AI Act Ready: AI Governance und AI-Metadatendokumentation in der Bankpraxis

Donnerstag, 10.04.2025

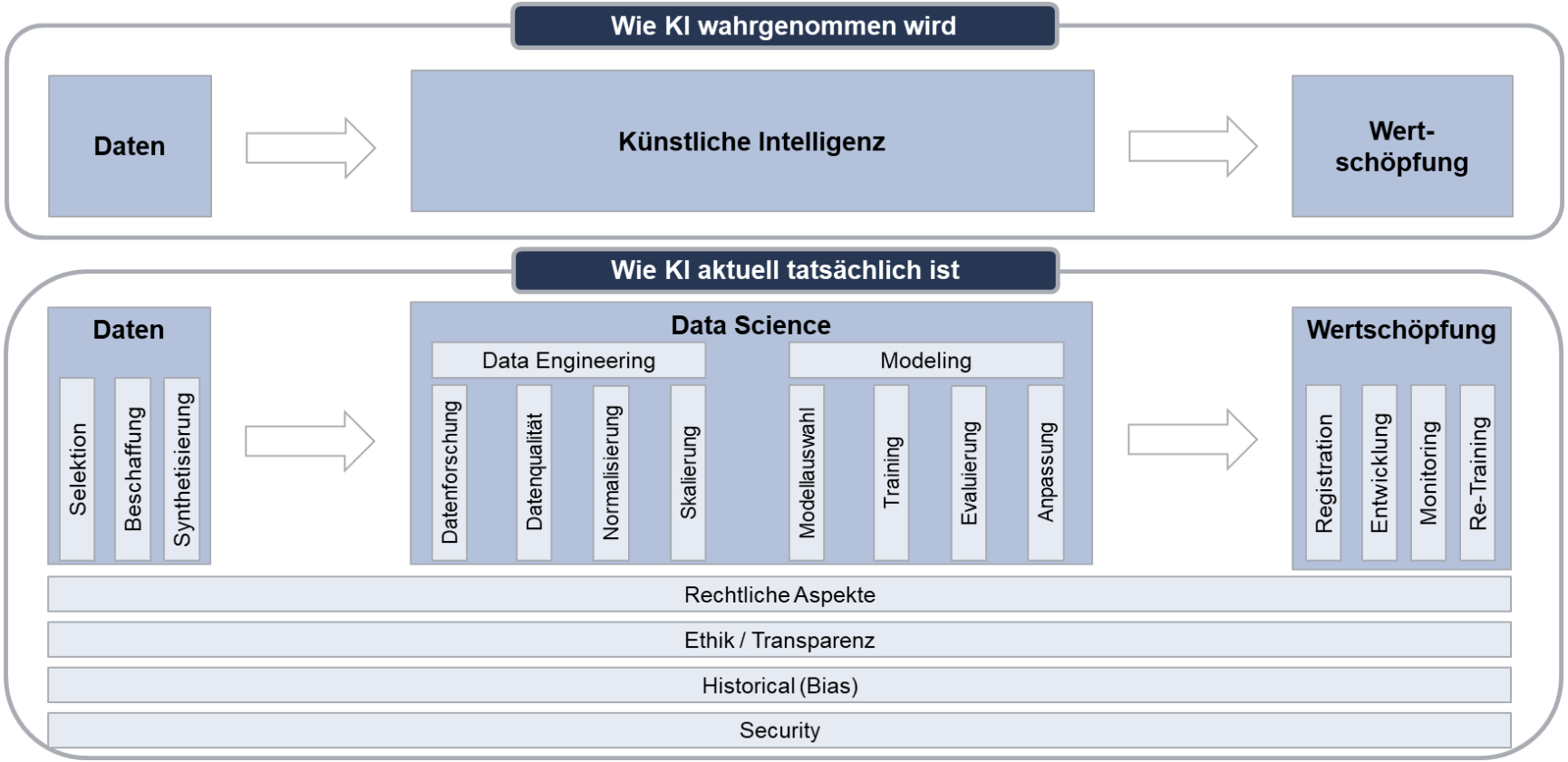
Der Volksbanken-Verbund

- Bankengruppe: 8 regionale Volksbanken
  + Ärzte & Apothekerbank
  + Marke SPARDA Bank
- Mitarbeiter: 3.158 Vollzeitäquivalente
- Vertriebstellen: 236 österreichweit
- Kunden: ~ 1 Million
  (Stand: 31.12.2024)

Volksbank Wien AG

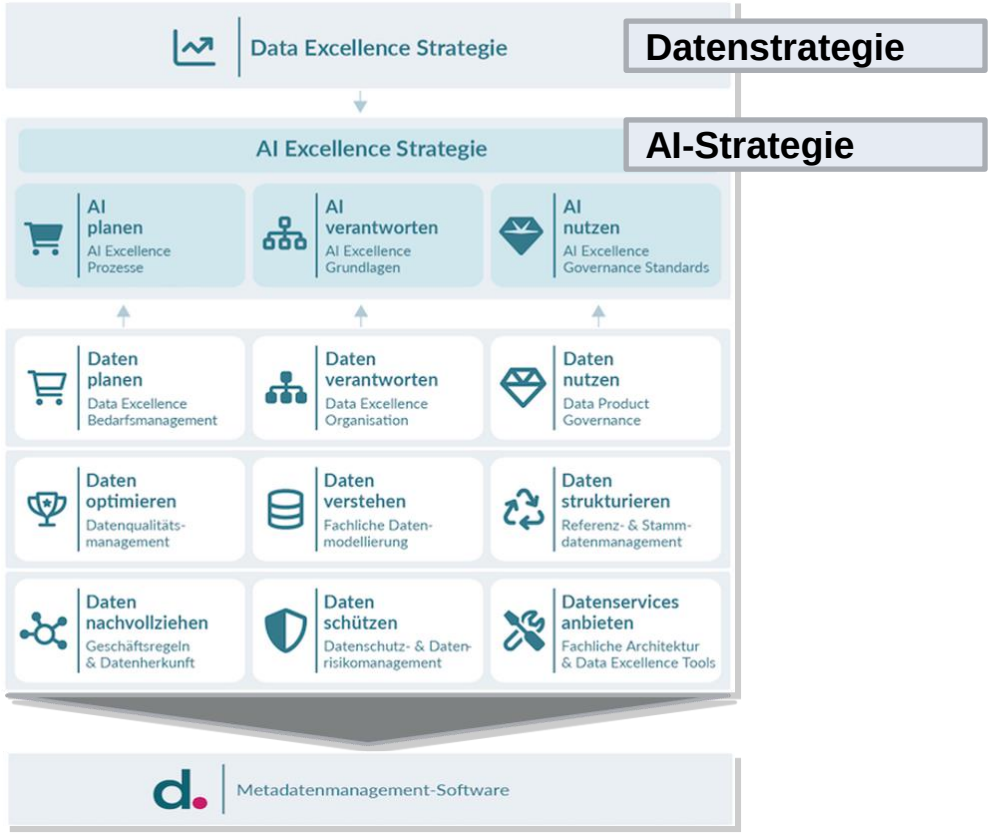
- Mitarbeiter: 1.306 Vollzeitäquivalente
- Vertriebstellen: 54 in mehreren Regionen
- Neben dem eigenen Retailgeschäft erfüllt die Volksbank Wien AG als Zentralorganisation übergeordnete Aufgaben.

Wahrnehmung vs Realität



© Andy Scherpenberg

AI-Strategie als Teil
der Datenstrategie



© dataspot.

Data Governance als Basis, ergänzt um AI

Datenarchitektur

Ergänzung um:

- AI Funktionen
- AI Modellen

Datenanforderungs-Management

Ergänzung um:

- Prozessschritte für Risikobewertung
- EU-AI-Act Dokumentation

Rollen, Meetings, Verantwortlichkeiten

Ergänzung um:

- Rollen im AI-Bereich

Herkunft & Verwendung der Daten

Ergänzung um:

- fachliche Lineage
- technische Lineage

VB-Fachdatenmodell

Ergänzung um:

- unstrukturierte Daten

Datenqualitäts-Management

Erweiterung auf:

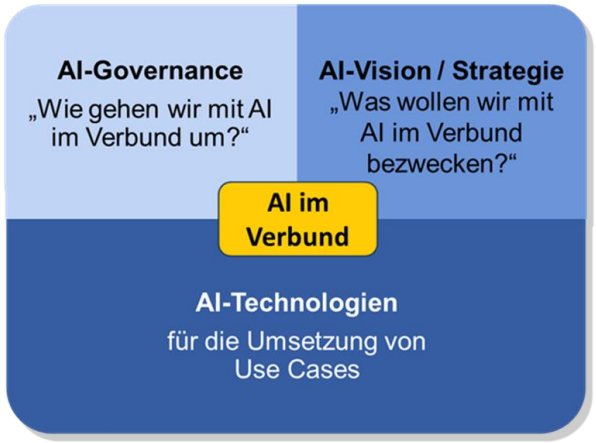
- unstrukturierte Daten

DQ-Reporting

Ergänzung um:

- AI relevante Informationen

- AI-Lifecycle-Management
- AI-rechtliche Vorgaben
- AI-Rahmenbedingungen
- AI-Datenprodukte & Bestandteile
- AI-Rollen, Meetings/Gremien
- AI-Qualitäts-Management
- AI-Reporting



→ AI = unterstützendes Tool zur Steigerung der Effektivität/Effizienz

→ Mitarbeiter aktiv, bewusst kritisch im Entscheidungsprozess eingebunden (→ Human in the Loop) & nicht im direkten Kontakt mit den Kund:innen

→ im Einklang mit Unternehmenszielen & -werten

VOLKSBANK WIEN

Maßnahmen zur Unterstützung der AI-Governance

AI-Prozesse

- AI-Governance Weiterentwicklung
- AI-Risiko- & Auswirkungs-management
- AI-Compliance Management
- AI-Klassifizierung
- AI-Datenmanagement

AI-Management

- AI-Organisation & Skills
- AI-Reporting
- AI-Monitoring & Auditmanagement

AI Governance Standards

- AI-Kreislauf Überwachung
- AI-Klassifizierungsvorgaben
- Fachliche- & Technische Dokumentation
- AI-Qualitätsmanagement

© dataspot.

AI-Rahmenbedingungen

Gesetzes- und Regelkonforme AI-Nutzung

- EU AI Act
- DSGVO
- Arbeitnehmerschutz
- IT-Sicherheit

Speicherung und Verarbeitung von Daten

Keine Weitergabe von bankinternen, vertraulichen Informationen nach außen

Zentral Verwaltung der AI-Funktion und AI-Modelle

Durch "Data Governance & Data Management"

Geistiges Eigentum

Achten auf Urheberschutz

Fachkräfte- und Talentwentwicklung

Sicherstellung Know-How

Ethische Grundhaltung

Keine:

- Diskriminierung
- Irreführung
- Manipulation

Überprüfung der AI-Ergebnisse

- Zuverlässigkeit
- Qualität
- Obektivität

Sicherheit und Robustheit

Überstehen potenzieller Bedrohungen durch Cyberangriffe oder Systemausfälle

Kennzeichungspflicht

Bild, Ton, Videos, die als echt erscheinen können

Dokumentation der AI

im Metadatenmanagementtool dataspot.

Risikoeinstufung

© Jeannette Gorzala

VOLKSBANK WIEN

AI Bestandteile

AI-Funktion

KI-System

- Konzepte des **maschinellen Lernens**
- **Logik- und wissensgestützte Konzepte**, inklusive
  - Wissensrepräsentation
  - Induktive/logische Programmierung
  - Wissensgrundlagen
  - Inferenz- und Deduktionsmaschinen,
  - symbolische Schlussfolgerungssysteme
  - Expertensysteme
- **Statistische Ansätze**
- Bayessche Schätz-, Such- und Optimierungsmethoden

KI-System

[...] ein **maschinengestütztes System**, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den **erhaltenen Eingaben für explizite oder implizite Ziele ableitet**, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

✅ Maschinelles Lernen

✅ Logik- & wissensbasierte Ansätze

❌ Einfache Datenverarbeitungen

❌ 'Einfache herkömmliche' Softwaresysteme & Programmieransätze

❌ Ausschließlich von natürlichen Personen definierte Regeln für automatisches Ausführen von Operationen

AI-Modell

- Machine Learning
  - Klassifikation
  - Vorhersage
- Deep Learning
  - Bildverarbeitung
  - Mustererkennung
- Reinforcement Learning (lernender Roboter)
  - Prozessoptimierung

KI-Modell mit allgemeinem Verwendungszweck

[...] ein KI-Modell, einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird, das eine **erhebliche allgemeine Verwendbarkeit** aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein **breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen**, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden.

- Large Language Models (LLMs)
  - Verstehen natürlicher Sprache
- Gen AI
  - Erstellung neuer Inhalte (Text, Bild, Audio)

© Jeannette Gorzala

AI-Rollen & Meetings

AI-Funktion Verantwortlicher

- Korrekte Metadaten im AI-Funktionen-Register
- Überwachung der Leistung & Sicherheit der AI-Funktion
- Verantwortung für Schulungen zur AI-Funktion
- Identifizierung potenzieller Risiken und Entwicklung von Strategien zur Risikomitigierung
- Integration der Ergebnisse in weiterführende Prozesse

AI-Modell Verantwortlicher

- Korrekte Metadaten im AI-Modell-Katalog
- Effektives Design, Implementierung und Zuverlässigkeit der AI-Modelle
- Ethische Vertretbarkeit der AI-Modelle, sowie Einhaltung der Datenschutz- und Regulierungs-bestimmungen
- Qualitätssicherung der Input-Daten

AI-Risikobewertungsteam

- Betriebsrat
- Compliance (Datenschutz)
- IT-Security
- ORG-IT
- Personalabteilung
- Rechtsabteilung
- Risikocontrolling

Data Manager & Data Steward

- Erweiterung der Rollen um AI-Themen

Datenqualität

Anwendung der:
- Data Governance Regelungen
- Erweiterung um unstrukturierte Daten

Ergebnisqualität

- Genauigkeit & Relevanz
- Benutzerfeedback
- Vergleich mit Experten Antworten

Regelmäßiges Review der AI-Funkionen

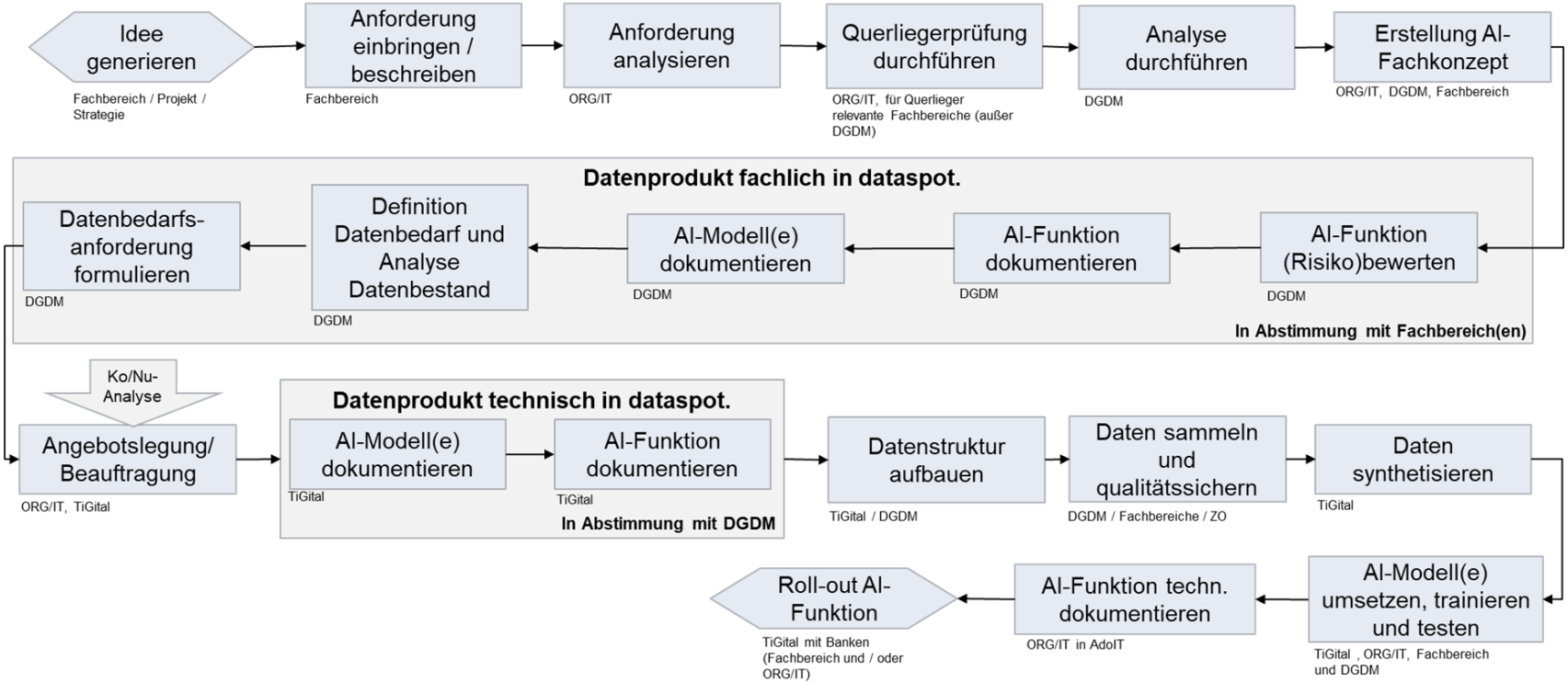
Prüfung der:
- Verantwortlichkeiten
- Funktionsweise
- Ergebnisse/Output
- Risikobewertung
- Dokumentation (AI-Funktion & AI-Modelle)

Promptingqualität (→ GenAI Models)

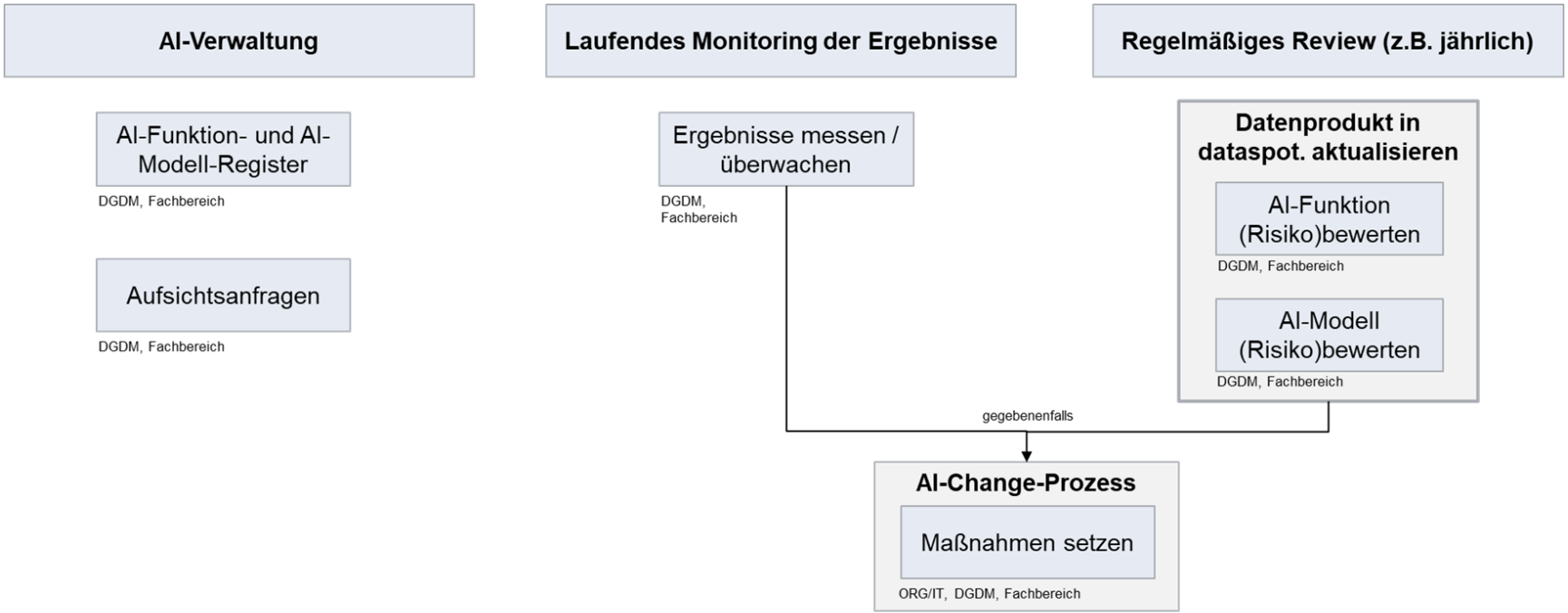
- klare, präzise Formulierung
- Kontext & Beispiele bereitstellen
- Iteratives Testen & Verfeinern
- Verwendung von Metaprompts
- Ethik und Sicherheit berücksichtigen

- Liste der AI-Funktionen
- Risikobewertung
- Status
- Nutzung
- Weiterentwicklung der AI-Modelle
- Eingetretene Risiken
- Einhaltung der AI-Governance

Volksbank AI-Lifecycle
Überblick



Volksbank AI-Lifecycle
Abwicklung



VOLKSBANK WIEN

Live Demo


VOLKSBANK