SPIRIT LEGAL®

KI & Datenschutz

Basics

WordCamp | Leipzig | 01. Juli 2023

Agenda

I. Datenschutz | DSGVO

1. Grundbegriffe
2. Rollenverteilung
3. Rechtsgrundlagen
4. Grundsätze und Pflichten

II. Künstliche Intelligenz | KI-VO

1. Wo stehen wir gerade?
2. Aufbau und Grundsätze
3. Rollenverteilung
4. Die Pflichten

III. Theorie anhand zweier Praxisbeispiele

Es geht los!

Die DSGVO-Basics, ohne die man wirklich nicht auskommt

Auf wen findet die DSGVO Anwendung?

- Die DSGVO findet Anwendung auf Unternehmen und Einrichtungen
  - mit einer Niederlassung in der EU („boots on the ground“);
  - die Waren und Dienstleistungen in der EU anbieten;
  - die das Verhalten von Menschen in der EU überwachen, egal von wo aus.
- Die DSGVO ist seit 2018 ein Vorbild für weltweite Datenschutzgesetze, z.B. in Brasilien, Japan und den USA

Wann findet die DSGVO Anwendung?

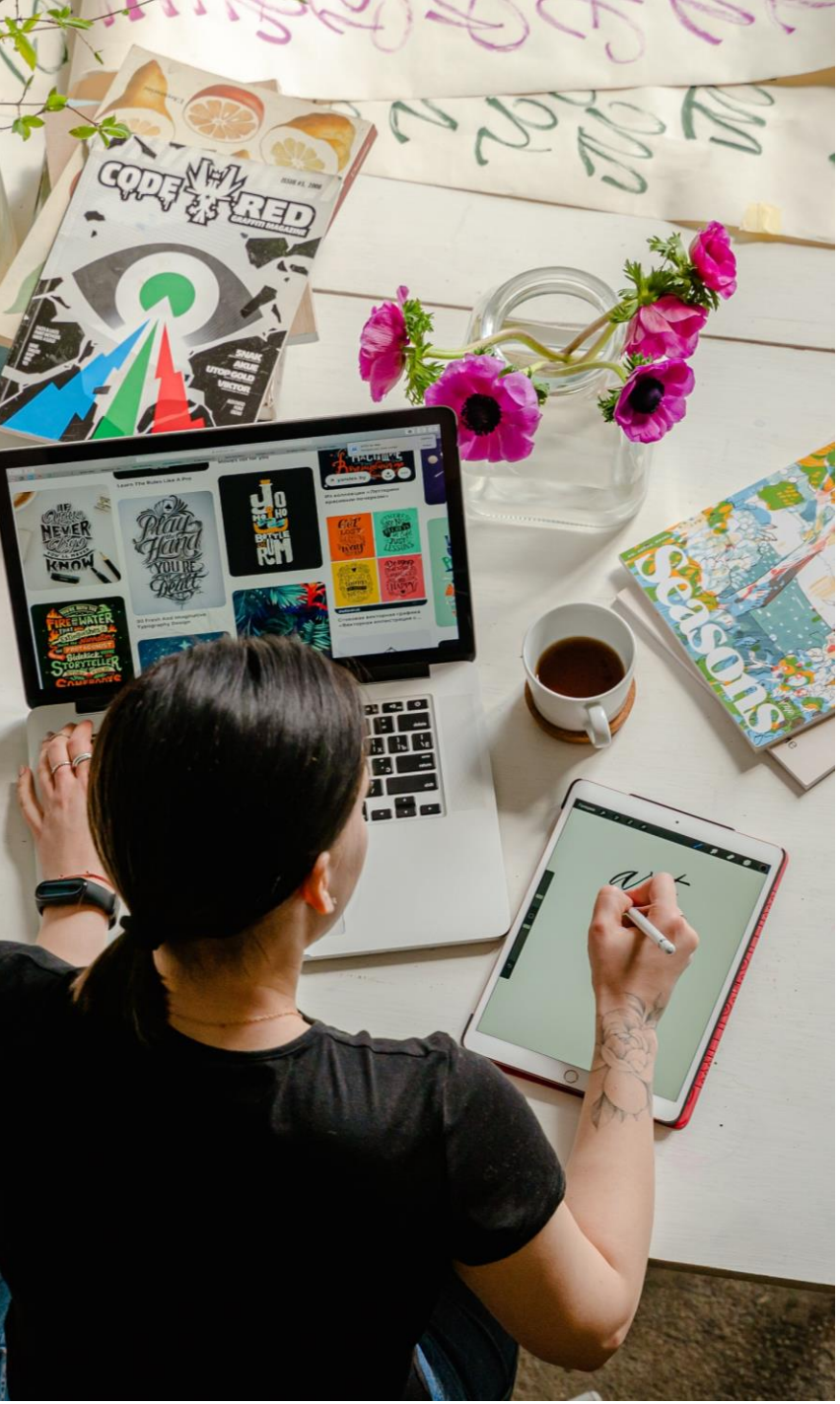
Nur Digitales zählt? Nein!

- Datenschutzrecht findet Anwendung, wenn
  - personenbezogene Daten betroffen sind,
  - die verarbeitet werden,
  - gleich, ob mittels IT oder auf Papier
- Ausnahme: ausschließlich persönliche/familiäre Tätigkeiten
  - Rein private Nutzung von Messengern
    - Tagebuch
  - Hochzeitsfotoalbum
- Praktische Konsequenz: DSGVO findet Anwendung auf alle Aufzeichnungen und Notizen im Rahmen der Gästeverwaltung oder HR, die Arbeitsbezug haben

Was sind „personenbezogene Daten“?

Alles, was eine Person identifizieren kann

- Name und Vorname
- Adresse
- Steuer-ID, Sozialversicherungsnummer, Ausweisnummer
- Mailadresse
- Standortdaten
- IP Adresse
- Cookie-IDs
- Werbe-IDs des Handys
- Ableitungen aus Daten
- Pseudonyme Daten („Gast 15”)



Wann verarbeite ich personenbezogene Daten?

Weiter Verarbeitungsbegriff

- Erheben
- Erfassen
- Organisieren
- Ordnen
- Speichern
- Verändern
- Auslesen
- Verwenden
- Löschen und Vernichten

Eine:r muss den Kopf hinhalten

Wer ist verantwortlich?

Rolle und Verantwortung

Wer muss den Kopf hinhalten?

- „Verantwortlicher“ ist jeder, der über die Zwecke und Mittel der Verarbeitung entscheidet
- Verantwortlicher = Zurechnungseinheit (Unternehmen, Behörde)
- Verantwortlicher hat alle (60+) Pflichten zu erfüllen und nachzuweisen
  - Volle Haftung
  - Schadensersatz, Art. 82
  - Unterlassung, Art. 79/nationales Recht
  - Bußgelder, Art. 83, 84
- Verantwortlich sein heißt immer volle Verantwortung zu tragen
- Man kann gemeinsam mit anderen verantwortlich sein

Wann ist eine Datenverarbeitung erlaubt?

Rechtsgrundlagen

Wann dürfen personenbezogene Daten verarbeitet werden?

Die Verarbeitung von Daten braucht eine Rechtsgrundlage

- Rechtsgrundlage kann sein
  - Ein **Vertrag** (Beherbergung) oder **Gesetz** (Bundesmeldegesetz), das die Verarbeitung erfordert,
  - **Lebenswichtige Interessen** einer Person,
  - **Rechtliche Verpflichtung** des Verantwortlichen,
  - Ein **überwiegendes berechtigtes Interesse** an der Datenverarbeitung,
  - Eine **Einwilligung**, wo es nicht anders geht

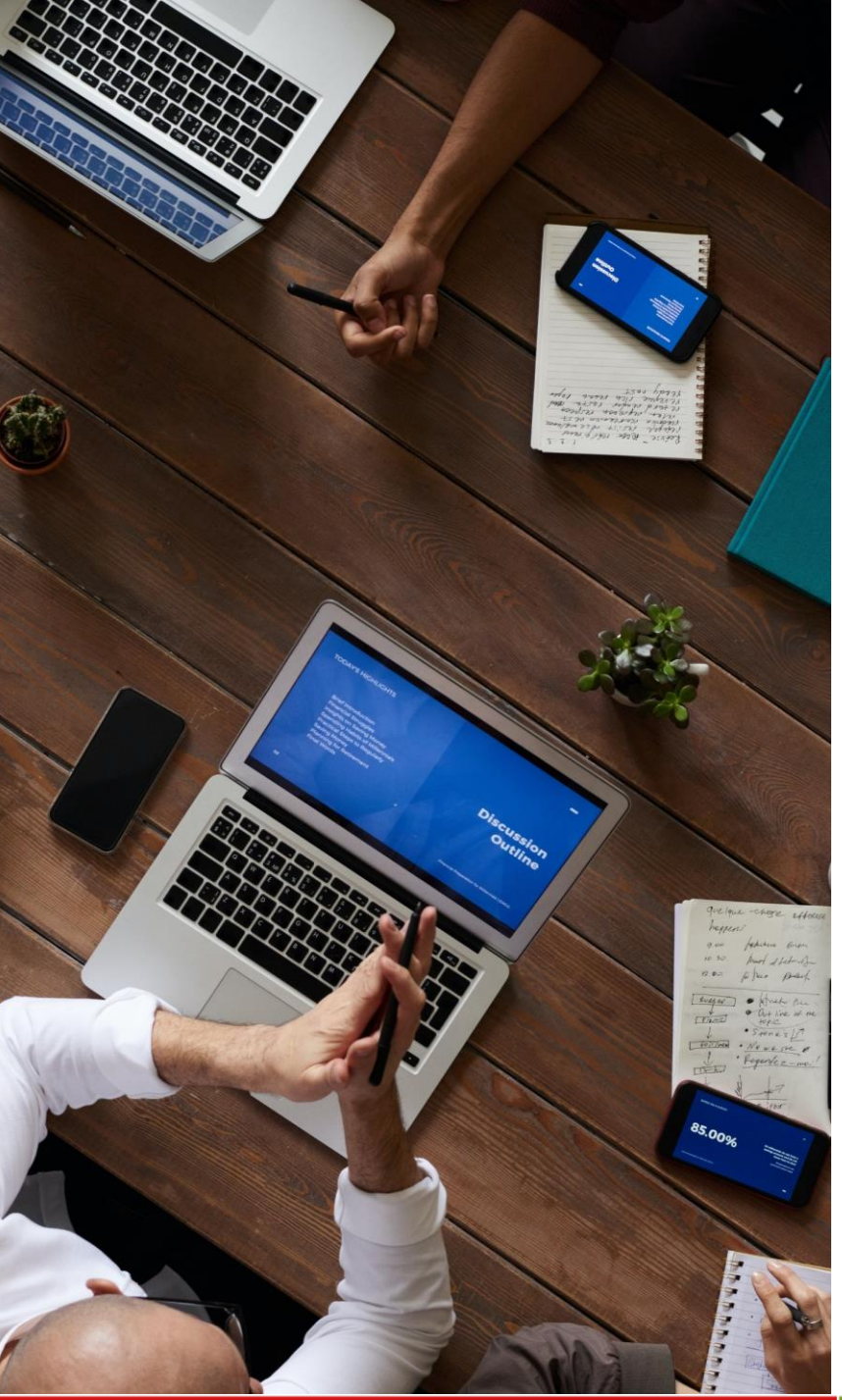
DSGVO

Die Pflichten

Pflichten

Richten sich nach nach der Rolle → Verantwortlicher

- Rechtsgrundlage
- Informationspflichten
- Verzeichnis von Verarbeitungstätigkeiten
- Technische und organisatorische Maßnahme
- Ggf. Datenschutzfolgeabschätzung
- Ggf. Benennung eines DSB
- Ggf. Meldungen bei Verstößen
- uvm.



Informationspflichten

- Identität und Kontaktdaten des Verantwortlichen/EU-Verteters/Datenschutzbeauftragten
- Art der Daten
- Zwecke der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- (Kategorien) von Empfängern
- Drittlandtransfer
- Speicherdauer
- Betroffenenrechte

Es geht weiter!

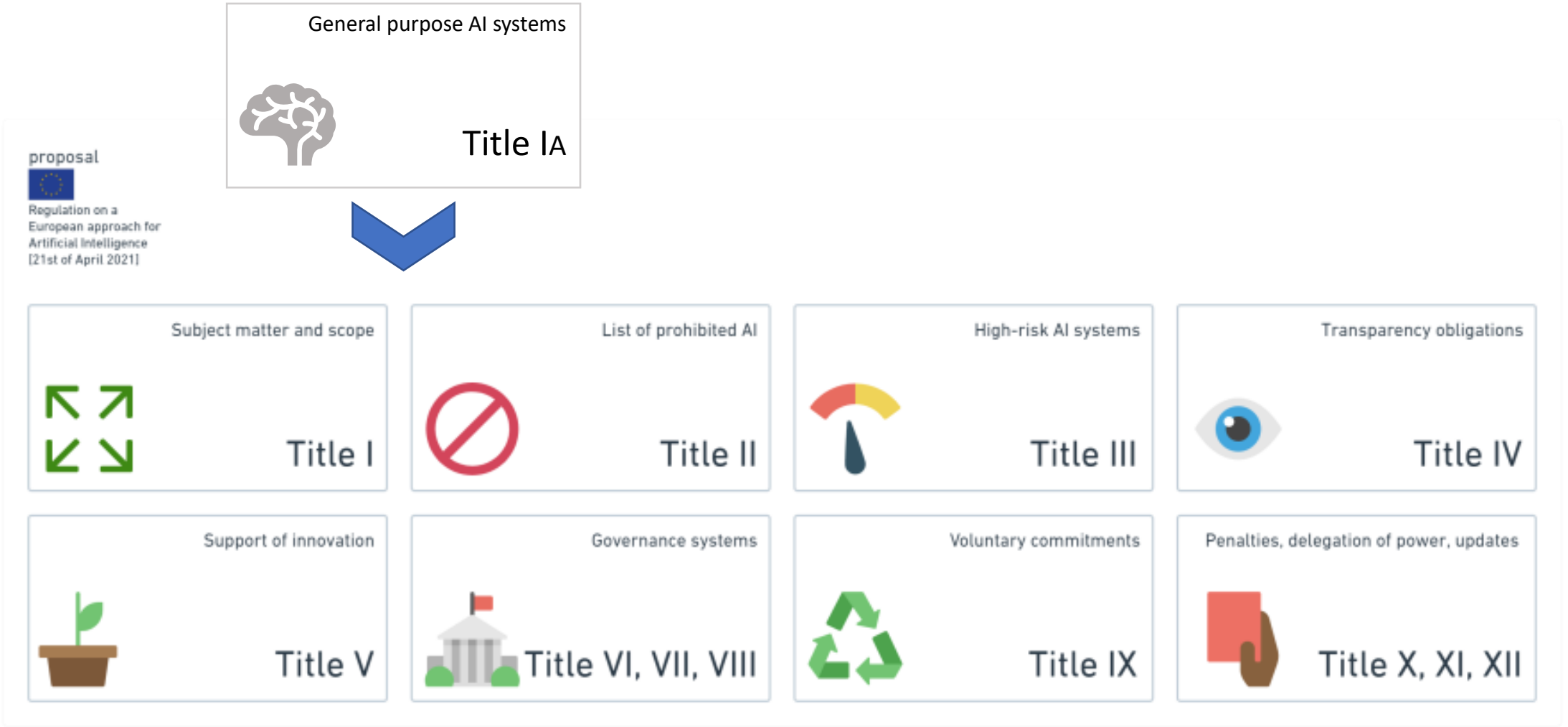
Die KI-VO – Ein Versuch der Regulierung

Wie viel Zeit bleibt uns noch?

KI-VO

Der Aufbau und Grundsätze

AI Act: Worum gehts eigentlich?

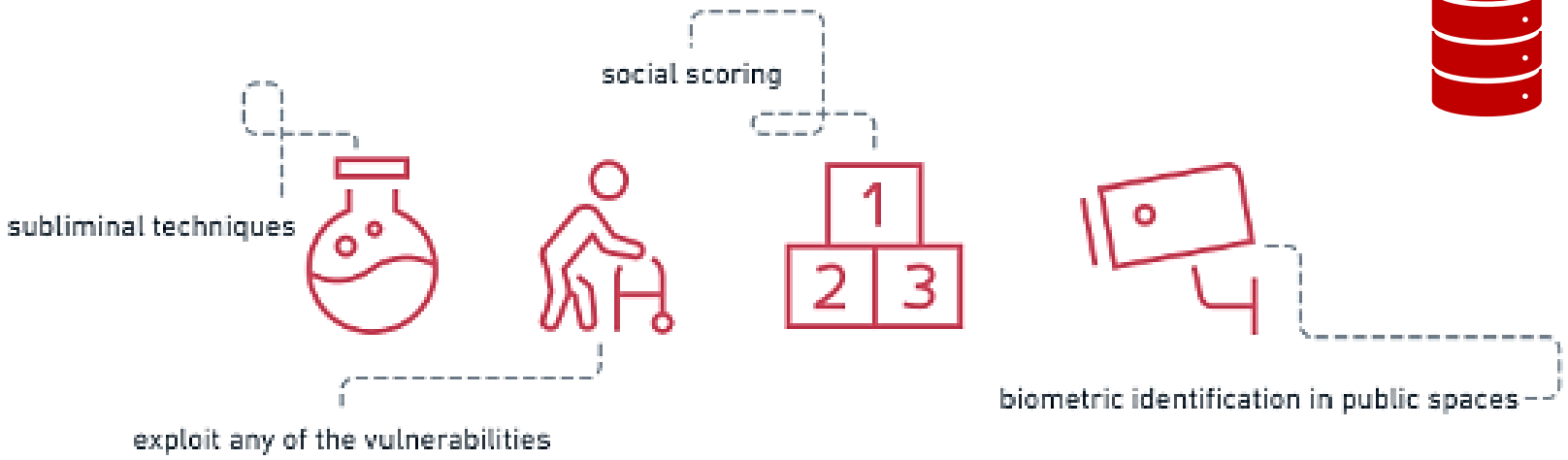


KI-System

(6) The notion of AI system ***in this Regulation*** should be clearly defined ***and closely aligned with the work of international organisations working on artificial intelligence*** to ensure legal certainty***, harmonization and wide acceptance***, while providing the flexibility to accommodate ***the rapid*** technological developments ***in this field***. ***Moreover, it*** should be based on key characteristics of artificial intelligence, ***such as its learning, reasoning or modelling capabilities, so as to distinguish it from simpler software systems or programming approaches. AI systems are designed to operate with varying levels of autonomy, meaning that they have at least some degree of indepe*** ***without h*** ***systems r*** ***that AI s*** ***implicit o*** ***purpose o*** ***content, v*** ***possible outputs produced by an AI system. For the purposes of this Regulation, environments should be understood as the contexts in which the AI systems operate, whereas outputs generated by the AI system, meaning predictions, recommendations or decisions, respond to the objectives of the system, on the basis of inputs from said environment. Such output further influences said environment, even by merely introducing new information to it.***

‘artificial intelligence system’ (AI system) means ***a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.***

Forbidden practices



biometric categorisation

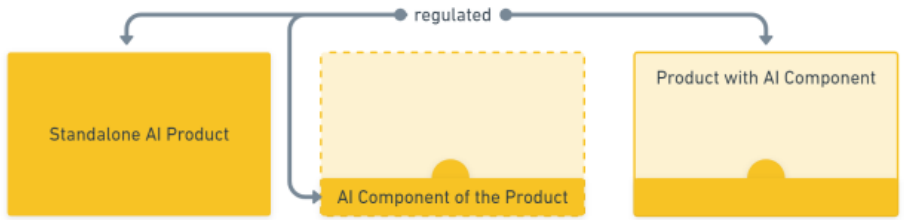
predictive policing

internet-scraped facial recognition databases

emotion recognition software

Geldbuße von bis zu 40 Mio. Euro oder 7% des gesamten weltweiten Jahresumsatzes

Was ist ein „hohes Risiko“?



ANNEX III

HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

+

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems ***falling under one or more of the critical areas and use cases*** referred to in Annex III shall be considered high-risk ***if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Where an AI system falls under Annex III point 2, it shall be considered high-risk if it poses a significant risk of harm to the environment.***

The Commission shall, 6 months prior to the entry into force of this Regulation, following consultation with the AI Office and relevant stakeholders, provide guidelines clearly specifying the circumstances where the output of AI systems referred to in Annex III would pose a significant risk of harm to the health, safety or fundamental rights of natural persons or cases in which it would not.

„Hohes Risiko“: Beispiele

unacceptable risks (Title II) → high risks (Title III) → minimal risks (Title IX)

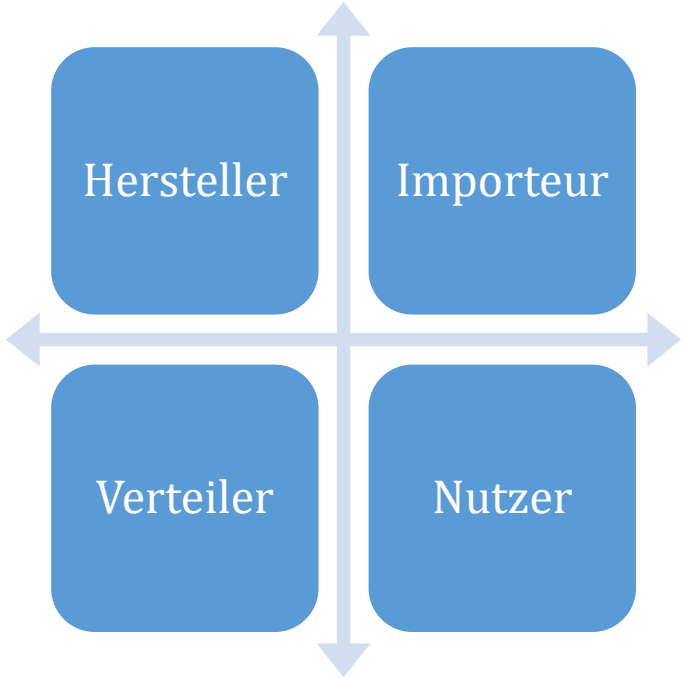
Remote Biometric Identification (RBI) von Personen (in Echtzeit oder im Nachgang)	Entscheidungen über den Zugang zu Bildungseinrichtungen oder Beurteilung von Studenten	Empfehlungssysteme von bekannten sozialen Medien	Rekrutierung, Entscheidungen über Arbeitsverträge und Überwachung der Arbeitsleistung
Bewertung der Kreditwürdigkeit von Personen	Bewertung der Anspruchsberechtigung für öffentliche Unterstützungsleistungen und -dienste	Individuelle Risikobewertungen zur Verwendung als Beweismittel in Strafverfolgungszusammenhängen	Vorhersage des Auftretens von Straftaten oder sozialen Unruhen
	Bearbeitung und Prüfung von Asyl- und Visumanträgen	Unterstützung von Richtern an Gerichten	

Eine:r muss auch hier den Kopf hinhalten

Rollenverteilung

Wer bin ich? Und wenn ja, wie viele?

- Entwickeln Sie ein KI-System?
- Erzeugt Ihr System selbständig Leistungen, die die Umwelt beeinflussen?
- Bringen Sie ein solches System unter Ihrer Marke auf den Markt?
- Bringen Sie ein solches System ohne Ihr Warenzeichen auf den Markt?
- Benutzen Sie ein solches System?

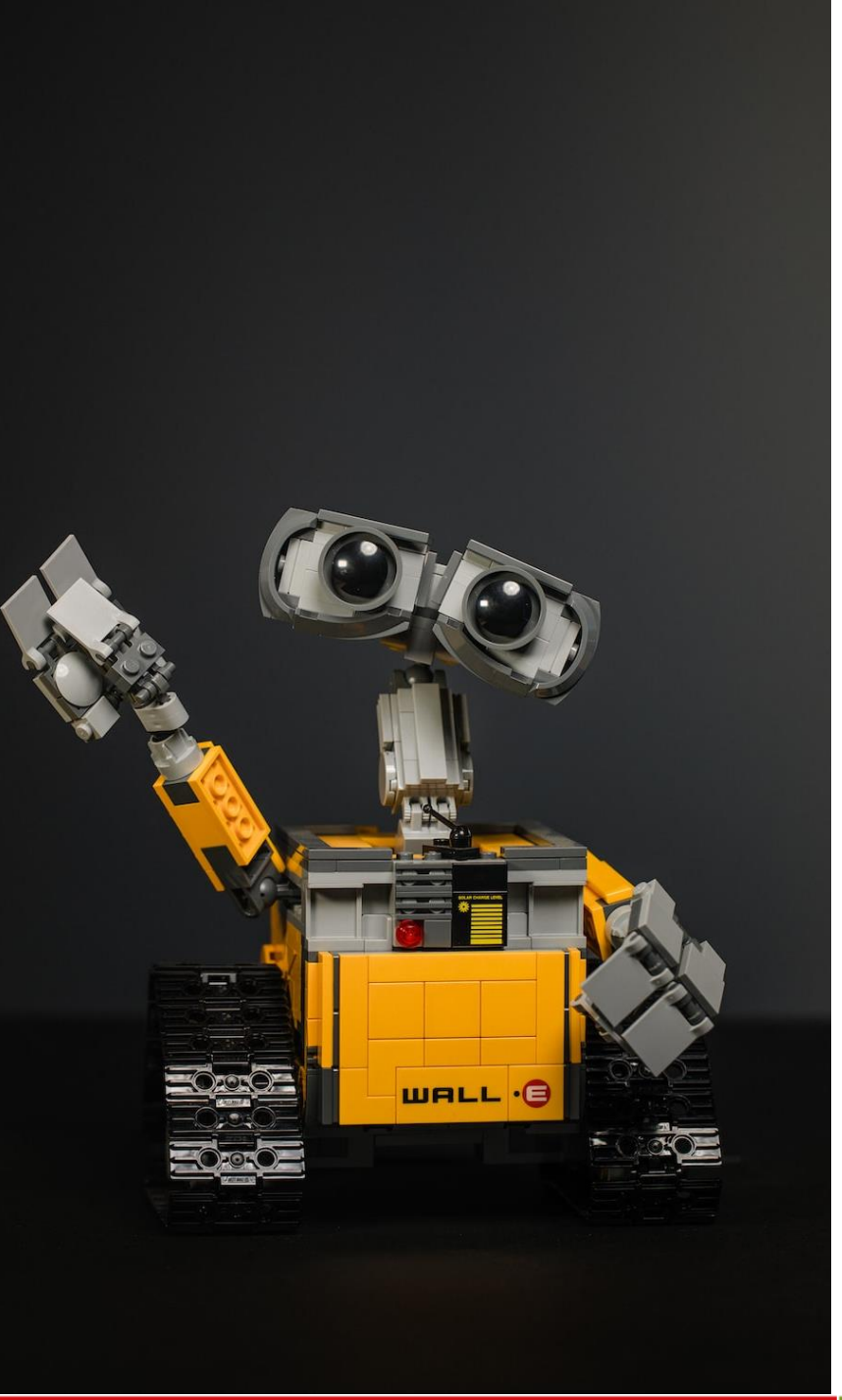


Was ist zu tun?

Die Pflichten

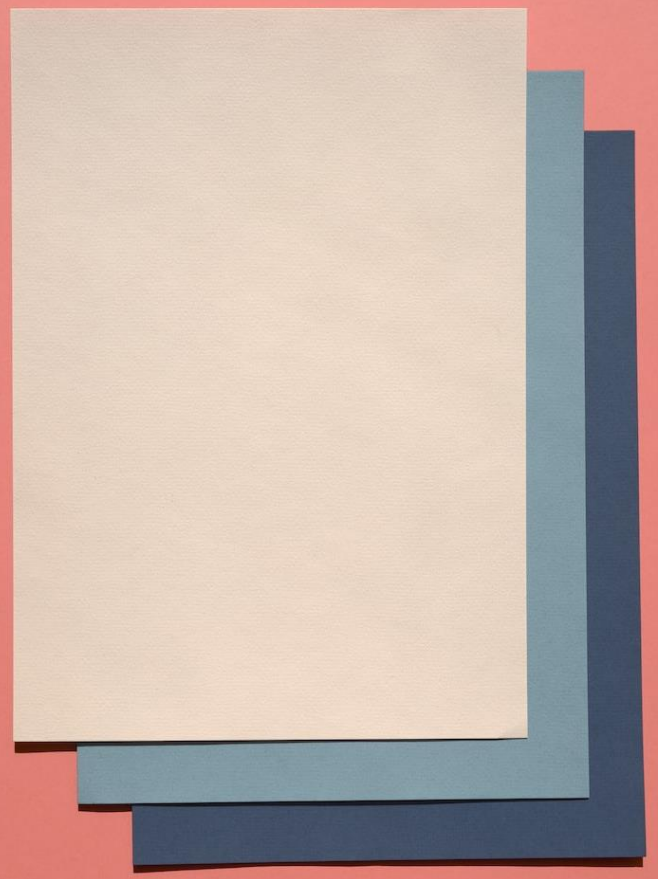
Hersteller

1. sicherstellen, dass die **Systeme den Anforderungen entsprechen**
2. Namen oder eingetragenes Warenzeichen sowie Anschrift angeben
3. eine **effiziente menschliche Aufsicht** gewährleisten
4. Spezifikationen für die **Eingabedaten** bereitstellen
5. über ein **Qualitätsmanagementsystem** verfügen
6. die **Dokumentation** zu erstellen und aufzubewahren
7. die automatisch erstellten **Protokolle** führen
8. eine **EU-Konformitätserklärung** zusammenstellen
9. die CE-Kennzeichnung anbringen
10. **Registrierung**
11. Korrekturmaßnahmen zu ergreifen, wenn das System nicht konform ist
12. auf begründete Aufforderung einer nationalen Aufsichtsbehörde die **Konformität nachzuweisen**
13. sicherstellen, dass das KI-System mit hohem Risiko die Anforderungen an die Zugänglichkeit erfüllt



Nutzer

1. die Systeme **gemäß den Anweisungen zu verwenden**
2. **menschliche Aufsicht** einführen und den Betrieb des Systems überwachen
3. Personen mit der Aufsicht betrauen, die über die erforderliche Kompetenz, Ausbildung und Autorität verfügen
4. sicherstellen, dass die **Robustheits- und Cybersicherheitsmaßnahmen** regelmäßig überwacht, angepasst und aktualisiert werden
5. sicherstellen, dass die **eingegebenen Daten für den vorgesehenen Zweck relevant sind**
6. den **Anbieter oder Händler zu informieren und die Nutzung aussetzen**, wenn sie zu einem Risiko führen könnte
7. **Meldung schwerwiegender Vorfälle** an den Anbieter und die nationalen Behörden
8. die automatisch erstellten Protokolle aufzubewahren
9. die **Arbeitnehmervertreter zu konsultieren**, bevor ein System eingeführt wird, das die Arbeitnehmer betrifft
10. die **natürlichen Personen darüber zu informieren**, dass sie dem Einsatz des KI-Systems mit hohem Risiko ausgesetzt sind
11. verwenden die bereitgestellten Informationen, um ihrer Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung nachzukommen
12. arbeiten mit den zuständigen nationalen Behörden zusammen



Hersteller von Basismodellen

1. die **Verringerung von vernünftigerweise vorhersehbaren Risiken** für Gesundheit, Sicherheit, Grundrechte, Umwelt sowie Demokratie und Rechtsstaatlichkeit nachweisen
2. nur Datensätze zu verarbeiten und einzubeziehen, die **geeigneten Maßnahmen zur Datenverwaltung** unterliegen
3. Entwicklung des Basismodells, das ein angemessenes Niveau an Leistung, Vorhersagbarkeit, Interpretierbarkeit, Korrigierbarkeit, Sicherheit und Cybersicherheit erreicht
4. Entwicklung des Basismodells, das in der Lage ist, den **Energieverbrauch, den Ressourcenverbrauch und die Abfälle zu verringern** und die Energieeffizienz zu erhöhen
5. Erstellung von technischen Unterlagen und verständlichen Anleitungen
6. **Qualitätsmanagementsystem** einrichten
7. **Registrierung**
8. die **technische Dokumentation 10 Jahre lang aufbewahren**

Hersteller von generativen KI-Modellen

Alle Pflichten wie für Hersteller von Basis-Modellen +

1. Einhaltung der **Transparenzpflichten**
2. das Stiftungsmodell so auszubilden, zu gestalten und weiterzuentwickeln, dass **angemessene Schutzvorkehrungen gegen die Erstellung von Inhalten** getroffen werden, **die gegen das Unionsrecht verstoßen**
3. unbeschadet der nationalen oder EU-Rechtsvorschriften zum Urheberrecht eine **Zusammenfassung der Verwendung von urheberrechtlich geschützten Ausbildungsdaten** zu dokumentieren und öffentlich zugänglich zu machen

Fast geschafft!

Wir schauen uns die Theorie anhand zweier Praxisbeispiele an!

Das Beispiel

KI im Recruitment-Prozess

KI-System wird mit allen Daten der bereits beschäftigten Personen „gefüttert“

Dem KI-System werden außerdem alle formalen Kriterien für die Stellenbeschreibung zugewiesen (Berufserfahrung, Abschluss, etc.)

Eingehende Bewerbungen werden von dem System geprüft, anhand:

formaler Kriterien, die auf die Job-Beschreibung passen	bereits beschäftigter Arbeitnehmenden, um Passgenauigkeit zu eruieren

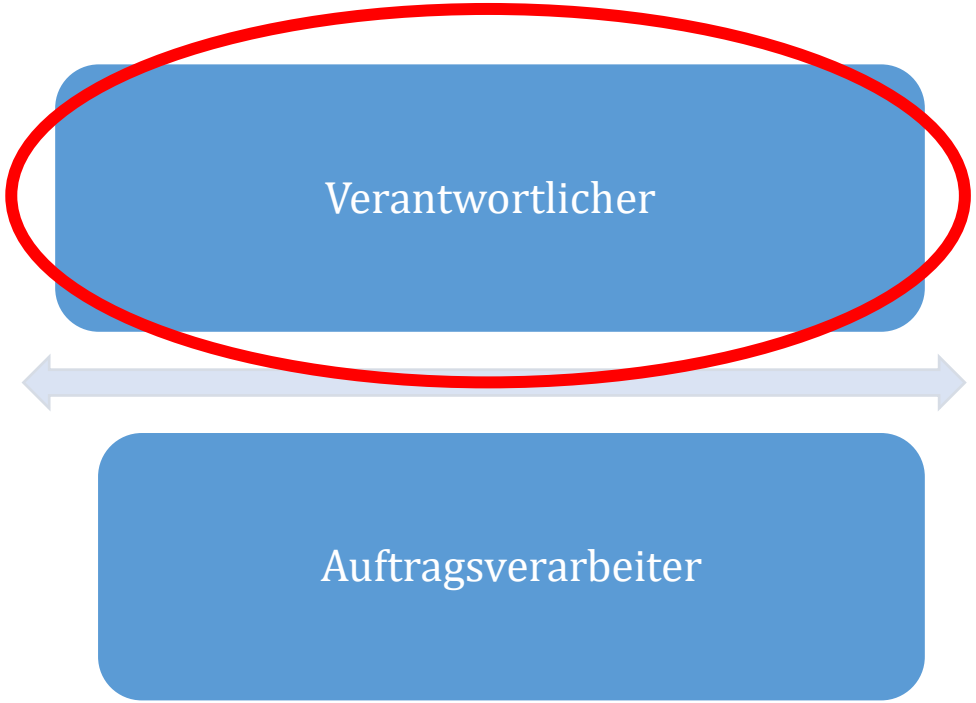
Das Problem

Bias & Diskriminierung

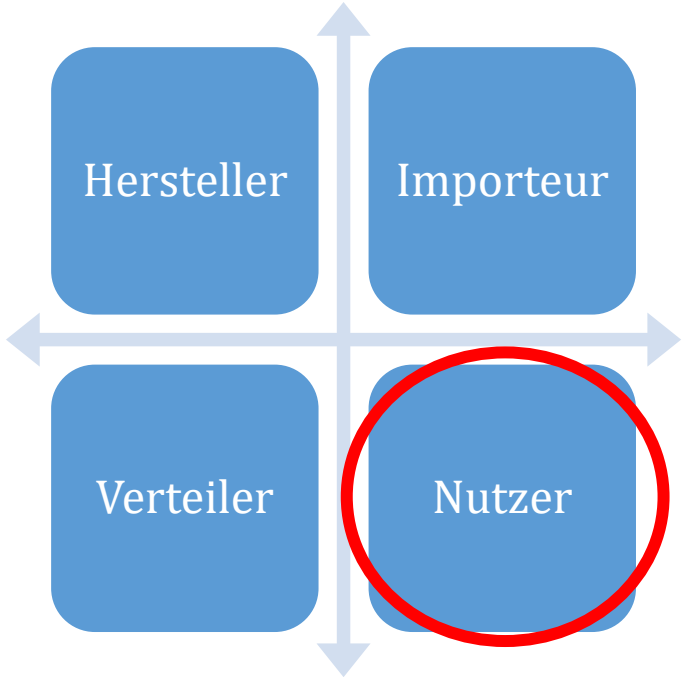
- Gesucht wird: Geschäftsführung
- Alle im Unternehmen tätigen Geschäftsführer sind weiß, männlich und zwischen 40 und 60 Jahre alt
- KI-System filtert anhand dieser Kriterien die Bewerbungsunterlagen
- Es werden weiße, männliche Bewerber zwischen 40 und 60 vorgeschlagen

Die Rollen

DSGVO:



KI-VO:



Das Risiko | KI- VO

RBI von Personen (in Echtzeit oder im Nachgang)

Entscheidungen über den Zugang zu Bildungseinrichtungen oder Beurteilung von Studenten

Empfehlungssysteme von bekannten sozialen Medien

Rekrutierung, Entscheidungen über Arbeitsverträge und Überwachung der Arbeitsleistung

Bewertung der Kreditwürdigkeit von Personen

Bewertung der Anspruchsberechtigung für öffentliche Unterstützungsleistungen und -dienste

Individuelle Risikobewertungen zur Verwendung als Beweismittel in Strafverfolgungszusammenhängen

Vorhersage des Auftretens von Straftaten oder sozialen Unruhen

Bearbeitung und Prüfung von Asyl- und Visumanträgen

Unterstützung von Richtern an Gerichten

Die Pflichten nach KI-VO & DSGVO

Rechtsgrundlage	Zweckbestimmung	Informationspflichten & Transparenz	Nutzung von geeigneten Daten	Verzeichnis von Verarbeitungstätigkeiten
Verwendung gemäß der Anleitung	Technische und organisatorische Maßnahmen / Cybersecurity	Human-in-the-loop & Überwachung	Protokollierung	DPIA & FRIA
Meldepflichten	Zusammenarbeit mit nationalen Behörden	Qualitäts- & Risikomanagement	Beteiligung des Betriebsrats	Registrierung und Zertifizierung

FYI

Nutzung von Basismodellen durch APIs

- „downstream providers“
- Hohes Risiko
- Pflichten für Hersteller anwendbar

Kontakt

Bettina Blawert

Rechtsanwältin
Certified Information Privacy Professional

E-Mail: bettina.blawert@spiritlegal.com

Tea Mustać

Mag. iur. (Rechtswissenschaften)
Certified Information Privacy Professional

E-Mail: tea.mustac@spiritlegal.com

www.spiritlegal.com