98)
<b>Chapter XII</b>	Penalties (Art. 99 - 101)
<b>Chapter XIII</b>	Final provisions (Art. 102 - 113)






The EU AI Act at a glance

**Addressees and obligations**



# The EU AI Act at a glance

Fear		1 + 2 + 4 + 5 + 7 + 20 + 25	Eyebrows raised and pulled together, upper eyelid raised, lower eyelid tense, lips parted and stretched
Happiness		6 + 7 + 12 + 25 + 26	Duchenne smile
Interest		1 + 2 + 12	Eyebrows raised, slight smile

Barrett et al, *Emotional Expressions Reconsidered*, p. 7

## Example:

- Emotional AI Ltd, Tokyo, develops the AI system „*Readme*“ to recognise emotions for interviews of all kinds
- The system is operated by AI Analytics, Inc., San Francisco and used for analyses of job interviews as a service for employers
- Siemens AG, Munich, has AI Analytics create analyses for decisions on hiring applicants

- **AI Act is applicable (Art. 2 - Use of the output in the EU)**
- Emotional AI is the provider of the AI system
- AI Analytics is the deployer of the AI system



The EU AI Act at a glance



**General-purpose AI models (GPAI)**

# The general-purpose AI (GPAI) model

## Definition

- Definition in Art. 3 para. 63

### Article 3

#### *Definitions*

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

- Very vague definition
- Specified as a matter of size by Commission guidelines

# The general-purpose AI (GPAI) model

## Obligations of providers of GPAI models

- **Obligations under Art. 53 para. 1**
  - Technical documentation, para. 1(a)
  - Information to providers of AI systems, para. 1(b)
  - Comply with Union copyright law and related rights, para. 1(c)
  - Publicly accessible summary of training data, para. 1(d)
- **Exemption for open-source models, para. 2**



# The general-purpose AI (GPAI) model

## The GPAI model with systemic risks

- **Definition in Art. 51**

### Article 51

#### *Classification of general purpose AI models as general purpose AI models with systemic risk*

1. A general-purpose AI model shall be classified as a general-purpose AI model with systemic risk if it meets any of the following requirements:

- (a) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks;
- (b) based on a decision of the Commission, ex officio or following a qualified alert from the scientific panel, it has capabilities or an impact equivalent to those set out in point (a) having regard to the criteria set out in Annex XIII

- **Obligations set out in Art. 55**

- - Evaluation of the model, para. 1 lit. a)
- - Risk assessment, para. 1 lit. b)
- - Information about “serious incidents,” para. 1 lit. c)
- - Cybersecurity, para. 1 lit. d)



The EU AI Act at a glance



**Transparency obligations and individual rights protection**

# Transparency obligations

## Overview

- **Transparency obligations for providers**
  - Clarification of interaction with an AI system to the natural person concerned (Art. 50(1))
  - Obligation of AI system providers to apply watermarking (Art. 50(2))
- **Transparency obligations for deployers**
  - Reference to the use of emotion recognition and biometric categorisation (Art. 50(3))
  - Disclosure of deepfakes (Art. 50(4) subpara. 1)
  - Disclosure of AI processing of published texts for information on matters of public interest (Art. 50(4) subpara. 2)

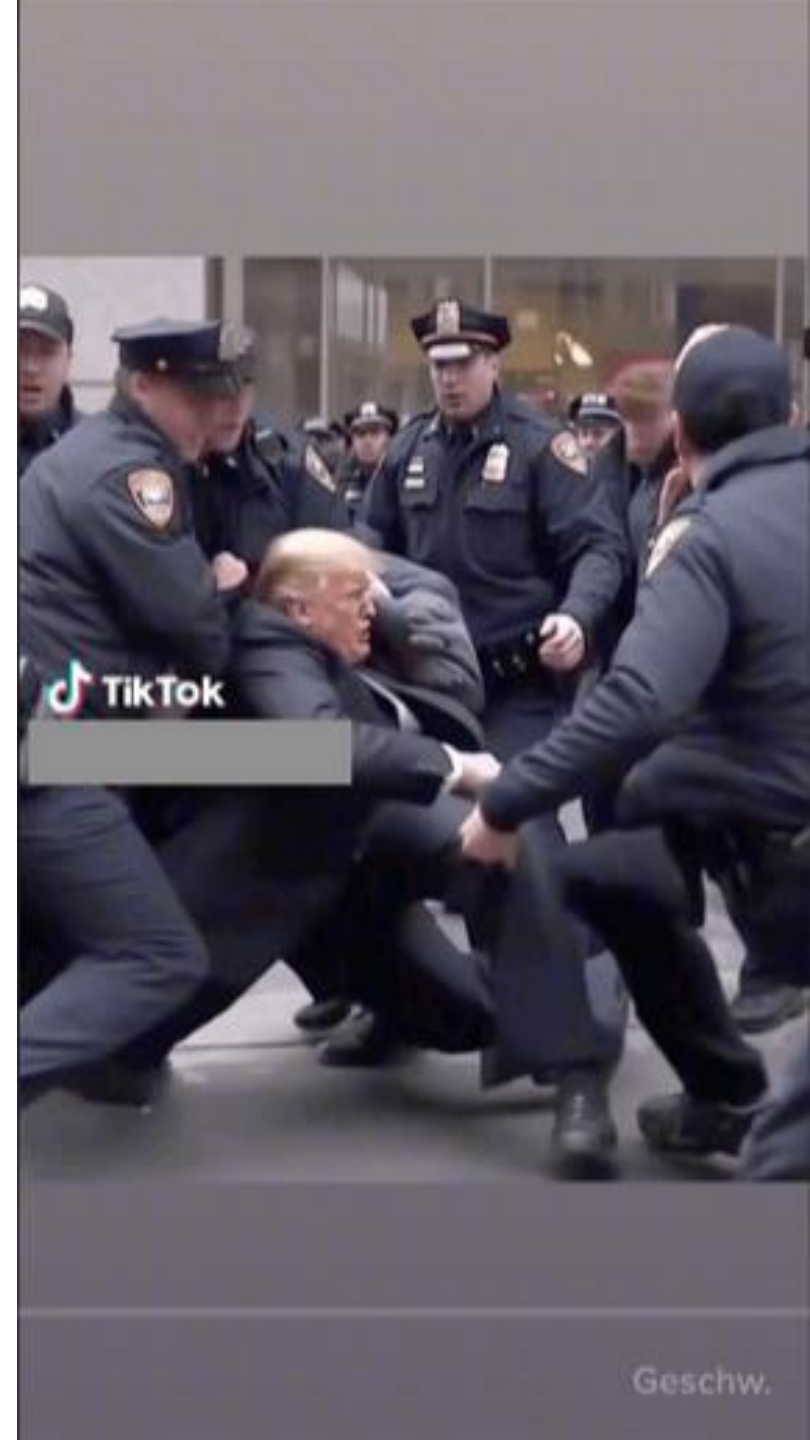
# Transparency obligations

## Conceptual regulatory gaps

- No regulation for the use of AI-generated content
- No regulation for communication through AI systems

FAKTENCHECK

**Künstliche Intelligenz generiert  
Bilder von Donald Trumps  
Festnahme – die gab es aber gar  
nicht**



# Individual rights protection

- **Right of appeal for everyone, Art. 85**
- **Right to explanation, Art. 86**
  - Scope of application: Decisions based on the output of an AI system
  - Entitled: Data subject
  - Obligated: Deployer of an AI system
  - Subject:
    - Role of the AI system in the decision-making process
    - Elements of the decision





The EU AI Act at a glance



**Institutional rules**

# Institutional rules

## Establishment of new authorities and facilities

### EU level

- AI Office (Art. 64)
- European Artificial Intelligence Board (Art. 65)
- Advisory forum (Art. 67)
- Scientific panel of independent experts (Art. 68)
- EU database for high-risk AI systems (Art. 71)

### National bodies of the Member States

- Notifying authority (Art. 70)
- Market surveillance authority (Art. 70)





# Institutional rules

## STANDARDS AND CERTIFICATION

### Standards

- Harmonised standards, Art. 40
- Common specifications, Art. 41

### Certification

- Notifying authority, Art. 28
- Notified bodies, Art. 31
- Procedure for notification of competent bodies, Art. 31
- Procedure for conformity assessments by notified bodies, Art. 34

## FRAMEWORK FOR SELF-REGULATION

### Codes of Conduct, Art. 95

- Codes for voluntary application of requirements
- Codes drawn by individual providers, groups of providers, stakeholders, academia etc.

### Codes of Practice, Art. 56

- Standards for GPAI Models
- Development of codes by providers and authorities

### Self-assessment for high-risk AI systems

- Internal conformity assessment, Art. 43
- Declaration of conformity, Art. 47



The EU AI Act at a glance



**Interim result**

# The EU AI Act at a glance

## Interim result

The AI Act...

- ... is **not a comprehensive legal framework** for AI
  - ... does not include liability
  - ... does not include automated decisions
  - ... does not regulate data protection aspects or intellectual property rights
- ... is a "**product safety law for AI**" with additions
  - Prohibitions
  - Transparency
  - Individual rights





# The regulation of high-risk AI systems

# The EU AI Act at a glance

## Risk management for high-risk AI systems

Chapter III High-risk AI systems (Art. 6 - 49)	
<b>Section 1</b>	Categorisation of AI systems as high-risk AI systems (Art. 6 - 7)
<b>Section 2</b>	Requirements for high-risk AI systems (Art. 8 - 15)
<b>Section 3</b>	Obligations of providers and deployers of high-risk AI systems and other parties involved (Art. 16 - 27)
<b>Section 4</b>	Notifying authorities and notified bodies (Art. 28 - 39)
<b>Section 5</b>	Standards, conformity assessment, certificates, registration (Art. 40 - 49)

- Demanding requirements for high-risk AI systems
- Extensive obligations for providers and deployers of high-risk AI systems
- Supervision much stricter for other AI systems



The regulation of high-risk AI systems

**The concept of high-risk AI systems**

# Risk management for high-risk AI systems

## Terms and concepts

- 1. AI systems as a safety component of a regulated product, Art. 6 para. 1 in conjunction with Annex I**
  - » AI system as a high-risk AI system if the product is subject to European product safety legislation and subsequently requires a conformity assessment by an independent third party

Objective of the AI Act:	Supplement to European product safety legislation with regard to AI systems
--------------------------	---

# Risk management for high-risk AI systems

## Terms and concepts

### 2. AI systems for use in high risk areas, Art. 6 para. 2 in conjunction with Annex III

- » Two-tier system for categorisation as a high-risk AI system
  - 1) Use of the output of the AI system in a high-risk area
  - 2) Specific risks posed by the system, Art. 6 para. 3

Objective of the AI Act:	Product safety law for software posing risks for personal rights
--------------------------	--

# Risk management for high-risk AI systems

## The concept of the high-risk AI system

### High-risk areas of Annex III

<b>Number 1</b>	Biometrics
<b>Number 2</b>	Critical infrastructure
<b>Number 3</b>	Education and vocational training
<b>Number 4</b>	Employment, workers' management and access to self-employment
<b>Number 5</b>	Access to and enjoyment of essential private services and essential public services and benefits
<b>Number 6</b>	Law enforcement
<b>Number 7</b>	Migration, asylum and border control management
<b>Number 8</b>	Administration of justice and democratic processes

# Risk management for high-risk AI systems

## High-risk AI system after use of the output (Art. 6 para. 2)

 **Complex chain of stakeholders in high-risk AI systems**

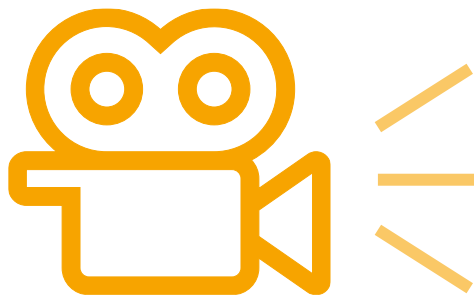
*Example: Video interview*



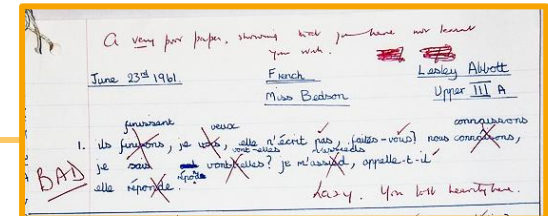
# Risk management for high-risk AI systems

## High-risk AI system after use of the output (Art. 6 para. 2)

- Special feature of the concept: **dependent on the use of the output**
- *Example:* Video emotion recognition
  - Use for training » simple AI system
  - Use for assessment in study/work » High-risk AI system



```
22  in = ...
23  again = false;
24  getline(cin, sInput);
25  system("cls");
26  stringstream(sInput) >> dblTemp;
27  ilength = sInput.length();
28  if (ilength < 4) {
29    again = true;
    continue;
    cout[ilength - 3] != '.' {
```





The regulation of high-risk AI systems



**The obligations of high-risk AI system providers**

# Risk management for high-risk AI systems

## The obligations of providers of high-risk AI systems

- **Obligation to manage the risk, Art. 16**
  - Risk management, Art. 9
  - Testing and, if necessary, certification of high-risk AI systems, Art. 9
  - Data governance, Art. 10
  - Technical documentation, Art. 11
  - Record-keeping, Art. 12
  - Ensuring human oversight, Art. 14
  - Cybersecurity, Art. 15
- **Quality management system, Art. 17**
- **Monitoring**





The regulation of high-risk AI systems



**Role switch in high-risk AI systems**

# Risk management for high-risk AI systems

## Role switch in high-risk AI systems



### Role changes in high-risk AI systems

Change of roles in the event of a substantial modification, insofar as attributable to the provider, Art. 25 (1) (b) AI Act

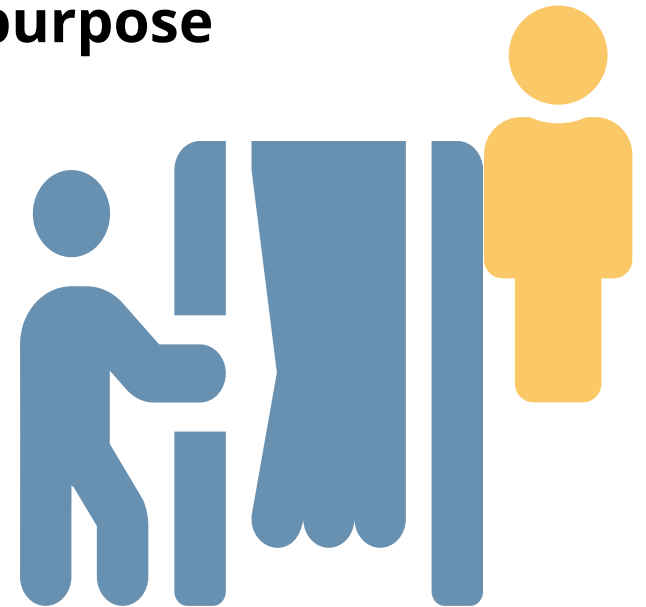
Change of roles in the event of a change of purpose, insofar as attributable to the operator, Art. 25 (1) (c) AI Act

# Risk management for high-risk AI systems

## The change of roles in high-risk AI systems

### Art. 25: Change of role from user to provider

- **Significant problems with modification and change of purpose**
- **Modification to the AI system**
  - » Can trigger the classification as “provider”
  - » Problem: AI systems are regularly modified



# Risk management for high-risk AI systems

## Role switch in high-risk AI systems

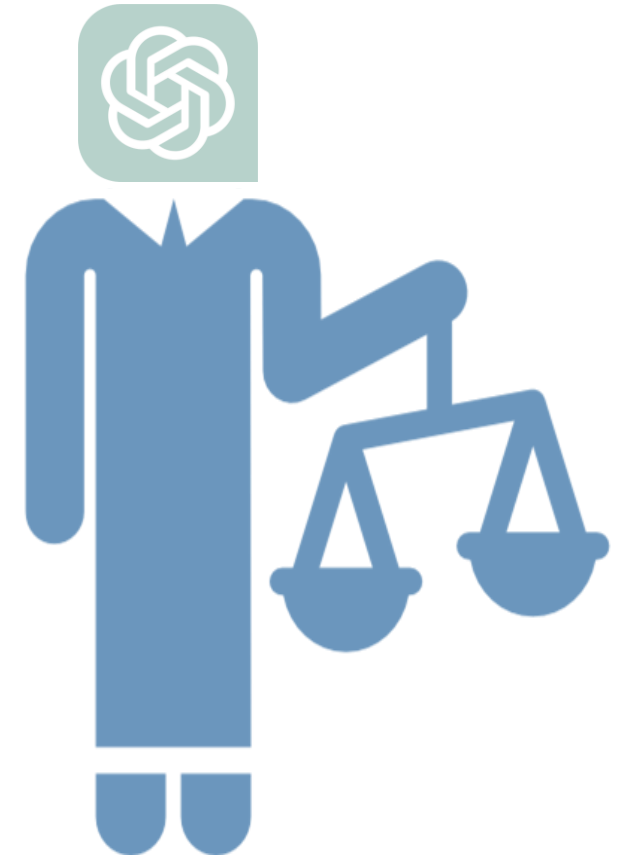
- **Change of purpose**

- » can trigger the classification as provider

- *Risk*: Change of purpose due to change in area of use

- *Examples*:

- Lawyer uses ChatGPT/AI tool for the statement of claim
- Judge uses ChatGPT/AI tool for the judgment





# AI Act - Strategies for Production Companies

# AI Act - Strategies for Production Companies

## Challenge: Actionable legal information for engineers



## Key Requirements

### Actionable legal information

- = Decision-related information
  - at the moment where decisions are made
  - relevant for the decision-making
  - understandable for non-lawyers

# AI Act - Strategies for Production Companies

## Practical information for SMEs



5 Methoden im Detail

Design Prinzipien Methode Checkliste Best Practice Beispiel

### 5.24 EaaS und KI-Verordnung (AI Act)

**Rechtliche Aspekte**

**Orientierungsfragen**

- Wird ein KI-System hergestellt oder genutzt?
- Ist das KI-System im Hochrisiko-Bereich verwendet?
- Sind die Anforderungen an Hochrisiko-KI-Systeme erfüllt?
- Wird ein KI-System zur Kommunikation mit Dritten eingesetzt?

1 - Kernidee formulieren 2 - Zielgruppen verstehen 3 - Leistungsangebot ableiten 4 - Organisation anpassen 5 - Partner identifizieren 6 - Machbarkeit abschätzen

**Zielsetzung**

- Kenntnis der Anwendbarkeit der KI-Verordnung bei EaaS-Diensten
- Kenntnis der Pflichten der KI-Verordnung für Anbieter und Nutzer von EaaS-Diensten

**Voraussetzung**

- Kenntnis der Verwendung von KI-Systemen bei EaaS-Diensten
- EaaS-Equipment als KI-System?
  - wenn ja: EaaS-Anbieter ist Anbieter des KI-Systems
  - wenn ja: EaaS-Nutzer ist (i.d.R.) nicht Anbieter, sondern Nutzer des KI-Systems
- Analysertools des EaaS-Anbieters als KI-System?
  - wenn ja: EaaS-Anbieter ist Anbieter oder Nutzer (Deployer) des KI-Systems
  - wenn ja: Dienstleister als KI-System? (Deployer) des KI-Systems
- Analysertools eines Dienstleisters als KI-System?
  - wenn ja: Dienstleister ist Anbieter oder Nutzer (Deployer) des KI-Systems
  - EaaS-Anbieter und EaaS-Nutzer sind weder Anbieter noch Nutzer des KI-Systems (sondern Empfänger einer Dienstleistung)

**Hintergrund**

Die KI-Verordnung (KI-VO) wird voraussichtlich im 1. Halbjahr 2024 verabschiedet und ist voraussichtlich ab 2026 in allen Teilen anwendbar, teilweise auch früher. Die Verordnung gilt in der gesamten EU und betrifft in erster Linie Hersteller und Nutzer von KI-Systemen, daneben auch Verkäufer und Importeure.

Die KI-Verordnung enthält vor allem drei wichtige Regelungsbereiche:

- Verbot bestimmter KI-Anwendungen (z.B. social scoring), Art. 5
- Pflichten zum Risiko-Management für Hochrisiko-KI-Systeme und für General Purpose AI Models
- Transparenzpflichten zur Kooperation mit Dritten und in Bezug auf deep fakes

Für die meisten KI-Systeme (ca. 80-90 Prozent) gelten nach der KI-Verordnung keine besonderen Pflichten. Die Einhaltung der Pflichten der KI-VO wird durch Aufsichtsbehörden überwacht. Die Aufsichtsbehörden haben scharfe Eingriffsbefugnisse und können hohe Bußgelder (max. 3 Prozent des jährl. Konzernumsatzes) verhängen.

**Die KI-Verordnung (AI Act)**

Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung) und zur Änderung bestimmter Rechtsakte der Union

- Gesetzgebungsvorschlag der EU-Kommission vom 21.4.2021 (COM(2021) final)
- Erlass und Inkrafttreten erwartet für 1. Halbj. 2024
- Geltung der KI-VO voraussichtlich ab 2026

71

5 Methoden im Detail

### 5.24 EaaS und KI-Verordnung (AI Act)

**KI-Systeme:** Begriff def. in Art. 3 Abs. 1 KI-VO = »maschinenbasiertes System«, das mit einer gewissen Autonomie agiert und das Ergebnisse erzeugt, die seine Umgebung beeinflussen können

- der Sache nach: Alle Software, die auf machine learning beruht und Hardware, die solche Software enthält

**Hochrisiko-KI-System:** Begriff def. in Art. 6 KI-VO = 2 Gruppen von Software

- (1) KI-System, das ein Produkt oder (häufiger) Sicherheitskomponente eines Produkts ist, das den in Anhang II genannten gesetzlichen Regeln des europäischen Produktsicherheitsrechts unterliegt
- (2) KI-System, das für einen in Anhang III Nr. 1-9 genannten Zweck verwendet wird

der Sache nach = »kritische« Bereiche, Überwiegend: Software zur Bewertung von Personen (z.B. Arbeitsbereich, Soziales, Ausbildung, Polizei/Justiz etc.)

**Anbieter (=Provider-) von KI-Systemen:** Begriff def. in Art. 3 Abs. 2 KI-VO = eine Person, die ein KI-System herstellt oder herstellen lässt und unter eigenem Namen vertreibt oder nutzt

- der Sache nach der Hersteller des KI-Systems

**Nutzer (=Deployer-):** Begriff def. in Art. 3 Abs. 3 KI-VO = eine Person, die ein KI-System in eigener Verantwortung nutzt

- der Sache nach der Betreiber des KI-Systems (das Unternehmen, nicht der Arbeitnehmer)

**Problemstellung und Leitlinien**

Beim EaaS sind zunehmend sowohl das Equipment (Software-Komponenten) als auch Analysysteme als KI-System einzustufen. Daher wird die KI-VO häufig anwendbar sein. Die Bedeutung der KI-VO für EaaS im Einzelnen kann derzeit nicht zuverlässig beurteilt werden. Es können aber bereits zentrale Probleme und Lösungsansätze benannt werden.

**1 Verletzung der Bestimmungen der KI-VO**

**Problem:** Der Anwendungsbereich der KI-VO ist sehr weit gefasst; KI-Systeme sind in fast allen Produkten enthalten. Die Bestimmungen der KI-VO sind vielfach unscharf, eine Anwendung der spezifischen Regeln kann leicht eintreten, ohne dass dies dem Hersteller oder Nutzer (deployer) bewusst ist. In diesem Fall werden die Bestimmungen der KI-VO oft nicht eingehalten. Dies kann aufsichtsrechtliche Maßnahmen und hohe Bußgelder zur Folge haben.

**Lösungsansatz:**

- Klärung der Anwendbarkeit der KI-VO
- Klärung der Anwendbarkeit der zentralen Regelungsbereiche (Verbot, Risikomanagement, Transparenz)
- Klärung und Befolgung der konkreten Anforderungen

**2 Die Rolle des EaaS-Anbieters im Kontext der KI-VO**

Der EaaS-Anbieter kann je nach Sachverhalt die Rolle des Anbieters als auch des Nutzers von KI-Systemen einnehmen. Der EaaS-Anbieter kann unwissentlich in die Rolle des Anbieters gelangen. In diesem Fall kann es sein, dass er Anforderungen der KI-VO unwissentlich verletzt und sich Sanktionen aussetzt. Die Kenntnis und Wahrung der Rolle ist zu jedem Zeitpunkt dringend erforderlich.

Drei Konstellationen sind zu unterscheiden:

- Der EaaS-Anbieter stellt ein KI-System selbst her oder lässt es herstellen, um es im eigenen Namen zu vertreiben oder zu nutzen.
- Hier ist der EaaS-Anbieter der Anbieter des KI-Systems. Wenn das KI-System im Hochrisiko-Bereich eingesetzt werden soll, sind die Pflichten für Hochrisiko-KI-Systeme zu beachten.
- Der EaaS-Anbieter nutzt das von einem Dritten hergestellte KI-System, um das EaaS anzubieten.
- Hier ist der EaaS-Anbieter der Nutzer des KI-Systems. Wenn er das KI-System jedoch wesentlich modifiziert oder zu einem anderen als dem vom Hersteller vorgesehenen Zweck verwendet, wird er nach Art. 28 KI-VO selbst zum Anbieter (Provider) des KI-Systems. Bei Verwendung im Hochrisiko-Bereich gelten die Pflichten für Hochrisiko-KI-Systeme.

72

### 5.24 EaaS und KI-Verordnung (AI Act)

- Der EaaS-Anbieter betreibt das von einem Dritten hergestellte KI-System im eigenen Namen.
- Hier ist der EaaS-Anbieter der Anbieter des KI-Systems. Es gilt dasselbe wie im Fall der Herstellung des KI-Systems durch den EaaS-Anbieter selbst.

**Lösungsansatz:**

- Vermeidung des unbeabsichtigten Einsatzes im Hochrisiko-Bereich
- Es ist darauf zu achten, in welchem Bereich (Hochrisiko-Bereich?) das System eingesetzt werden soll. Beim Vertrieb von KI-Systemen sind die Einsatzzwecke klar zu bestimmen, der Einsatz im Hochrisiko-Bereich ist ggf. auszuschließen.
- Vermeidung des unbeabsichtigten Rollenwechsels
- Der Rollenwechsel vom Nutzer zum Anbieter eines KI-Systems ist bei Verwendung im Hochrisiko-Bereich ggf. zu vermeiden, da die Pflichten für Hochrisiko-KI-Systeme gelten.

**3 Unwissentliche Verwendung von KI-Systemen im Hochrisiko-Bereich**

**Problem:** Die Verwendung von KI-Systemen folgt in der arbeitstäglichen Wirtschaft auf nachfolgenden Etappen, zum einen durch nachfolgende Hersteller in der Produktionskette, zum anderen durch den Nutzer (Deployer). Nach dem Konzept der KI-VO ist



### Equipment-as-a-Service (EaaS)

#### Methodenleitfaden zur praktischen Anwendung des EaaS-Canvas

Holger Kett | Dimitri Evckenko | Jürgen Falkner | Mirko Schneider | Stephan Nebauer | Oliver Schöllhammer | Jens Neuhüttler | Georg Borges

# AI Act - Strategies for Production Companies

## Practical information for SMEs

- **Actionable legal Information information for Engineers**
  - Key questions
  - Checklist
  - Background information
  - Possible solutions

### 5.21 EaaS und Datenschutz

treten. Soweit weder eine Auftragsverarbeitung noch eine Rechtfertigung sichergestellt werden kann, darf die Datenverarbeitung, dh die Erbringung der jeweiligen Dienstleistung, nicht erfolgen. Für die unter (1) identifizierten Vorgänge liegt im Fall der Auftragsverarbeitung die Verantwortlichkeit für die Datenverarbeitung beim EaaS-Nutzer, der EaaS-Anbieter ist insoweit Auftragsverarbeiter. Bei den unter (2) identifizierten Vorgängen handelt der Dienstleister als Unterauftragsverarbeiter des EaaS-Anbieters. Dies ist zulässig, wenn explizit eine Unterauftragsverarbeitung vereinbart und implementiert wird.

#### Lösungsansatz:

- Prüfung, ob und inwieweit die unter (1) und (2) identifizierten Datenverarbeitungsvorgänge als Auftragsverarbeitung gestaltet werden können
- Implementierung der Auftragsverarbeitung im Verhältnis zum EaaS-Nutzer
- Implementierung der Auftragsverarbeitung im Verhältnis zu Dienstleistern des EaaS-Anbieters

#### Ergebnisse

- Klarheit über Anforderungen der DSGVO an Datenverarbeitung im EaaS
- Auflistung identifizierten Maßnahmen zur datenschutzkonformen Gestaltung von EaaS



# AI Act - Strategies for Production Companies



The million-dollar question: When should you call a lawyer?



Product idea	✓
Prototype	✓
Product distribution	✓
Complaint	✓
Claim for damages	✓

# AI Act - Strategies for Production Companies

## Law as a do-it-yourself concept

		if (+)	if (-)
<b>Scope of production</b>	<b>Products containing AI components</b>		
	<b>AI systems / large AI models</b>		
<b>Intended use of the product</b>	<b>Are the products subject to a ban?</b>		
	<b>Does the AI system's intended use involve human contact?</b>		
	<b>Is it a general-purpose AI system?</b>		
	<b>Is it a product in a regulated sector?</b>		
	if +: Need for third-party conformity assessment?		
	if + AI system = safety component?		
	<b>AI system with potential use in high-risk areas?</b>		

# AI Act - Strategies for Production Companies

## Surviving in a High-Risk Environment



### Resources

Harmonised standards and standardisation documents (Art. 40 AI Act)

Common specifications (Art. 41 AI Act)

Presumption of conformity with certain requirements (Art. 42 AI Act)

Codes of practice (Art. 56 AI Act)

Guides

AI regulatory sandboxes (Art. 57 AI Act)

Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes (Art. 60 AI Act)

AI Office (Art. 64 AI Act)

Measures for providers and deployers, in particular SMEs, including start-ups (Art. 62 AI Act)

Single information platform (Art. 62 Abs. 3 lit. b)

Derogation for micro-enterprises within the meaning of Recommendation 2003/371/EC (Art. 63 AI Act)

Drafting of statements, recommendations and written contributions

Codes of conduct and guidelines (Chapter 10 of the AI Act)

Institute of legal informatics



**Conclusion**

# Conclusion

- **“Europe – A surprisingly AI-friendly environment”**



Presentation Borges,  
Tokyo 28th March  
2026

- **AI Act – a barking dog never bites**

- Reduced and reasonable duties for providers and deployers of AI products
- Challenge: legal certainty and access to legal information for producers
- Key actions:
  - Involving lawyers (the „legal design guys“) at an early stage
  - Providing actionable information for engineers





# Thank you very much!

**Prof. Dr. Georg Borges**

georg.borges@uni-saarland.de | [www.rechtsinformatik.saarland](http://www.rechtsinformatik.saarland)



## ...further reading:

*Borges, G.:*  
**Die europäische KI-Verordnung (AI Act) - Teil 1 Überblick, Anwendungsbereich und erste Einschätzung, CR 2024, 497 ff.**

*Borges, G.:*  
**Die europäische KI-Verordnung (AI Act) Teil 2 - Risikomanagement für Hochrisiko-KI-Systeme, CR 2024, 565 ff.**

*Borges, G.:*  
**Die europäische KI-Verordnung (AI Act) Teil 3 - Transparenzpflichten, Durchsetzung, Gesamtbewertung, CR 2024, 633 ff.**

