

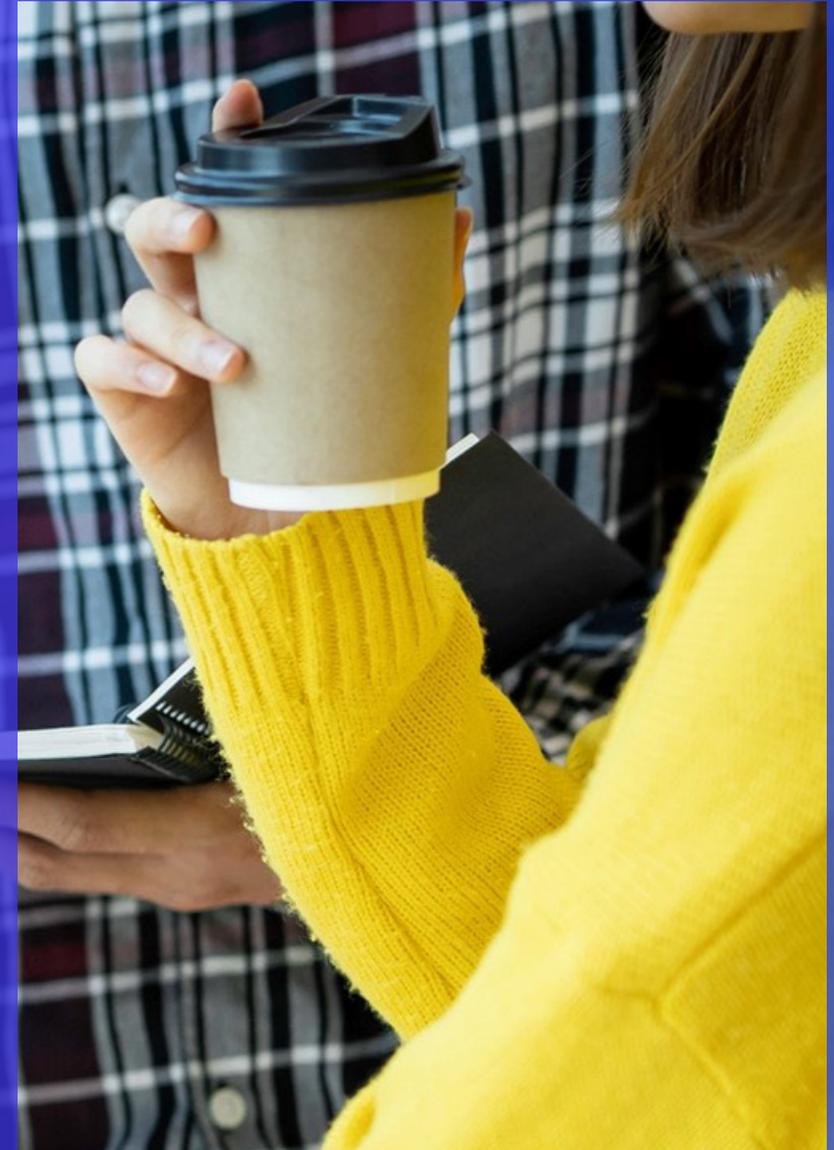


Breakfast Update Handelsrisiko: Zukunftsthemen in 30 Minuten

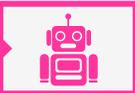
Machine Learning im Risikomanagement – Aktuelle Entwicklungen

Webcast

—
24. Mai 2023



Agenda der Webcast-Reihe

	10.05.	Kapitalmarkt im Umbruch – Effekte im Überblick
	17.05.	ESG im Marktpreisrisiko – Erste Erfahrungen und Lösungsansätze
Heute 	24.05.	Machine Learning im Risikomanagement – Aktuelle Entwicklungen
	31.05.	Überblick CSRBB und die Auswirkungen auf die Steuerung der Handelsrisikopositionen
	07.06.	Counterparty Credit Risk und Initial Margin – Zurück im Fokus?
	14.06.	Model Risk Management – Banken unterschätzen die Risiken einer unzureichenden Modell-Governance
	21.06.	Erfahrungen aus dem Energy Trading – Was können Banken aus den Turbulenzen im Energiesektor lernen?

Ihre heutigen Referenten



Dr. Christoph Anders
Manager

Themenschwerpunkte:

- Machine Learning im Risikomanagement
- Marktpreisrisiko, Zinsrisiko
- Datenanalyse und Machine Learning



Dr. Daniel Wehl
Assistant Manager

Themenschwerpunkte:

- Daten Analyse und Prototyping
- Machine Learning im Risikomanagement
- Testmanagement

Q&A Support



Dr. Philipp Prasse
Assistant Manager

Themenschwerpunkte:

- Marktpreis- & Kontrahentenrisikomessung
- Machine Learning im Risikomanagement

Unsere Themen für heute

- 01 News zum EU AI Act**
- 02 Auswirkung auf Modell-Landschaft**
- 03 Herausforderung durch Erklärbarkeit & Fairness Anforderungen an Modelle**

Machine Learning bringt viele Use Case in Banken mit sich, bisher fehlt jedoch noch die regulatorische Sicherheit



“We are on the verge of putting in place *landmark legislation* that must resist the challenge of time. It is crucial to build citizens’ trust in the development of AI, to set the European way for dealing with the extraordinary changes that are already happening, as well as to *steer the political debate on AI at the global level*. We are confident our text balances the *protection of fundamental rights* with the need to provide *legal certainty to businesses* and stimulate innovation in Europe”

Brando Benefei – Mitglied des Europäischen Parlaments
Nach der Abstimmung über Änderungen am EU AI Act am 11.05.23 im
Binnenmarktausschusses und dem Ausschusses für bürgerliche Freiheiten

Das EU Parlament reagiert damit auf die Sorgen der Bevölkerung und aktuelle technische Entwicklung

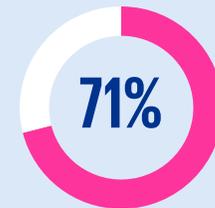
Das Stimmungsbild in der Gesellschaft...



Drei aus vier Teilnehmern (75 %) geben an bereit zu sein einem KI System zu vertrauen, wenn Sicherheitsmechanismen die ethischen und verantwortlichen Gebrauch sicherstellen bestehen.



Nur zwei aus fünf Teilnehmern halten die derzeitigen Sicherheitsmaßnahmen rund um KI (Regeln, Regulierungen und Gesetze) für ausreichend.



Die große Mehrheit der Teilnehmer (71 %) hält, KI Regulierung für nötig

Quelle: KPMG Studie - Trust in Artificial Intelligence: A global study (2023) [LINK](#)

... spiegelt sich in den Plänen des EU Parlaments wider



European Parliament
@EuroparL_EN

Artificial Intelligence: new transparency and risk-management rules for AI systems have been endorsed by Parliament's internal market and civil liberties committees.

All MEPs are expected to vote on the mandate in June so that negotiations can start with the Council.

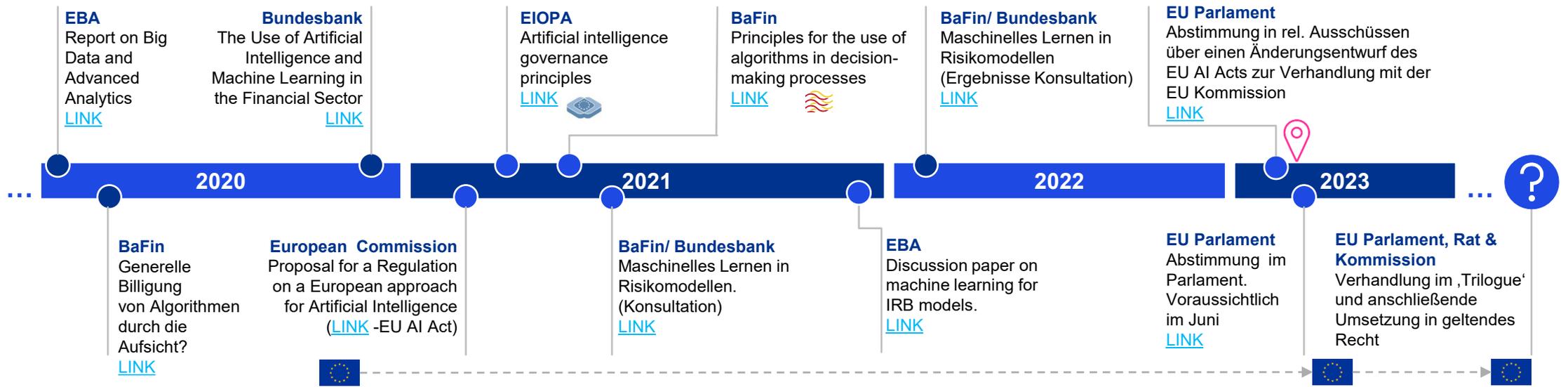
ARTIFICIAL INTELLIGENCE

- Once approved, new EU rules will be the world's first rules on Artificial Intelligence
- MEPs include bans on biometric surveillance, emotion recognition, predictive policing AI systems
- Tailor-made regimes for general-purpose AI and foundation models like GPT
- The right to make complaints about AI systems



Quelle: Offizieller Twitter Account des Europäischen Parlaments, 11.05.23

Regulator & KI /ML – Der Weg zur Gesetzgebung ist lang, die EU ist nach wie vor führend



Einordnung der Veröffentlichungen	Regulation/legislation			Principles		Diskussionspapiere	
	<ul style="list-style-type: none"> • Auswirkungen der Veröffentlichungen unterschiedlich • Regulatorische Vorgaben nur durch EU AI Act 	Europäische Union 	European Commission (EU AI Act)	EIOPA	EBA EIOPA	BaFin Bundesbank	
	Deutschland		BaFin				

Der Entwurf des EU AI Act bisher: Durch breite Definition von KI & Machine Learning sind Banken bereits betroffen

Entwurf des EU AI Act



“the proposal focuses on ‘high-risk’ AI use cases”

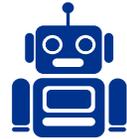
“high-risk AI systems need to respect a set of **specifically designed requirements**”

„must be **assessed for conformity** with these requirements before being placed on the market“



Ziel des EU AI Acts: Schutz von privat Personen / Gesellschaft vor Risiken, die aus der Nutzung von künstlicher Intelligenz hervorgeht

- Untergliederung der Methoden in **vier Risikoklassen**. Fokussierung auf **High-Risk Ansätze**
- Hohe Anforderung an High-Risk Ansätzen bzgl. Governance, Validierung und Conformity Assessment.



Breite Definition von künstlicher Intelligenz

- Ansätze die bereits in der Nutzung von Banken sind werden als KI klassifiziert
- Bsp: logistische Regression die im Scoring verwendet werden gelten als Machine Learning



Bankanwendung als High-Risk Klassifiziert

- Verschiedene Bereiche werden grundsätzlich als High Risk klassifiziert
- Bsp: „*Access to and enjoyment of essential private services and public services.*“
- Kreditscoring explizit genannt



Neue Anforderungen an High-Risk Ansätze

- Risk Management System, Data Governance,
- *Transparency and provision of information to users, Human oversight*
- Quality Management System für Compliance

Im EU Parlament diskutierte Änderungen und mögliche Auswirkungen auf Banken



Verbotene Ansätze werden erweitert, z.B. um

- ‚Predictive Policing‘
- Willkürliches Auslesen biometrischer Daten aus social media oder Überwachungskameras zum Training von Gesichtserkennung



Ansätze mit hohem Risiko werden erweitert, z.B. um

- Schaden an Gesundheit, Sicherheit, der Grundrechte oder der Umwelt
- Systeme zur Wählerbeeinflussung und ‚Recommender‘ in social media



Generative KI – Transparenz Maßnahmen

- Schutz von Grundrechten, Gesundheit, Sicherheit, Umwelt, Demokratie & Rechtsstaat
- Risikoassessment und –mitigation
- Zusätzliche Transparenz, z.B. Offenlegung KI Urheberschaft und der verwendeten Trainingsdaten, Sicherstellen, dass keine illegalen Inhalte erzeugt werden



Innovationsförderung und Schutz der Bürgerrechte

- Ausnahmen von den Regelung sind z.B. für die Forschung möglich
- Einrichtung regulatorischer Sandboxes / kontrollierter Umgebungen in denen Anwendungen vor ihrem Einsatz geprüft werden können
- Ermöglichen von Beschwerden über und zur Verfügungstellung von Erklärungen zu hoch Risiko Anwendungen

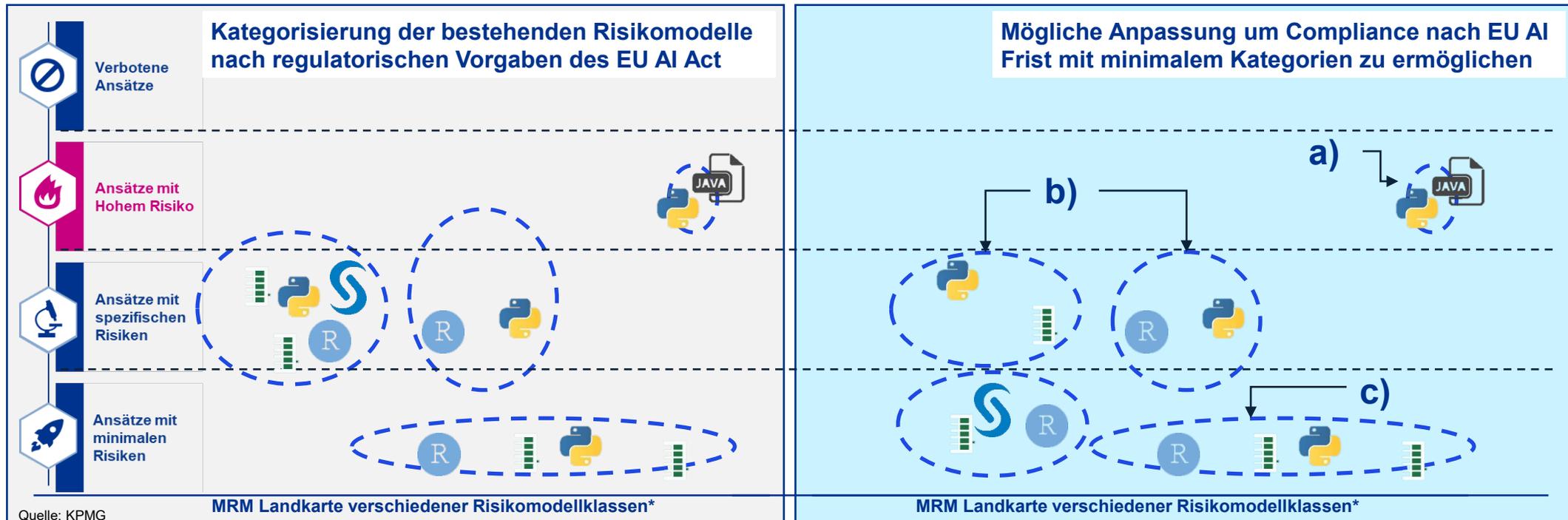
Erwartete zusätzlich Auswirkungen auf Banken, insb. im Marktrisiko / MRM gering

- Breite Definition für ML bleibt, umfasst also grundsätzlich weiterhin bestehende stat. Modelle
- Kreditscoring bleibt hoch Risiko
- Größte Änderung: Regulierung von generativer KI

Vorbereitung auf bestehenden Entwurf des AI Acts erscheint sinnvoll

Konkretisierung der bevorstehenden Regulierung des EU AI Acts – direkte Auswirkung auf MRM Modelle (live oder geplant)

– Durch die geplante Verschärfung der Regulatorik erwarten wir, dass sich die Modell Landschaft signifikant verändern wird



– Für bestehende Modelle sollte geprüft werden, ob der Umbau für die regulatorische Anforderung verhältnismäßig ist:

- Implementierung regulatorischer Anforderungen
- Modifikation des Modells um geringere Risikokategorie zu erzielen
- Keine regulatorischen Anforderungen erforderlich

* Zufällig Annahme bezüglich der Risikoklassen und verwendeten Modellen

ML und stat. Modelle können bereits jetzt mit der Erwartung der EU verglichen und ggfs. erweitert werden

„Trustworthy AI“ ist Grundlage der Regulierung von KI und ML der EU

1 Vorrang menschlichen Handelns und Aufsicht

2 Technische Robustheit und Sicherheit

3 Privatsphäre und Data Governance



4 Transparenz

5 Vielfalt, Nichtdiskriminierung und Fairness

6 Gesellschaftliches und ökologisches Wohlergehen

7 Rechenschaftspflicht

(¹) Ethics guidelines for trustworthy AI (April 2019) [LINK](#)

NIST & ISO Standardisierung

- NIST und ISO haben Standards zum Risiko Management für KI / ML Modelle entwickelt
- Orientierung / Parallelen zu Trustworthy AI erkennbar
- Gesetzgeber könnten sich an diesen Standards orientieren oder sie ggfs. sogar aufgreifen

Erweiterung bestehender Governance, z.B. MRM Framework

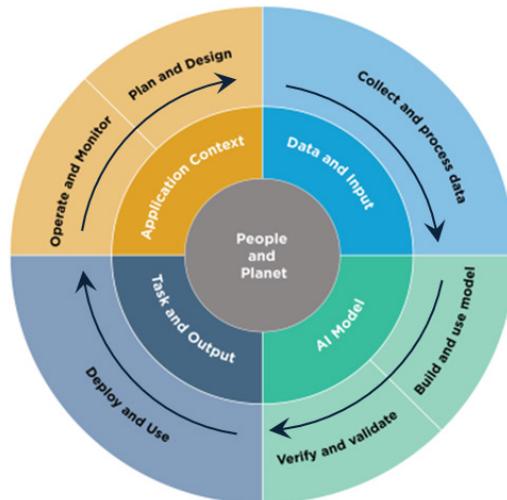
- Bestehende Modellrisiko Management (MRM) Frameworks sind nicht ausreichend für KI / ML Modelle, können aber erweitert werden
- Transparenz und Fairness sind zentrale Punkte die noch nicht inkludiert sind



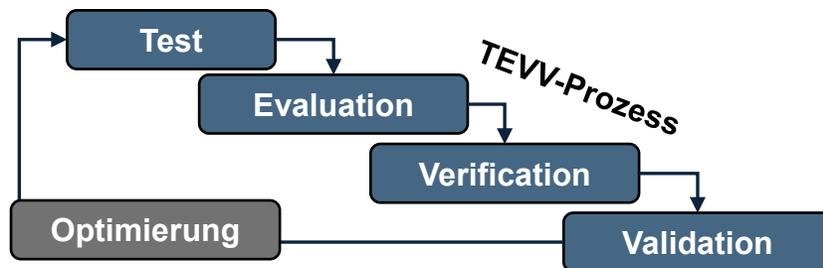


NIST Definition für KI / ML Lebenszyklus & trustworthiness

Grundgerüst – KI / ML Lebenszyklus



Quelle: NIST AI Audience [LINK](#)



AI Trustworthiness



Quelle: NIST AI Risks and Trustworthiness [LINK](#)

Erklärbarkeit and Interpretierbarkeit

- **Erklärbarkeit** ist erreicht wenn, „wie wurde entschieden“ beantwortet werden kann
- **Interpretierbarkeit** ist erreicht wenn, „wieso wurde so entschieden“ immer beantwortet werden kann
- Zentral verknüpft ist auch: **Transparenz**, „was passiert im System“ muss beantwortet werden können

Fairness – schädlichen Vorurteilen gemanagt

Fairness zielt auf die Sorge um Gleichheit und Gerechtigkeit ab

- Schädliche Vorurteile und Diskriminierung sind zentrale Themen (Datengrundlage)
- Standards für Fairness sind komplex und schwer zu definieren, bspw. durch unterschiedlich Wahrnehmung in verschiedenen Kulturen oder je nach Anwendung



Mit Regulatorischen Veröffentlichungen und Spezifika von KI & ML lassen sich Fokus Themen für die Governance ableiten

	Anforderung	Neuartigkeit	Komplexität
Angemessenheit	Ähnliche Anforderung wie an traditionelle Modelle: KI & ML Ansätze erfordern neue Ansätze der Validierung, stärkere Fokussierung auf Daten, laufende Überwachung notwendig.	 BCBS (z.B. risk data aggregation & risk reporting), Basel Core Principles, CRR II/III, TRIM	 Bedingt durch die hohe Komplexität der Modelle und dem spezifischem Modelzyklus
Transparenz / Erklärbarkeit	Erklärbarkeit der Methode eines der kritischsten Thema bei KI & ML: Anwendung neuer Methoden wie XAI – Explainable AI notwendig. Ansätze erfordern Know-How Aufbau und neue technische Lösungen	 Nur wenige Vorgaben in bestehender Regulatorik (CRRII/III)	 Machine Learning Algorithmen i.A. Black-Boxes
Fairness, Ethik	Hohe Gesellschaftliche Relevanz - Aktuell noch nicht ausreichend berücksichtigt Intensive Forschung und Weiterentwicklungen im Thema zu beobachten. Erfordert neue Betrachtungsweise auf Daten, Methoden und Ergebnisse	 Keine Berücksichtigung in bisheriger Regulatorik für Banken.	 Front-to Back zu Berücksichtigen, keine Erfahrungswerte, unpräzise Vorgaben.
Accountability	Zusätzlich Anforderungen im Vergleich zu traditionellen Modellen Human-in-the-Loop: Menschliche Einflussnahme bei Entscheidungen Human-on-the-Loop: Menschlicher Einfluss im Design und Review	 BCBS (Corporate governance principles for banks), Basel Core Principles, CRR II/III	 Prozessualer Aufwand mit Ressourceneinsatz inkl. Dokumentation
Datenschutz, Third Party	<ul style="list-style-type: none"> • Datenschutz: Sicherstellung der Privatsphäre in allen Schritten der Verarbeitung ggf. Abfrage über Verwendung der Daten für Training • Third Party: Gleiche Anforderungen wie bei In-House Anwendungen 	 Umfangreiche Detaillierung und Regulierung durch DSGVO	 Neue Kundenkommunikation und Datenschutzkonzepte notwendig



Transparenz und Fairness sind sowohl wichtige als auch sehr stark herausfordernde Themen

Angemessenheit

Transparenz / Erklärbarkeit

Fairness, Ethik

Accountability

Datenschutz, Third Party

Fairness, Ethik eng mit Transparenz / Erklärbarkeit verbunden

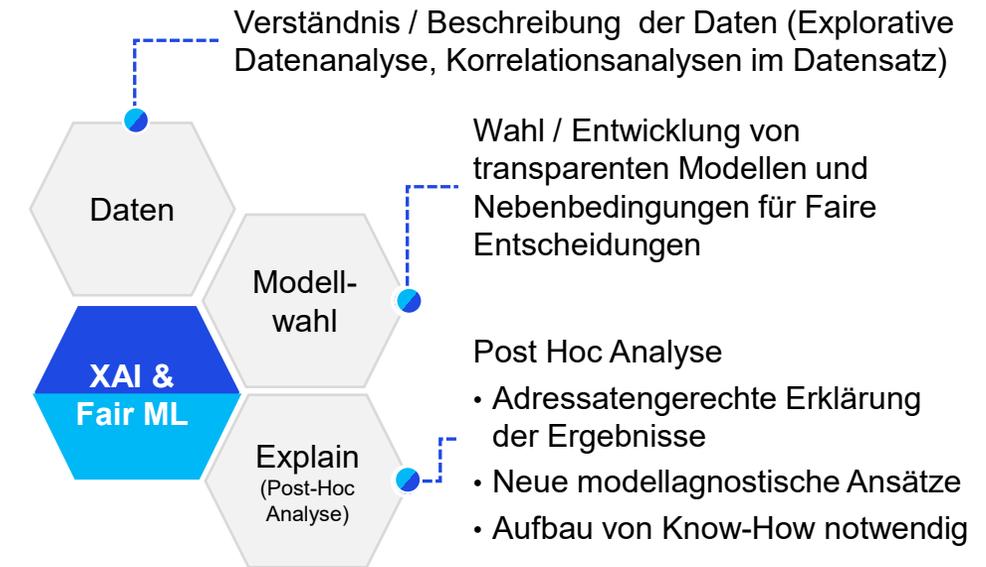
Herausforderung für Banken

- **Komplexität & Menge der Daten**
(Sicherstellung das in Daten kein Bias vorliegt)
- **Methodenwahl – Abwägung zwischen Performance, Transparenz und Fairness**
- **Black Box Charakter von ML Ansätzen erschwert Erklärbarkeit**
- **Laufende Überwachung + Darstellung ggü. unterschiedliche Adressaten**
- **Definition Fairness und deren Operationalisierung** (inkl. Abgrenzung positiv Bias)
- **Definition von ethischen Vorgaben**
(Fairness nicht identisch mit Ethischen Verhalten)

Explainable AI (XAI) und Fair AI als Ankerpunkt für Transparenz, Erklärbarkeit und Fairness

Herausforderung für Banken

Explainable AI und Fair AI beschreiben neuartige Ansätze um Machine Learning Methoden transparent, erklärbar und Fair zu machen



Die Definition und Umsetzung von Fairness in mathematischen Formeln sind eine der größten Herausforderungen für Banken

Was ist Fairness?

Die Definition des Begriffs "Fairness" hängt von der jeweiligen Perspektive und Umständen ab.

Folglich gibt es keine einheitliche Definition, die auf alle Fälle zutrifft⁽¹⁾, z.B:



(Antidiskriminierungs-)Gesetz



Philosophie



Sozialwissenschaften / Öffentliche Meinung

Die Definition von Fairness ist in diesen Bereichen in der Regel sehr abstrakt. Für die ML-Anwendungen ist eine Übersetzung in mathematische Begriffe notwendig.



Quantitative Bereiche

In **quantitativen Bereichen** ist Fairness ein mathematisches Problem, bei dem eine Art von Kriterien erfüllt werden muss

Herausforderungen

- Es gibt keine richtige Antwort, wenn es darum geht, Fairness zu definieren
 -
 - Unterschiedliche Interessengruppen haben ein unterschiedliches Verständnis von Fairness (Kunden, Management, Regulierungsbehörden, unterschiedliche Kulturen)
 -
 - Die Übersetzung einer Fairness-Definition in mathematische Formeln ist nicht immer eindeutig und kann zum Verlust von Nuancen führen
 -
 - Die Wahl einer Fairness-Definition bedeutet, Kompromisse einzugehen - und diese Kompromisse müssen dokumentiert und verstanden werden
 -
 - Unlauterkeit kann nicht nur durch das Modell, sondern auch durch die Verwendung oder den Benutzer des Modells selbst entstehen
 -
 - Eine unsachgemäße Anwendung von ML führt zur Reproduktion oder sogar zur Verstärkung von Verzerrungen

Ansätze zur Gewährleistung von Fairness

Quantitative Maßnahmen (Beispiele)

- Definition und Verwendung verschiedener Fairness-Kennzahlen
- Vorverarbeitungsmethoden - Anpassung der Trainingsdatenbank
- Prozessbegleitende Methoden - Anpassung des Modells selbst, das zum Lernen verwendet wird
- Post-Processing - Anpassung der Ergebnisse des maschinellen Lernalgorithmus

Qualitative Maßnahmen (Beispiele)

- Dokumentation des Modells und der getroffenen Entscheidungen
- Checklisten mit verschiedenen allgemein anerkannten Fairness-Kriterien
- Bedienungsanleitungen, Anwenderschulungen, Sensibilisierung von Entwicklern und Anwendern

⁽¹⁾ Diese Sache wird Fairness genannt: Disziplinäre Verwirrung, die einen Wert in der Technologie verwirklicht. Mulligan, Kroll, Kohli Wong. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Artikel 119 (November 2019)

Fairness kann in jedem Schritt der Modellimplementierung sowohl überprüft als auch eingeführt werden

Quellen für mangelnde Fairness

Daten-erfassung  Input-Daten basiert teilweise auf historischen Daten, die manuell von Personen erstellt wurden. Datenselektion bzw. Reduktion im Modelsetup kann auch zu **ungleichmäßigen Verteilungen** führen

Transparenz/Erklärbarkeit  Die Art und Weise, wie das **Modell** entwickelt wurde oder wie das Modell trainiert wurde, führt zu ungerechten Ergebnissen

Fairness, Ethik  Nachdem das Modell trainiert wurde, müssen die Ergebnisse **interpretiert** werden, um sie weiter zu verarbeiten.

Anpassung um Fairness zu gewähren

Pre-Processing  Anpassen der Input-Daten entsprechend der gewählten Fairness Definition z. B. synthetische Daten für **unterrepräsentierte Gruppen** erstellt werden

In-Processing  Training berücksichtigt neben bspw. Genauigkeit weitere definierte **Fairnesskriterien**, um sicherzustellen, dass diese vom Model eingehalten werden.

Post-Processing  Die **Ergebnisse** können **direkt angepasst** werden, z.B. indem es für bestimmte Minderheiten-gruppen einfacher wird, ein "positives Modellergebnis" zu erhalten.

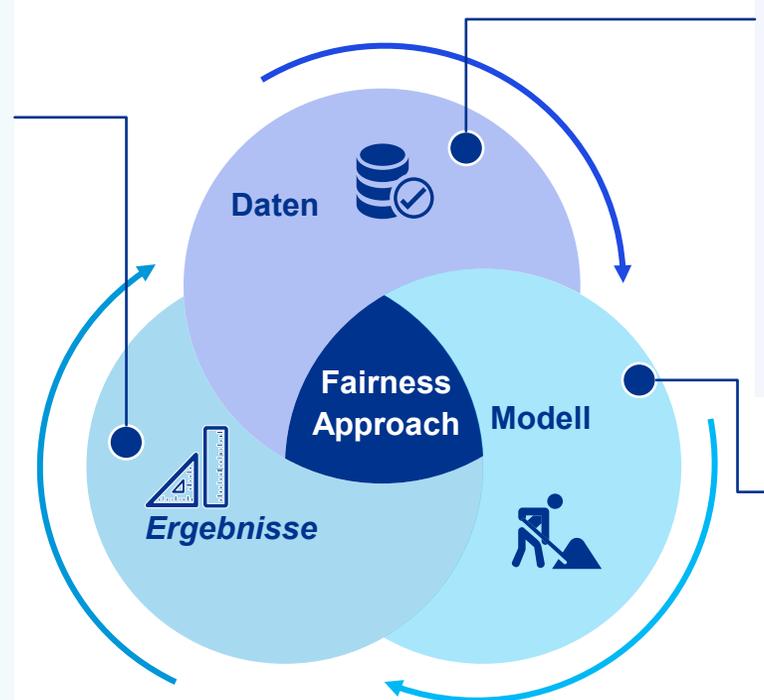
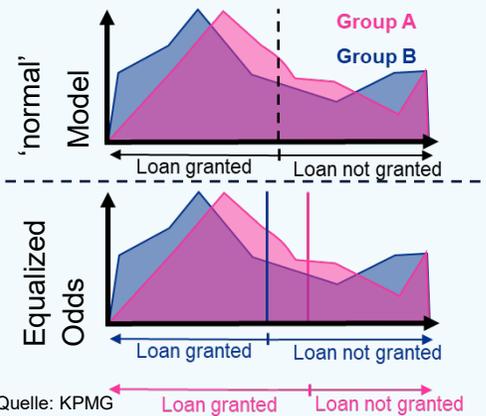
 **Da mangelnde Fairness auf allen drei Ebenen vorhanden sein kann - d.h. in den Daten, dem Modell und seiner Verwendung - muss die Überprüfung der gewählten Fairness Metrik erfolgen**

Beispielhafte Implementierungsansätze für Fairness im generischen ML Ansatz

Post-Processing

Die Ergebnisse können direkt angepasst werden, z.B. unterschiedliche Grenzwerte

- Equalized Odds
- Calibrated equalized odds



Pre-Processing

Der Vorverarbeitung von Daten können die Trainings-daten verändert werden, um Verzerrungen zu verringern:

- Sampling
- Reweighting, Relabeling
- Data Transformation
- Synthetic Data

In-Processing

In-Processing-Algorithmen versuchen, das Lernverfahren für ein maschinelles Lernmodell zu ändern, z. B.

- Adversarial Debiasing
- Prejudice Remover
- Exponentiated-gradient reduction

- Die Stellschrauben für **Fairness** und **Erklärbarkeit** sind exzellente Ansatzpunkte um die geforderten regulatorischen Anforderungen zu implementieren
- Bspw. sollen für generative Modelle alle Trainingsdaten zugänglich und gesondert abgelegt werden, was in ein Modell mit Pre-Processing leicht ermöglicht wird, da direkt die adjustierten Trainingsdaten zugänglich und ablegbar wären.

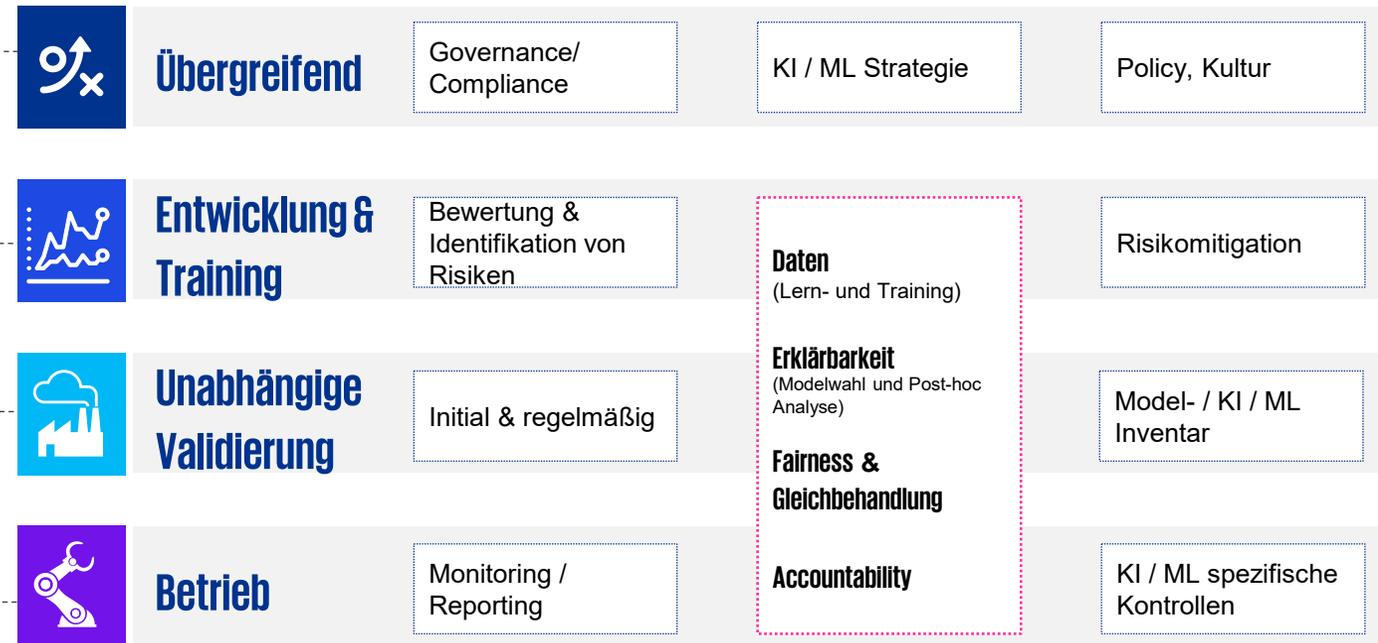
Spezifische Anforderungen und Regulatorik erfordern strikte Governance – Synergien zu bestehendem Framework möglich

KI & ML Governance

- Bei Verwendung von Machine Learning ist die Governance anzupassen bzw. zu erweitern:
 - Grundlage EU AI act
 - Einbettung 7 Punkte von trustworthy AI
- Integration in die bestehenden Prozesse (z.B. Model-Governance) ist möglich
- Analyse der verwendeten Risikoklasse des verknüpften regulatorischen Aufwands
- Anpassung bzw. Umstrukturierung der Prozesse für bestehende Ansätze (z.B. Kreditscoring) bedingt durch Fokus von **Fairness** und **Erklärbarkeit** ggf. notwendig



Komponenten einer KI / ML Governance



Quelle: KPMG

IT-Framework

Ausblick & Zusammenfassung – Zeit für Ihre Fragen, Anmerkungen und Ideen

01

EU AI Act – Kernthemen & News

- Einstufung der Modelle in Risiko Kategorien, mit besonderen Auflagen für “high-risk” Modelle
- Verankerte zentrale Aspekte in der Modellkonzeption
- Eine weitere Hürde im Gesetzgebungsprozess wurde genommen, Auswirkungen auf Banken unverändert

02

Herausforderung durch auferlegte Regulatorien

- Identifikation aller potenziell betroffenen Modelle
- Umbau bestehender Modelle zur besseren Vorhersagen ohne regulatorische Konsequenzen zu befürchten

03

Chancen für die zukünftige Modellentwicklung

- Planungssicherheit für neue klassische sowie KI / ML Modellentwicklungen
- Neuorganisation des MRM auf einem sicheren, regulatorischen Fundament
- Erweiterung der MRM Tools durch KI / ML mit klar definierten, regulatorischen Anforderungen



Nächste Woche: CSRBB und die Auswirkungen auf die Steuerung der Handelsrisikopositionen

	10.05.	Kapitalmarkt im Umbruch – Effekte im Überblick
	17.05.	ESG im Marktpreisrisiko – Erste Erfahrungen und Lösungsansätze
	24.05.	Machine Learning im Risikomanagement – Aktuelle Entwicklungen
Next 	31.05.	Überblick CSRBB und die Auswirkungen auf die Steuerung der Handelsrisikopositionen
	07.06.	Counterparty Credit Risk und Initial Margin – Zurück im Fokus?
	14.06.	Model Risk Management – Banken unterschätzen die Risiken einer unzureichenden Modell-Governance
	21.06.	Erfahrungen aus dem Energy Trading – Was können Banken aus den Turbulenzen im Energiesektor lernen?

Kontakte



Matthias Peter
Partner, Financial Services
+49 172 3006809
matthiaspeter@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt am Main



Dr. Christoph Anders
Manager, Financial Services
+49 151 10628659
christophanders@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft
Schlossgartenstrasse 1
68161 Mannheim



Janek Gallitschke
Senior Manager, Financial Services
+49 174 3016082
jgallitschke@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt am Main



Dr. Daniel Wehl
Assistant Manager, Financial Services
M +49 160 328 4942
danielwehl@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft
Ganghoferstraße 29
80339 München



kpmg.de/socialmedia

kpmg.de

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2023 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.

Document Classification: KPMG Public

Alles aber hier kann wsl zeitnah weg



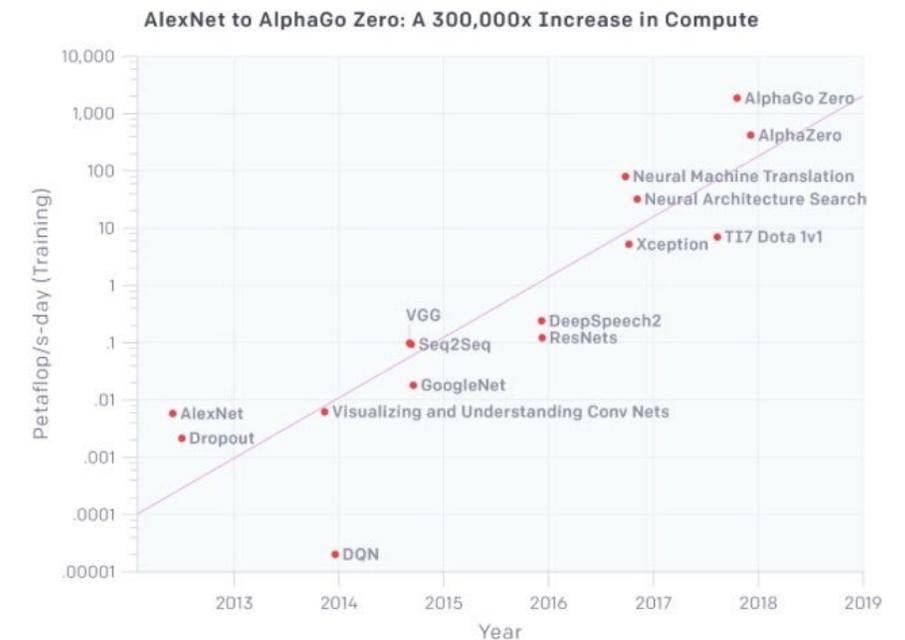
Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2023 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.

Document Classification: KPMG Public

ChatGPT – Breakout der generativen KI & Erhöhter Druck und Dringlichkeit der fehlenden Regulierung

- Neben ChatGPT veröffentlicht Google ebenfalls generative Chat KI'
- Amazon plant ebenfalls sich zu beteiligen ob über fertig Lösungen a la ChatGPT oder den computing Dienst Amazon Web Services (AWS) an Firmenkunden
- Geht das Entwickeln mit generativer KI ins ungebremst weiter?
- Steigerung der Rechenleistung in den größten KI-Projekten der vergangenen Jahre
- In den Jahren 2012 bis 2017 gab es eine Steigerung um den Faktor 300.000
- Verdoppelung der Rechenleistung alle 3.5 Monate, bei Moore's Law ist die Doppelungsrate 18 Monate
- Wachstum wird durch Hardware irgendwann gebremst -> Anpassung der Chip-Entwicklung etc. ...



[Palm 2: Google soll morgen neues KI-Modell vorstellen \(t3n.de\)](https://t3n.de)

[Nach Microsoft und Google: Jetzt steigt auch Amazon ins KI-Rennen ein - DER AKTIONÄR \(deraktionaeer.de\)](https://deraktionaeer.de)

Machine Learning wird in Banken vom Front bis ins Back Office angewendet

Kunden-Akquise / Sicherung

- Individualisierung von Kundenangebot inkl. Cross-Selling,
- „Self-Driving Finance“ & Verbesserung der Kundenerfahrung
- Identifikation von Marktpotentialen

Datenmanagement

- Verbesserung und Automatisierung, Prüfung der Datenqualität
- Inhaltliche und prozessuale Optimierung des internen / regulatorischen Reportings

Risikomanagement

- Verbesserung der Berechnungsmethodik
- Verbesserung der Datenqualität
- Intradayfähigkeit
- Prozessoptimierung, Validierung



Neugeschäftsabschluss

- Verbesserung Kundeninformationen inkl. KYC
- Verbesserung von Geschäftsentscheidungen (Kreditscoring, Pricing)

Compliance & Fraud

- Identifikation von Geldwäsche (AML)
- Erkennen Konto-/ Kreditkartenbetrug
- Unterstützung von Cybersecurity
- Überwachung von Händleraktivitäten

Markt-Infrastruktur

- Optimierung der „Post-Trade“ Prozesse
- Verbesserung der Trade Execution (in instabilen Märkten)

Auswahl an Use Cases

Der EU Entwurf "Regulation on a European approach for Artificial Intelligence" ist nicht spezifisch für Finanzinstitute – Banken sind jedoch betroffen

Überblick⁽¹⁾

Der Knackpunkt



"... a proportionate and risk-based European regulatory approach"

"... provides for a technology-neutral definition of AI systems that is future-proof"

"The proposed draft regulation lays down a ban on a limited set of uses of AI"

- "... the proposal focuses on so-called 'high-risk' AI use cases"
- "high-risk AI systems need to respect a **set of specifically designed requirements**"
- "High-risk AI systems **must be assessed for conformity** with these requirements **before being placed** on the market or put into service."
- "**other uses of AI systems** are only subject to minimal transparency requirements"



Effekte auf Finanzinstitute vorhanden –
Regulatorik mit Ziel des Schutzes der Kunden und allg. Kunden- und Menschenrechte

Wichtige Aspekte

Definition von Machine Learning (Art. 3 & Annex I)

- Sehr weitgehende Definition von ML

- "supervised, unsupervised and reinforcement learning,[...] including deep learning."
- „Logic- and knowledge-based approaches“,
- "Statistical approaches, Bayesian estimation, search and optimization methods"

Einstufung High- Risk AI (Art.6 & Annex III)

- Verwendung allgemeiner Grundsätze & konkreter Beispiele
- Auch für Banken relevant

- Beispiel:** "Access to and enjoyment of essential private services and public services and benefits":
- "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score"

Anforderung an High-Risk AI (Art. 8-51 & Annex IV)

- Sehr umfangreiche Anforderungen inkl.
- Genehmigungsverfahren

Anforderungen (Auszug):

- Risk Management System, Data & data Governance, Dokumentation
- Transparency and provision of information to users, Human oversight
- Quality Management System für Compliance

Non High-Risk AI

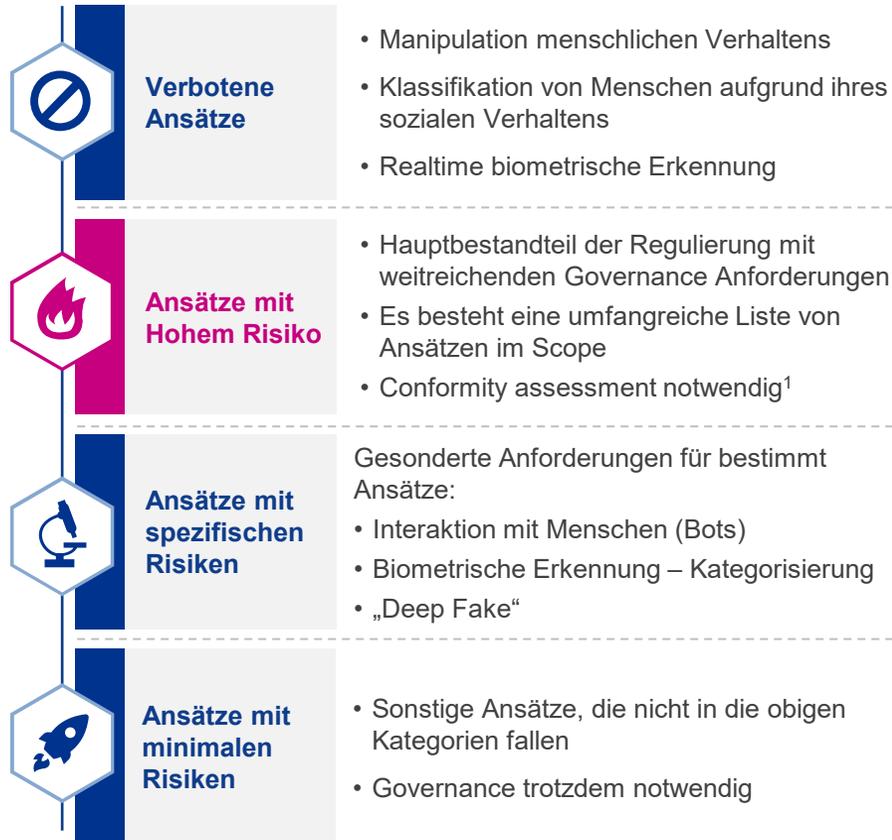
- Sehr weitgehende Definition von ML

- Informationspflicht von natürlichen Personen wenn diese mit AI Systemen interagieren
- Transparenz bei "emotion recognition system" "biometric categorisation system" oder bei AI Systemen die Bilder oder Videos manipulieren

(1) Published: April 2021: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence>

EU AI Act Details – für Hochrisiko AI Anwendungen gibt es hohe Anforderungen bzgl. der Governance – Kredit scoring wird explizit genannt

Clustering der AI Ansätze



(1) Teilweise muss das Assessment durch eine "third party/ notified bodies" erfolgen -

Details - Ansätze mit hohem Risiko

Scope

- ! In Anhang III des EU AI Act erfolgt eine Konkretisierung der Hoch-Risikoansätze. Für Banken und Versicherungen ist die Kategorien 5 relevant:
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistung:
„KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Kreditpunktebewertung natürlicher Personen verwendet werden sollen, [...]“
- Überprüfung des Scopes durch Aufsicht möglich

Conformity Assessment and Presumption

- ! Vor Einführung: Durchführung eines Assessments der Einhaltung der Anforderungen des AI-Acts
- Self-Assessment möglich, nur in Ausnahmen Conformity Assessment durch „notified bodies“
- Basis des Assessments kann auf harmonisierten Standards beruhen oder auf Basis des AI Acts
- Governance Anforderung für High-Risk untergliedert sich in X Themengebiete
- Durchführung eines post-market Monitorings notwendig

Standardisierungs-Frameworks

- **ISO & NIST -> es gibt Bemühungen zur Standardisierung von Risk Management für AI Modelle – EU AI Act könnte auch darauf abheben (siehe Mail-Extract von Janek)**
- **Key Punkte aus ISO:**
- **Key Punkte aus NIST die zentral für die trustworthiness von AI Modellen sind**
 - Trustworthiness von AI – was macht trustworthiness aus: zB Fairness, INterpreteability, Explainability, Robustness etc.
([NIST AIRC - AI Risks and Trustworthiness](#))
 - Ggf welche Prozesse müssen Unternehmen dafür aufsetzen (high level) – siehe NIST AI Risk Management Framework