Webinar: EU AI Act für Kostenträger

DACH, 25. Oktober 2023


„We are at the iPhone moment of AI“
Jen-Hsun Huang, CEO of NVIDIA

Die CEOs von OpenAI und Alphabet bitten Regierungen und Behörden, die Kräfte von AI zu regulieren, die ihre Konzerne entfesselt haben.

„We can have a dramatically more prosperous future; but we have to manage risk to get there."
Sam Altman, CEO of OpenAI

Key Trust Factor: Fairness

Key Trust Factor: Robustness - Gefahren durch Adversarial Attacks

Original Bild

Next image

Prediction

Run Neural Network

Prediction: „Stop sign“

Probability: 99,85 %

Prediction is correct

Adversarial Bild

Turn this image into a:

120 km/hr

Select an attack:

Carlini & Wagner (Stronge

Prediction

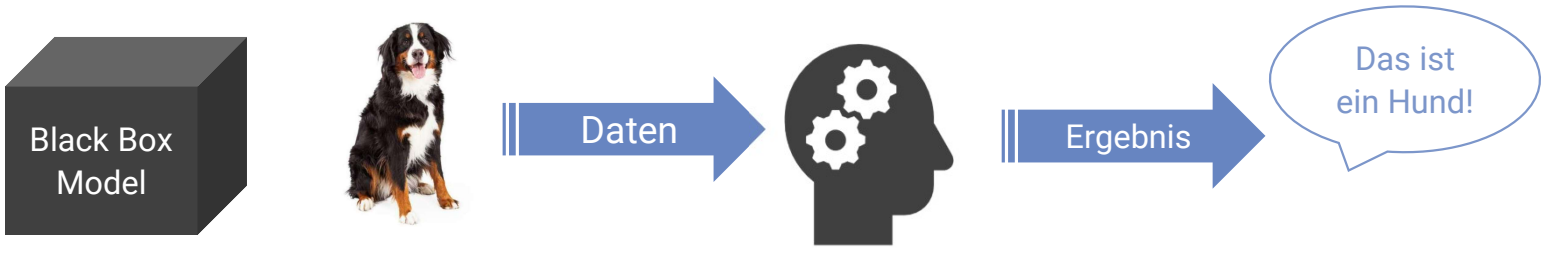
Run Neural Network

Prediction: „120 km/hr“

Probability: 99,91 %

Prediction is wrong! Attack succeeded!

Key Trust Factor: Explainability



ChatGPT befeuert die Diskussion um Regeln für AI

USA

AI Risk Management Framework (2022 Draft)

Senator-only AI briefings seit June 2023

Kalifornien

- CCCP
- Draft zu AI und automatisierten Systemen in Recruiting-Prozessen (2022)

EU

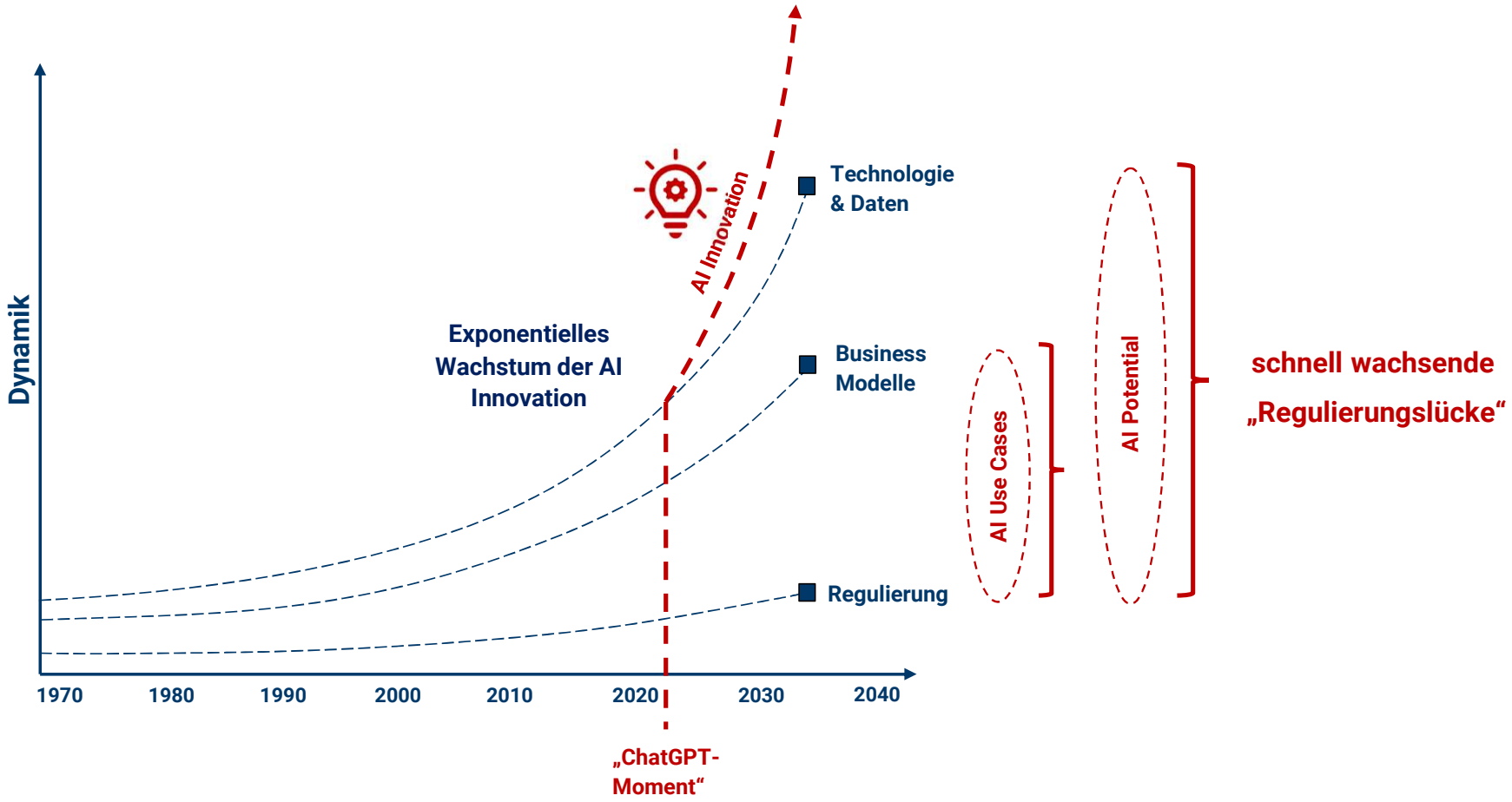
- DSGVO (2018) - einige Klauseln mit Impact auf AI
- EU AI Act (Draft 2021, EU Parlament Juni 2023) – ein risiko-basierter Ansatz für den Einsatz von AI
- EU Digital Services Act (2021 Draft) – auch Regelungen für AI

China

Internet Information Service Algorithmic Recommendation Management Provisions (2022) – Umfassende Regeln für die Regulierung von Algorythmen

NTT DATA

AI im Spannungsfeld von Innovation und Regulierung



NTT DATA

Daten und AI Regulierung in der EU

Die aktuellen EU-Regulierungen im Bereich Daten und AI fokussieren auf Zugang und Verfügbarkeit, sowie Transparenz und Vertrauen.

EU Data Act (EHDS / GDNG)

- Anwendbar für Hersteller von Smart Devices (IoT) und Cloud Provider
- IoT Produkte müssen eine Schnittstelle bieten, um auf die gesammelten und geneierten Daten zuzugreifen

EU AI Act

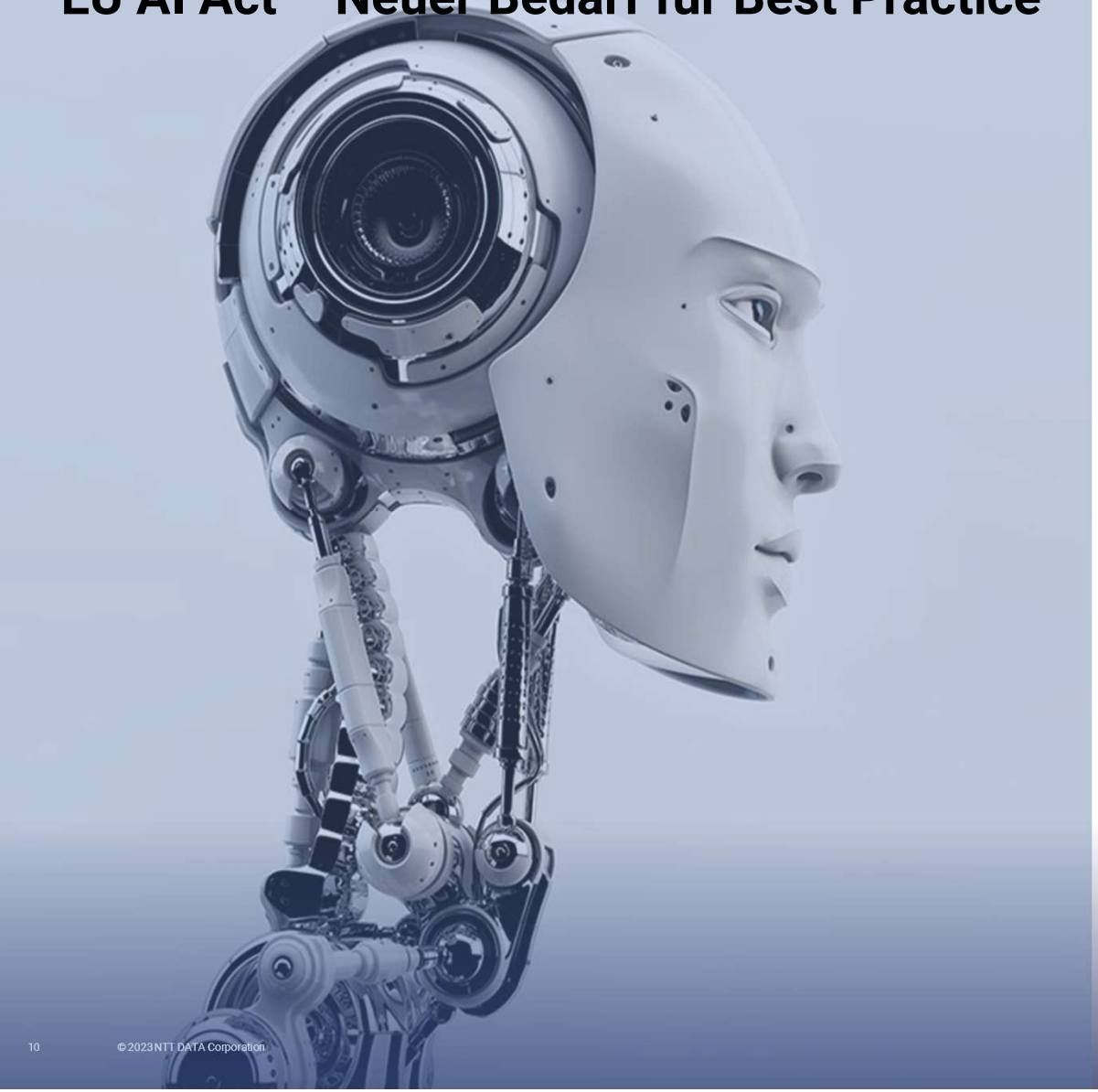
- Fokus auf Vertrauen in AI-Systeme und Exzellenz
- Risiko-basierter Ansatz für den Umgang mit AI
- Verbot bestimmter AI Systeme
- Obligatorische Conformity Assessments for hoch-risiko Applikationen

EU Data Governance Act

- Ein Framework für den Austausch von Daten in der EU
- Regeln für die Wiederverwendung von öffentlichen Daten und Data Brokering

NTT DATA

EU AI Act – Neuer Bedarf für Best Practice



AI Risiken

Ein umfassendes Risikomanagement für AI-Applikationen ermöglicht sichere und vertrauensvolle AI.

Strafzahlungen

Massive Strafzahlungen i.H.v. 4%-6% des globalen Umsatzes oder 30 Mio EUR drohen bei Nicht-Einhaltung.

Neue Lösungen

AI Risiko Assessments, AI Governance und MLOps, um AI-Risiken zu identifizieren, zu managen und zu mitigieren, um Strafzahlungen und Reputationsschäden zu vermeiden.

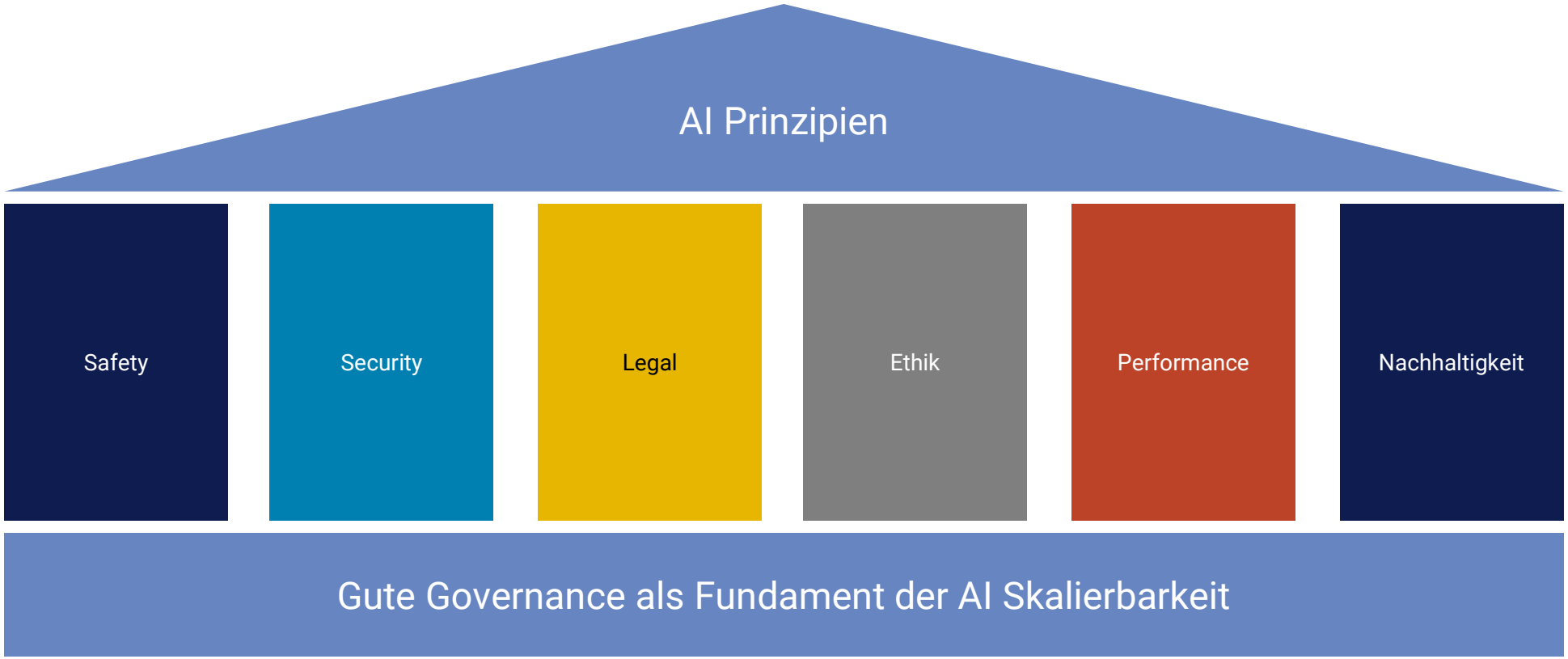
EU AI Act

Wichtige Definitionen: AI-Risikoklassifikation

Der Risikobegriff steht im Zusammenhang mit Gesundheit, Sicherheit und den Grundrechten einer Person.

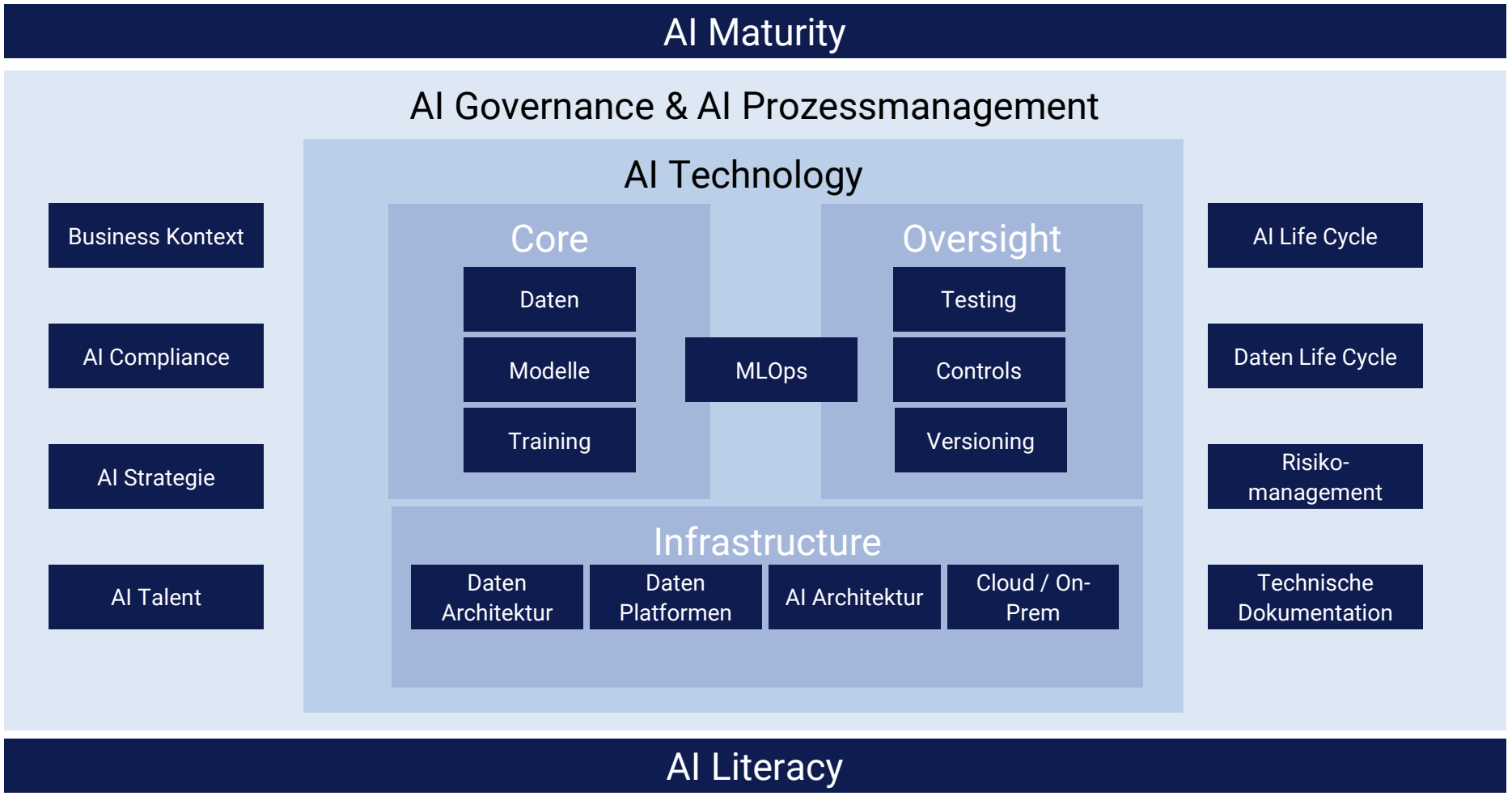
Risiko Klassifikation	Risiko Level Beschreibung	Anforderungen & Risikomitigierung
INAKZEPTABLES RISIKO	Anwendung von AI, die gegen die Werte der EU verstößt und die Grundrechte, die Gesundheit oder die Sicherheit verletzt. Beispiel: Social Scoring	Strafzahlungen von bis zu 30 Mio. EUR. Die Anwendungen müssen abgeschaltet werden.
HOHES RISIKO	Eine begrenzte Anzahl von AI-Systemen, die sich nachteilig auf die Sicherheit der Menschen oder ihre Grundrechte auswirken. Beispiel: Kredit Scoring	Obligatorische Anforderungen für alle AI-Systeme mit hohem Risiko und Sanktionen bei Nichteinhaltung werden festgelegt.
BEGRENZTES RISIKO	AI-Systeme, die: 1. mit Menschen interagieren 2. Inhalte generieren oder manipulieren. Beispiel: Chat / Voice Bots, Deepfakes	Transparenzverpflichtungen sind erforderlich (d. h. Disclaimer ähnlich der DSGVO).
MINIMALES RISIKO	Die große Mehrheit der AI-Systeme fällt in diese Kategorie, in der die neuen Regeln nicht eingreifen. Beispiel: Spam-Filter	Ein freiwilliger Code of Conduct wird empfohlen.

AI Governance zur Einhaltung von AI Prinzipien



NTT DATA

AI Qualitätsframework



Exemplarische Roadmap

DIENSTAG, 24. OKT 2023

NTT DATA und TÜV SÜD arbeiten für mehr Qualität bei KI-Anwendungen zusammen

Sicherheit von KI-Systemen als Wirtschafts-Booster

München, 24. Oktober 2023 – NTT DATA setzt zukünftig den KI-Qualitätsrahmen von TÜV SÜD ein, um für mehr Vertrauen in Anwendungen mit Künstlicher Intelligenz (KI) zu sorgen und deren Qualität zu sichern. Die Kooperationsvereinbarung umfasst die Nutzung des TÜV SÜD KI Qualitätsrahmens und entsprechender Analysewerkzeuge, damit Kunden von NTT DATA KI-Anwendungen marktorientiert und mit hohen Qualitätsanforderungen entwickeln können.

Presseanfragen für Deutschland, Österreich, Schweiz

https://de.nttdata.com/newsroom/2023/ntt-data-und-tuev-sued-arbeiten-fuer-mehr-qualitaet-bei--ki-anwendungen-zusammen

NTT DATA

Trusted Global Innovator