KI-Reallabore im Sinne der KI-Verordnung

Umsetzungsempfehlungen für Behörden

Version: 1.0

Veröffentlichung: 18.09.2025

Bearbeitet von: Maria Rill, Antonio Scaduto, Aline Vugrincic, Christina Erler

– Inhaltsverzeichnis

1 Einleitung

Dieses Dokument richtet sich an Entscheidungsträgerinnen und Entscheidungsträger in Behörden auf kommunaler, Landes- und Bundesebene, die den Betrieb eines KI-Reallabors im Sinne der KI-Verordnung (KI-VO) in Erwägung ziehen. Es bietet konkrete Handlungs- und Umsetzungsempfehlungen zur erfolgreichen Initiierung, Durchführung und Verstetigung von KI-Reallaboren im öffentlichen Sektor. Es basiert auf der wissenschaftlichen Analyse der Regulatorik zu Reallaboren sowie der Umsetzung bereits existierender Reallabore und stellt keine Rechtsberatung dar. Ziel ist es, praxisorientierte Leitlinien bereitzustellen, die sowohl strategische als auch operative Aspekte berücksichtigen: von der Bedarfsermittlung über die Projektplanung bis hin zur Evaluation und Skalierung.

Künstliche Intelligenz (KI) zählt zu den zentralen Zukunftstechnologien unserer Zeit und bietet enorme Potenziale zur Effizienzsteigerung, Entscheidungsunterstützung und innovativen Leistungserbringung im öffentlichen Sektor. Um diese Potenziale systematisch und verantwortungsvoll zu erschließen, bedarf es experimenteller Räume, in denen neue Technologien unter realen Bedingungen erprobt und weiterentwickelt werden können – sogenannte KI-Reallabore.

KI-Reallabore ermöglichen es Behörden, innovative KI-Anwendungen praxisnah zu testen, regulatorische Rahmenbedingungen zu evaluieren und gleichzeitig gesellschaftliche, ethische und datenschutzrechtliche Fragestellungen frühzeitig in die Entwicklung einzubeziehen. Damit leisten sie einen wichtigen Beitrag zur digitalen Souveränität und zur zukunftsfähigen Ausgestaltung staatlicher Aufgabenwahrnehmung. Zusätzlich schaffen Behörden mit dem Betrieb von Reallaboren eine Schnittstelle zu Wissenschaft und Wirtschaft, die es ihnen ermöglicht Einblicke in innovative Technologien und deren Anwendung zu erhalten und den Austausch zwischen Wirtschaft und Wissenschaft zu fördern.

Die Einrichtung und der Betrieb von KI-Reallaboren wird bereits unter anderem in Forschungsprojekten in verschiedenen Domänen wie beispielweise Mobilität und Gesundheit durchgeführt. Die KI-VO fordert nun die Einrichtung von sogenannten „Regulatory Sandboxes“, zu Deutsch auch „Reallabore“, von zuständigen Behörden. Konkretisierungen und Harmonisierungen für den Betrieb von KI-Reallaboren sind zwar erst mit der Veröffentlichung von Durchführungsrechtsakten zu erwarten. Jedoch können bereits auf bestehende Reallaboren aus dem Finanz-, Gesundheits- und Mobilitätsbereich Erfahrungen gewonnen und in Empfehlungen überführt werden. Im Rahmen dieses Dokuments werden allgemeine Empfehlungen exemplarisch insbesondere für KI-Reallabore im Sinne der KI-VO für den Gesundheitssektor dargestellt. Da die Empfehlungen keine konkrete Behörde adressieren, sondern allgemeingehalten sind wird entsprechend nicht auf konkrete Spezifika, die sich aus unterschiedlichen Behörden für die operative Umsetzung ergeben könnten, eingegangen.

2 Executive Summary

Mitgliedstaaten sind nach Art. 57 KI-VO verpflichtet, bis August 2026 nationale KI-Reallabore einzurichten. Reallabore können insbesondere zur Verbesserung der Rechtskonformität, Förderung von Best Practices und Innovationen eingesetzt werden. Der Gesundheitsbereich unterliegt spezifischen regulatorischen Rahmenbedingungen, wie dem Medizinprodukterecht, Arzneimittelrecht, verschärften Datenschutzbestimmungen und verschiedenen Haftungsregelungen. Diverse Stakeholder (Krankenhäuser, Arztpraxen, Pharmaunternehmen, Medizintechnikhersteller, Patienten, Pflegepersonal usw.) sind davon betroffen und müssen eng in die Prozesse eingebunden werden.

1. Was sind KI-Reallabore?

Zweck: Sie sind kontrollierte Testumgebungen, die Innovationen im Bereich künstlicher Intelligenz (KI) fördern, indem sie es Entwicklern ermöglichen, ihre KI-Systeme unter realen oder simulierten Bedingungen zu testen, bevor sie auf den Markt kommen.[1]

Rechtliche Grundlage: Die EU-KI-Verordnung (KI-VO), insbesondere die Artikel 57-61 KI-VO, verpflichtet die Mitgliedstaaten, mindestens ein KI-Reallabor einzurichten.

Ziele: KI-Reallabore sollen Rechtssicherheit schaffen, den Marktzugang erleichtern, Innovation fördern und regulatorisches Wissen aufbauen, Art. 57 Abs. 9 KI-VO.

2. Aufbau und Organisation

Zuständige Behörde: Laut aktuellem Entwurf zu Umsetzung der KI-VO wird die Bundesnetzagentur (BNetzA) diese Rolle einnehmen.[2] Auf Landesebene sind bisher keine Rollen benannt. Die Zusammenarbeit mit anderen relevanten Akteuren, wie Datenschutzbehörden und sektorspezifischen Aufsichtsbehörden (z.B. BaFin, KBA), ist dabei essenziell.

Personal: Ein multidisziplinäres Team ist erforderlich, bestehend aus Fachexperten für Technik, Recht und Betriebswirtschaft sowie Domänenspezialisten (z.B. für Gesundheit, Mobilität oder Finanzen).

Infrastruktur: Eine sichere und kontrollierte technische Testumgebung ist unerlässlich, ebenso wie der Zugang zu geeigneten Daten (reale oder synthetische) und die notwendige rechtliche Infrastruktur, wie standardisierte Verträge und ein Compliance-Framework.

3. Kernvoraussetzungen für den Betrieb

[1] BOTTA in: Martini/Wendehorst, Kommentar zur KI-VO, Art. 57 Rn. 4.

[2] https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/CDR_Anlage1-250911_RefE_KIVO-Durchf%C3%BChrungsgesetz_Entwurf_barrierefrei.pdf , zuletzt abgerufen 22.09.2025.

Datenschutz: Die Einhaltung der DSGVO ist von höchster Bedeutung. Dies erfordert technische Maßnahmen wie die Verschlüsselung und Pseudonymisierung von Daten sowie organisatorische Maßnahmen wie Datenschutz-Folgenabschätzungen (DSFA) und regelmäßige Audits.

Kommunikation: Ein regelmäßiger, strukturierter Austausch mit Regulierungs- und Aufsichtsbehörden ist entscheidend. Jährliche Berichte und eine systematische Aufbereitung der gesammelten Erkenntnisse (sogenannte "Lessons Learned") sind dabei essenziell, um zukünftige Gesetzesanpassungen zu unterstützen.

Stakeholder-Einbindung: Neben den Entwicklern müssen auch andere Akteure wie Endnutzer, Verbraucherschutzorganisationen und die Zivilgesellschaft einbezogen werden, um eine breite Akzeptanz und gesellschaftliche Relevanz zu gewährleisten.

Datenanforderungen: Der Zugang zu qualitativ hochwertigen realen oder synthetischen Daten ist für das Training und Testen von KI-Systemen unverzichtbar.

Risikomanagement: Ein kontinuierliches Risikomanagement-Framework ist notwendig, um potenzielle Gefahren (z.B. Grundrechtsverletzungen, Sicherheitsrisiken) frühzeitig zu erkennen, zu bewerten und zu mindern.

4. Phasenmodell für Projekte

Phase 1 - Aufbau und Vorbereitung: In den ersten Monaten werden die technische und organisatorische Infrastruktur sowie die rechtlichen Grundlagen geschaffen.

Phase 2 - Durchführung und Betrieb: Die Projekte werden kontinuierlich begleitet und überwacht. Eine flexible Steuerung und ein iteratives Vorgehen ermöglichen es, auf neue Erkenntnisse zu reagieren.

Phase 3 - Evaluation und Lessons Learned: Nach Abschluss eines Projekts werden die Ergebnisse systematisch ausgewertet (quantitativ und qualitativ). Die gewonnenen Erkenntnisse fließen in die Weiterentwicklung der regulatorischen Rahmenbedingungen ein.

5. Praktische Umsetzung & Erfolgsfaktoren

Schnelle Implementierung:

Ein realistischer Zeitplan sollte die Vorgaben der KI-Verordnung berücksichtigen. Eine schnelle Umsetzung erfordert eine klare Ressourcenplanung und das Sichern von Budgets.

Erfolgsfaktoren:

Klare Vision und Mandate: Jeder Beteiligte sollte die Ziele und Verantwortlichkeiten kennen.

Stakeholder-Buy-in: Alle relevanten Akteure müssen von Anfang an eingebunden werden.

Regulatorische Flexibilität: Die vorhandenen Ermessensspielräume sollten genutzt werden.

Kontinuierliches Lernen: Ein System zur Erfassung und Umsetzung von Erfahrungen ist unerlässlich.

Risikominimierung: Reputations- und rechtliche Risiken können durch transparente Kommunikation, enge Abstimmung mit Aufsichtsbehörden und eine restriktive Rechtsauslegung minimiert werden.

Rechtliche Herausforderungen und Lösungsansätze:

Haftung und Verantwortung: Nach Art. 57 Abs. 12 KI-VO bleiben KI-System-Anbieter nach geltendem Haftungsrecht für Schäden an Dritten haftbar. Gleichzeitig sollen keine Geldbußen verhängt werden, wenn Anbieter der Anleitung der zuständigen Behörde folgen. Diese Herausforderung sollten die Behörden adressieren und berücksichtigen, indem sie den Anbietern entsprechende Informationen und Hinweise geben. Es sollte klar zwischen zivilrechtlicher Haftung und behördlichen Geldbußen unterschieden werden. Um diesen Herausforderungen zu begegnen könnten Versicherungsmodelle für Reallabor-Teilnehmer entwickelt, Haftungsfragen vertraglich geregelt und im Vorfeld eine ausführliche Risikoanalyse durchgeführt werden.

Datenschutz: KI-Projekte sind häufig von internationalen Daten abhängig. Datenschutzrechtliche Regelungen zum Datenaustausch und der Verwendung diverser Anwendungen sind dabei zu beachten. Die Einhaltung der Regelungen der DSGVO durch Privacy Engineering (datenschutzfreundliche Systemgestaltung) und Nutzung von Federated Learning Approaches (verteiltes Training ohne/mit möglichst geringem Datentransfer) ist ein Ansatz mit dem den Herausforderungen begegnet werden kann. Behörden sollten dementsprechend sicherstellen, dass entsprechende Vereinbarungen durch die Reallabor-Nutzer untereinander getroffen wurden.

Regulierungskonflikte: Es kann zwischen bestehenden und sektorspezifischen Vorschriften, bspw. aus dem Medizin- oder Finanzbereich, und den Vorgaben der KI-VO zu Konflikten kommen. Eine enge behördenübergreifende Koordination, Entwicklung von harmonisierten Auslegungsrichtlinien, um Widersprüche auflösen zu können; Einrichtung einer zentralen Anlaufstelle für regulatorische Anfragen (One-Stop-Shop) wird als Lösungsweg empfohlen.

3 Empfehlungen zur Umsetzung von Reallaboren

Die Empfehlungen basieren sowohl auf einer systematischen Literaturrecherche zu regulatorischen Grundlagen und bestehenden Reallaboren als auch auf eigenen praktischen Erfahrungen beim Aufbau des KI-Reallabors ROUTINE[3] (Reallabor zum Transfer digitaler Gesundheitsanwendungen und KI ins Gesundheitswesen).[4] Daraus ergeben sich für uns folgende essenzielle Punkte für die Einrichtung von KI-Reallaboren speziell im Bereich Gesundheit aber auch generell für die Bereiche Mobilität und Finanzdienstleistung:

- Vor dem Beginn eines KI-Reallabors müssen **Machbarkeit, Nachfrage, mögliche Ergebnisse und Nebenwirkungen eingehend und nachhaltig identifiziert und bewertet** werden. KI-Reallabore können nur erfolgreich sein, wenn sie mit den erforderlichen finanziellen Mitteln und personellen Ressourcen ausgestattet werden. Daher ist es wichtig, dass potenzielle Aufsichtsbehörden von KI-Reallaboren über diese Parameter informiert sind, damit sie den Reallaboren entsprechend ausreichende Mittel zur Verfügung stellen können. Andernfalls könnte dies zu einem Misserfolg führen. In der Vergangenheit sind Reallabore, bei denen diese Anforderungen nicht oder nur ungenügend vor dem Start identifiziert und bewertet wurden, oft gescheitert.[5]
- Ebenfalls von höchster Priorität ist, dass die Behörde, die an den KI-Reallaboren teilnimmt bzw. diese beaufsichtigt, über die **nötige Expertise** verfügt, um die verschiedenen anzuwendenden Verordnungen zu durchdringen und technische Lösungen abzuleiten.[6] Die Teilnehmenden am Reallabor sowie die Stakeholder werden im Verlauf des Reallabors immer wieder mit ungeklärten Fragen zu rechtlichen oder Governance-Themen auf die Behörden zugehen. Es ist von erheblichem Vorteil, wenn sich die leitende bzw. beaufsichtigende Behörde die jüngste Vergangenheit der Reallabore ansieht, insbesondere in der FinTech-Branche des Vereinigten Königreichs. Dabei können Berichte der Financial Conduct Authority sowie der UNSGSA zu Reallaboren herangezogen werden. Dort gibt es bereits „Lessons Learned" über die Einrichtung von Reallaboren. Auch wenn Reallabore noch in den „Kinderschuhen" stecken – das gilt insbesondere in Deutschland – gibt es bereits erste Hinweise darauf, wie sie gewinnbringend und erfolgreich aufgebaut und durchgeführt werden können.[7]
- **Eine starke Kommunikation zwischen den Regulierungs- und Aufsichtsbehörden** sollte angestrebt werden. Nur so kann sichergestellt werden, dass die in den Reallaboren gewonnenen Erkenntnisse nicht wirkungslos bleiben, sondern in den regulatorischen Rahmen und die praktische Umsetzung einfließen. Insbesondere müssen die Datenschutzbehörden, wie in Art. 57 Abs. 10 KI-VO vorgesehen, an den Reallaboren teilnehmen. Es ist davon auszugehen, dass in den Reallaboren eine große Menge an (sensiblen) Daten verarbeitet wird. Ebenso ist mit dem Bedarf und der Notwendigkeit einer

[3] https://ki-reallabor-bw.de .
[4] Die tiefergehende Analyse ist Teil einer noch unveröffentlichten Ausarbeitung und dient dem rechtswissenschaftlichen Diskurs.
[5] Early Lessons on Regulatory Innovations to Enable Inclusive FinTech - S. 31, UNSGSA; Regulating Fintech in the EU: the Case for a Guided Sandbox - RINGE, RUOF, S. 618; "Thinking Outside the Box?", S. 11, RUSCHEMEIER
[6] („Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders", S. 138 Kap. 4.2 – BRINKER.
[7] "The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation", S. 15, GOO, HEO, zumindest konnte dies für den Zusammenhang zwischen Regulatory Sandboxes und Innovation in der FinTech-Branche beobachtet werden.

Weiterverarbeitung personenbezogener Daten in den Reallaboren zu rechnen. Hier steht insbesondere Art. 59 Abs. 1 KI-VO, sowie dessen Verhältnis zur DSGVO im Fokus.[8] Daher ist eine feste Betreuung durch die Datenschutzbehörden von besonderem Vorteil.

- Aufsichtsbehörden sollten insbesondere folgende Punkte im Blick behalten: Unzureichenden Verbraucherschutz, Verwässerung von Vorschriften, übermäßig großzügige Ausnahmeregelungen und Ungleichbehandlung von (potenziellen) Teilnehmenden.[9] Diese Punkte waren in den vergangenen Jahren häufig Kritikpunkte an den Reallaboren. Zwar werden insbesondere Transparenz und Nichtdiskriminierung in Art. 58 Abs. 2 lit. a) KI-VO erwähnt. Wie dies genau zu bewerkstelligen ist, muss jedoch noch durch die Kommission in Durchführungsrechtsakten gemäß Art. 58 Abs. 1 KI-VO festgelegt werden.

Aus unserer Sicht empfiehlt sich ein dreistufiges Verfahren für den Aufbau und die Durchführung eines Reallabors nach der KI-VO:

- **Aufbau des Reallabors**: Machbarkeit, Nachfrage, mögliche Ergebnisse und Nebenwirkungen eines KI-Reallabors werden nachhaltig identifiziert und bewertet; potenzielle Teilnehmende und Stakeholder und Endnutzer werden ermittelt und eingeladen, Fachexperten für Technik, BWL und zur rechtlichen Beratung werden identifiziert und stehen in einem Advisory Board dem Reallabor zur Verfügung.
- **Durchführung des Reallabors**: Die identifizierte Problemstellung wird durch die Teilnehmenden erarbeitet, die Behörde steht für rechtliche Fragen als "Sparring-Partner" zur Verfügung, Risiko für Rechte und Freiheiten von EU-Bürger*innen werden gemonitort, eine fortlaufende Risikobewertung durch die Behörde findet statt, Absprache mit Regulierungsbehörden, um bereits gelerntes weiter zu kommunizieren.
- **Abschluss & Lessons Learned**: Zum Ende des Reallabors ist es essenziell, dass der Prozess reflektiert wird, damit anschließende Reallabore von positiven wie auch negativen Entwicklungen profitieren.

Für die Etablierung von KI-Reallaboren sind konkret folgende Punkte notwendig:

- Der Einsatz von Reallaboren könnte die Produktentwicklung fördern. Dazu muss die **Zuständigkeit** der nationalen und regionalen Aufsichtsbehörden in Deutschland gemäß der EU-KI-Verordnung **geklärt und festgelegt** werden.

- Es wird empfohlen, ein KI-Reallabor als regionalen Modellversuch auch auf Landesebene zu etablieren und damit einen Bottom-up-Ansatz zu verfolgen, statt auf eine bundesweite Initiative zu warten. Die Landesbeauftragten für den Datenschutz und die

[8] BOTTA in Martini/Wendehorst, Kommentar zur KI-VO, Art. 58 Rn. 5 ff.
[9] "Thinking Outside the Box?", S. 11, RUSCHEMEIER.

Informationsfreiheit (LfDI) sollten dabei als regionale Aufsichtsbehörde benannt werden. Auch weitere Aufsichtsbehörden (Marktüberwachung) sollten hinzugezogen werden.

Detaillierte Empfehlungen zum Betrieb und der Durchführung von Reallaboren für Behörden sind in den folgenden Abschnitten dargestellt.

Von bereits bestehenden Erfahrungen im Umgang mit Reallaboren, insbesondere im Energiebereich, FinTech Gesundheit und Mobilität sollte unbedingt gelernt und die unterschiedlichen Bedürfnisse der jeweiligen Sektoren beachtet werden. Es gibt bereits Erfahrungsberichte und Literatur im Umgang mit Reallaboren, die dazu beitragen können, Hürden für die Behörden zu verringern.

Des Weiteren wird empfohlen, dass Behörden prüfen, inwiefern nicht bereits der Betrieb von KI-Reallaboren im Sinne der KI-VO aus ihrem Aufgabenbereich sich herleiten lassen könnte und der Betrieb beispielsweise zum Erkenntnisgewinn zur Umsetzung von KI-Reallaboren möglich wäre.[10]

[10] Angelehnt an das laufende Projekt der Bundesnetzagentur mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2025/09-KI-Reallabor.html .

4 Was wir uns von einer Behörde im Kontext der KI-VO wünschen

Für die erfolgreiche Etablierung und Durchführung von KI-Reallaboren ist die aktive Rolle der zuständigen Behörden entscheidend. Reallabore können nur dann ihre Funktion als Innovationsmotor erfüllen, wenn Behörden nicht ausschließlich als Kontrollinstanz auftreten, sondern zugleich eine gestaltende und unterstützende Rolle einnehmen. Als Forschungstransfereinrichtung, die selbst ein KI-Reallabor betreiben möchte, und auf Grundlage unserer praktischen Erfahrungen aus dem Reallabor ROUTINE (vgl. Executive Summary[11]), wünschen wir uns daher insbesondere folgende Punkte:

- **Klare Zuständigkeiten und Ansprechpartner:** Es bedarf einer eindeutigen Benennung, welche Behörde für KI-Reallabore verantwortlich ist, und der Einrichtung von festen Kontaktstellen. Nur so können Fragen im laufenden Betrieb zügig geklärt und Unsicherheiten vermieden werden.
- **Begleitende Beratung statt reiner Kontrolle**: Behörden sollten Reallabore nicht nur beaufsichtigen, sondern als beratende Partner agieren. Eine enge Zusammenarbeit ermöglicht es, gemeinsam kreative und rechtskonforme Lösungen zu entwickeln.
- **Rechtssicherheit und Orientierung**: Reallabore benötigen verlässliche Rahmenbedingungen. Dazu gehören Leitlinien, Interpretationshilfen und klare Orientierung zur Anwendung der KI-VO, auch im Zusammenspiel mit anderen relevanten Rechtsakten wie der DSGVO oder dem Data Governance Act.
- **Flexibilität und Innovationsfreundlichkeit**: Behörden sollten vorhandene regulatorische Spielräume nutzen, um Innovationen nicht unnötig zu behindern. Reallabore sind auf ein innovationsfreundliches Umfeld angewiesen, das neue Ansätze testbar macht.
- **Effiziente Prozesse und kurze Reaktionszeiten:** Verfahren und Rückmeldungen müssen so ausgestaltet sein, dass sie den Innovationszyklen von Reallaboren entsprechen. Lange Bearbeitungszeiten gefährden die Funktionsfähigkeit und Glaubwürdigkeit von Reallaboren.
- **Systematische Nutzung der Ergebnisse von Reallaboren:** Erkenntnisse aus Reallaboren sollten von den Behörden strukturiert aufgenommen und in die Weiterentwicklung von Regulierung und Aufsicht einbezogen werden. Dies stärkt die lernende Dimension von Reallaboren und vermeidet, dass gewonnene Erfahrungen ungenutzt bleiben.

[11] https://ki-reallabor-bw.de/blog/

5 Detaillierte Analyseergebnisse

5.1 Rechtsgrundlage und Anwendungsbereich

Rechtsgrundlage: Art. 57-61 der Verordnung (EU) 2024/1689 (KI-Verordnung)

Zentrale Verpflichtung: Nach Art. 57 Abs. 1 S. 1 KI-VO sorgen die Mitgliedstaaten dafür, dass ihre zuständigen Behörden mindestens ein KI-Reallabor auf nationaler Ebene einrichten, das bis zum 2. August 2026 einsatzbereit sein muss.

Definition KI-Reallabor: Die KI-Reallabore bieten eine kontrollierte Umgebung, um Innovation zu fördern und die Entwicklung, das Training, das Testen und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem bestimmten zwischen den Anbietern oder zukünftigen Anbietern und der zuständigen Behörde vereinbarten Reallabor-Plan zu erleichtern.

Nach Art. 57 Abs. 9 KI-VO sollen KI-Reallabore zu folgenden Zielen beitragen:

- **Rechtskonformität:** Verbesserung der Rechtskonformität für die Einhaltung der Regulierungsvorschriften
- **Best Practice-Austausch:** Förderung des Austauschs bewährter Verfahren
- **Innovation:** Förderung von Innovation und Wettbewerbsfähigkeit
- **Regulatorisches Lernen:** Beitrag zum evidenzbasierten regulatorischen Lernen
- **Marktzugang:** Erleichterung des Zugangs zum EU-Binnenmarkt, insbesondere für KMU

5.2 Systematische Einrichtung und Organisation von KI-Reallaboren

5.2.1 Institutionelle Grundvoraussetzungen

5.2.1.1 Organisatorische Struktur

- **Zuständige Behörde:** Bestimmung der federführenden nationalen Behörde mit ausreichenden Mitteln (Art. 57 Abs. 4 KI-VO)
- **Interinstitutionelle Kooperation:** Zusammenarbeit mit anderen einschlägigen Behörden und Einbeziehung anderer Akteure des KI-Ökosystems
- **Datenschutzbehörden:** Einbeziehung der nationalen Datenschutzbehörden in den Betrieb des KI-Reallabors

5.2.1.2 Personelle Ausstattung

- **Multidisziplinäre Expertise:** Fachexperten für technische, betriebswirtschaftliche und rechtliche Aspekte
- **Domänenspezialisten:** Je nach Ausrichtung des Reallabors (Gesundheit, Mobilität, Fintech etc.)
- **Regulierungsexperten:** Personen mit Erfahrung in regulatorischen Sandboxes

5.2.2 Infrastrukturelle Voraussetzungen

5.2.2.1 Technische Infrastruktur

- **Sichere Testumgebung:** Kontrollierte Umgebung für KI-System-Tests
- **Dateninfrastruktur:** Zugang zu echten oder synthetisierten Datensätzen
- **Monitoring-Systeme:** Kontinuierliche Überwachung von Risiken und Leistung

5.2.2.2 Rechtliche Infrastruktur

- **Vertragliche Grundlagen:** Standardisierte Reallabor-Pläne und Vereinbarungen
- **Compliance-Framework:** Systeme zur Überwachung der Rechtseinhaltung
- **Datenschutz-Tools:** DSGVO-konforme Verarbeitungsverfahren

5.3 Kernvoraussetzungen für funktionsfähige KI-Reallabore

5.3.1 Datenschutz und Datensicherheit bei der Integration

5.3.1.1 Rechtliche Grundlagen

- **DSGVO-Compliance:** Sicherstellung der Einhaltung der Datenschutz-Grundverordnung
- **Art. 59 KI-VO:** Weiterverarbeitung personenbezogener Daten für KI-Systeme im öffentlichen Interesse
- **Rechtsgrundlagen:** Prüfung der Rechtsgrundlagen nach Art. 6 DSGVO

5.3.1.2 Praktische Umsetzung

Technische Maßnahmen:

- Verschlüsselung personenbezogener Daten
- Pseudonymisierung und Anonymisierung wo möglich
- Access Controls und rollenbasierte Zugriffsbeschränkungen
- Audit-Logs und Nachverfolgbarkeit

Organisatorische Maßnahmen:

- Datenschutz-Folgenabschätzung (DSFA) vor Projektbeginn
- Auftragsverarbeitungsverträge mit Teilnehmern
- Schulung aller Beteiligten zu Datenschutzanforderungen
- Regelmäßige Compliance-Audits

5.3.2 Kommunikation mit Regulierungs- und Aufsichtsbehörden

5.3.2.1 Strukturierter Austausch

Interne Koordination:

- Koordination der Tätigkeiten und Zusammenarbeit im Rahmen des KI-Gremiums
- Regelmäßige Abstimmung mit Marktüberwachungsbehörden
- Einbeziehung sektorspezifischer Aufsichtsbehörden (BaFin, Bundeskartellamt etc.)

Externe Berichterstattung:

- Jährliche Berichte an das Büro für Künstliche Intelligenz[12] und das KI-Gremium
- Abschlussberichte für einzelne Projekte
- Öffentliche Bereitstellung von Berichten oder Zusammenfassungen

5.3.2.2 Feedback-Loop zur Gesetzgebung

- Systematische Sammlung und Aufbereitung von Lessons Learned
- Empfehlungen für Rechtsanpassungen
- Input für delegierte Rechtsakte und Durchführungsverordnungen

5.3.3 Einbeziehung echter Stakeholder

5.3.3.1 Stakeholder-Kategorien

Primäre Stakeholder:

- KI-Entwickler und -Anbieter (insbesondere KMU und Start-ups)
- Endnutzer der KI-Systeme
- Betroffene Personen (bei personenbezogenen Daten)

Sekundäre Stakeholder:

- Branchenverbände und Kammern
- Verbraucherschutzorganisationen
- Wissenschaftliche Einrichtungen
- Zivilgesellschaftliche Organisationen

5.3.3.2 Partizipationsverfahren

Strukturierte Einbindung:

[12] Europäisches AI Office in Brüssel.

- Stakeholder-Beiräte für strategische Ausrichtung
- Regelmäßige Konsultationsverfahren
- User Journey Mapping mit Endnutzern
- Co-Design-Ansätze bei der Entwicklung

Transparenz und Kommunikation:

- Öffentliche Informationsveranstaltungen
- Regelmäßige Updates über Fortschritte
- Feedback-Mechanismen für kontinuierliche Verbesserung

5.3.4 Datenanforderungen: Echte oder synthetische Daten

5.3.4.1 Datenqualität und -authentizität

Echte Daten:

- Zugang zu realen Datensätzen unter strikten Datenschutzauflagen
- Repräsentativität der Daten für den Anwendungsbereich
- Qualitätssicherung und Datenvalidierung

Synthetische Daten:

- Einsatz fortgeschrittener Syntheseverfahren (GANs, VAEs)
- Validierung der statistischen Eigenschaften
- Sicherstellung der Realitätsnähe für Testzwecke

5.3.4.2 Datenzugang und -bereitstellung

- Zentrale Datenplattformen für Reallabor-Teilnehmer
- Standardisierte APIs und Datenformate
- Versionierung und Dokumentation der Datensätze

5.3.5 3.5 Kontinuierliches Risikomanagement

5.3.5.1 Risikobewertungsframework

Systematische Risikoidentifikation:

- Risikokategorien: Grundrechte, Gesundheit, Sicherheit, Diskriminierung
- Risikobewertungsmatrix nach Eintrittswahrscheinlichkeit und Schadenshöhe
- Dynamische Anpassung bei Projektfortschritt

Monitoring-Indikatoren:

- Technische KPIs (Accuracy, Bias, Robustheit)

- Rechtliche Compliance-Metriken
- Gesellschaftliche Impact-Indikatoren

5.3.5.2 Risikominderungsmaßnahmen

Präventive Maßnahmen:

- Ex-ante-Risikoanalyse vor Projektstart
- Risikobasierte Auswahl von Teilnehmern
- Implementierung von Safeguards

Reaktive Maßnahmen:

- Befugnis zur vorübergehenden oder dauerhaften Aussetzung des Testverfahrens
- Eskalationsverfahren bei kritischen Risiken
- Notfallpläne für Schadensbegrenzung

5.4 Domänenspezifische Ausgestaltung von KI-Reallaboren

5.4.1 4.1 Systematische Domänenanalyse

5.4.1.1 Stakeholder-Mapping

Sektor Gesundheit:

- Regulatoren: EMA, Paul-Ehrlich-Institut, Landesbehörden
- Akteure: Krankenhäuser, Praxen, Pharmaunternehmen, Medizintechnik
- Endnutzer: Patienten, Ärzte, Pflegepersonal

Sektor Mobilität:

- Regulatoren: KBA, Verkehrsministerien, Straßenverkehrsbehörden
- Akteure: Automobilhersteller, Zulieferer, ÖPNV-Betreiber
- Endnutzer: Fahrzeugführer, Fahrgäste, Verkehrsteilnehmer

Sektor Finanzdienstleistungen:

- Regulatoren: BaFin, Bundesbank, EZB
- Akteure: Banken, Versicherungen, FinTechs, PaymentAnbieter
- Endnutzer: Verbraucher, Unternehmen, Investoren

5.4.1.2 Bedarfsanalyse und Zieldefinition

SMART-Zielsetzung:

- **Specific:** Konkrete KI-Anwendungsfälle definieren
- **Measurable:** Messbare Erfolgskriterien festlegen
- **Achievable:** Realistische Ziele im regulatorischen Rahmen
- **Relevant:** Relevanz für gesellschaftliche Herausforderungen
- **Time-bound:** Zeitgebundene Meilensteine

5.4.2 Sektorspezifische Besonderheiten

5.4.2.1 Regulatorische Rahmenbedingungen

Gesundheitsbereich:

- Medizinprodukterecht (MDR)
- Arzneimittelrecht (AMG)
- Haftungsrecht für medizinische KI

Finanzbereich:

- Bankenaufsichtsrecht
- Versicherungsaufsichtsrecht
- Geldwäscheprävention
- DORA (Digital Operational Resilience Act)

5.4.2.2 Gesetzliche Ausnahmen und Flexibilitäten

- **Experimentierklauseln:** Identifikation bestehender Experimentierklauseln
- **Ausnahmegenehmigungen:** Möglichkeiten temporärer Rechtsabweichungen
- **Proportionalitätsprinzip:** Ermessensspielraum bei der Anwendung der Rechtsvorschriften

5.5 Projektmanagement in KI-Reallaboren

5.5.1 Projektkonstruktion und Governance

5.5.1.1 Konkrete Projektpläne

Reallabor-Plan nach Art. 57 Abs. 5 KI-VO:

- Gegenstand und Dauer der Testphase
- Art und Zweck der KI-System-Entwicklung
- Kategorien betroffener Personen
- Technische und organisatorische Schutzmaßnahmen
- Risikominderungsstrategien

5.5.1.2 Verantwortlichkeitsverteilung

Rollenmatrix:

- **Behördliche Projektleitung:** Gesamtverantwortung und Aufsicht
- **Fachliche Projektleitung:** Technische und fachliche Koordination
- **Compliance Officer:** Rechts- und Regelkonformität
- **Stakeholder Manager:** Kommunikation und Partizipation
- **Data Protection Officer:** Datenschutz und Privacy

5.5.1.3 Vertragliche Vereinbarungen

Standardisierte Vertragswerke:

- Teilnahmeverträge mit klaren Rechten und Pflichten
- Service Level Agreements für technische Infrastruktur
- Datenschutzvereinbarungen und Auftragsverarbeitungsverträge, Joint-Controllership-Agreements
- Geheimhaltungsvereinbarungen und IP-Regelungen

5.5.2 5.2 Berichtswesen und Monitoring

5.5.2.1 Strukturiertes Reporting

Interne Berichterstattung:

- Monatliche Statusberichte an Behördenleitung
- Quartalsweise Risiko- und Compliance-Reports
- Ad-hoc-Berichte bei kritischen Ereignissen

Externe Berichterstattung:

- Schriftlicher Nachweis für erfolgreich durchgeführte Tätigkeiten
- Abschlussbericht mit detaillierter Darlegung der Tätigkeiten und Erkenntnisse
- Öffentliche Transparenzberichte (anonymisiert)

5.5.2.2 Einbezug der Aufsichtsbehörden

Strukturierter Dialog:

- Regelmäßige Round Tables mit relevanten Aufsichtsbehörden
- Gemeinsame Arbeitsgruppen zu spezifischen Themen
- Peer Learning zwischen verschiedenen Reallaboren

Austausch mit Entwicklern:

- Leitfäden zu regulatorischen Erwartungen und Anforderungen
- Technische Workshops und Schulungen
- Feedback-Schleifen zu praktischen Umsetzungsfragen

5.6 Drei-Phasen-Modell für KI-Reallabor-Projekte

5.6.1 Phase I: Aufbau und Vorbereitung

5.6.1.1 Infrastruktur-Setup (Monate 1-3)

Technische Infrastruktur:

- Einrichtung der Testumgebung
- Implementierung von Monitoring-Tools
- Datenschutz- und Sicherheitsmaßnahmen

Organisatorische Vorbereitung:

- Team-Aufbau und Rollendefinition
- Stakeholder-Identifikation und -Ansprache
- Entwicklung von Standards und Prozessen

5.6.1.2 Rechtliche Grundlagenarbeit

Regulatorische Klärung:

- Mapping anwendbarer Rechtsvorschriften
- Identifikation von Ausnahmen und rechtlicher Flexibilität
- Entwicklung von Compliance-Checklisten

Vertragliche Vorbereitung:

- Erstellung standardisierter Vertragsvorlagen
- Klärung von Haftungs- und Verantwortungsfragen
- IP-rechtliche Vereinbarungen

5.6.2 Phase II: Durchführung und Betrieb

5.6.2.1 Kontinuierliche Begleitung

Projektmonitoring:

- Wöchentliche Statusmeetings mit Teilnehmern
- Kontinuierliche Risikoüberwachung
- Technische Performance-Überwachung

Adaptive Steuerung:

- Flexible Anpassung an neue Erkenntnisse
- Skalierung erfolgreicher Ansätze
- Frühzeitige Intervention bei Problemen

5.6.2.2 Lernen und Anpassung

Iterative Verbesserung:

- Regular Reviews und Retrospektiven
- Anpassung von Prozessen und Standards
- Wissenstransfer zwischen Projekten

5.6.3 Phase III: Evaluation und Lessons Learned

5.6.3.1 Systematische Auswertung

Quantitative Evaluation:

- KPI-basierte Erfolgsmessung
- Statistische Auswertung der Projektergebnisse
- Kosten-Nutzen-Analyse

Qualitative Evaluation:

- Stakeholder-Interviews und -Befragungen
- Fallstudien-Entwicklung
- Best Practice-Identifikation

5.6.3.2 Wissenstransfer und Skalierung

Konkretisierungen für Aufsichtsbehörden:

- Praxisleitfäden für regulatorische Anwendung
- Empfehlungen für Rechts- und Verordnungsanpassungen
- Standards für ähnliche Reallabore

Öffentlichkeitsarbeit:

- Publikation von Lessons Learned
- Fachkonferenzen und Workshops
- Peer-to-Peer-Austausch mit anderen Behörden

5.7 Lernen von bestehenden Reallabor-Implementierungen

5.7.1 Erfahrungen aus anderen Sektoren

5.7.1.1 Energiesektor - Regulatory Sandbox

Erfolgreiche Ansätze:

- Klare Zielsetzung und begrenzte Laufzeit
- Enge Kooperation zwischen Regulierer und Marktteilnehmern
- Iterative Anpassung der Regulierung basierend auf Erfahrungen

Übertragbare Lessons Learned:

- Bedeutung klarer Exit-Strategien
- Notwendigkeit kontinuierlicher Stakeholder-Kommunikation
- Wert von Cross-Sector Learning

5.7.1.2 FinTech-Sandboxes

BaFin Digital Lab und andere Ansätze:

- Strukturierte Beratungsangebote für innovative Unternehmen
- Enge Verzahnung mit bestehenden Aufsichtsprozessen
- Fokus auf Verbraucherschutz und Marktintegrität

Anwendbare Prinzipien für KI-Reallabore:

- Proportionaler Ansatz basierend auf Risikobewertung
- Klare Kommunikation regulatorischer Erwartungen
- Integration in bestehende Aufsichtsstrukturen

5.7.1.3 Gesundheitswesen - Medical Device Innovation

Medizinprodukte-Pilotprojekte:

- Strikte Sicherheits- und Wirksamkeitsanforderungen
- Phasenweise Erprobung mit steigender Komplexität
- Enge Zusammenarbeit mit klinischen Partnern

Übertragung auf KI-Reallabore:

- Mehrstufige Testverfahren
- Klinische und ethische Expertise einbinden
- Patientensicherheit als oberste Priorität

5.7.1.4 Mobilitätssektor - Autonomous Vehicle Testing

Connected and Automated Mobility:

- Geographisch begrenzte Testfelder
- Stufenweise Erhöhung der Autonomie-Level
- Intensive Datenerfassung und -analyse

Relevante Aspekte:

- Bedeutung realistischer Testbedingungen
- Notwendigkeit umfassender Datenerfassung
- Wichtigkeit öffentlicher Akzeptanz

5.7.2 Sektorspezifische Unterschiede und Anpassungsbedarfe

5.7.2.1 Regulierungsunterschiede

Risikobasierte Ansätze:

- **Gesundheit:** Höchste Sicherheitsanforderungen, extensive klinische Prüfungen
- **Finanzdienstleistungen:** Fokus auf Systemstabilität und Verbraucherschutz
- **Energie:** Versorgungssicherheit und Netzstabilität im Vordergrund
- **Mobilität:** Verkehrssicherheit und Haftungsfragen zentral

5.7.2.2 Bedarfsunterschiede

Technologische Anforderungen:

- **KI-spezifisch:** Algorithmische Transparenz, Bias-Vermeidung, Erklärbarkeit
- **Datenintensität:** Höhere Anforderungen an Datenschutz und -sicherheit
- **Lernende Systeme:** Dynamische Regulierung für adaptive Systeme

Gesellschaftliche Akzeptanz:

- Höhere Sensibilität bei KI-Systemen in kritischen Bereichen
- Notwendigkeit transparenter Kommunikation über KI-Risiken
- Einbeziehung ethischer Überlegungen in Designprozesse

6 Zitierte bzw. weiterführende Literatur

https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/early-lessons-on-regulatory-innovation-to-enable-inclusive-fintech/ - Early Lessons on Regulatory Innovations to Enable Inclusive FinTech – UNSGSA.

https://www.fca.org.uk/publications/research/regulatory-sandbox-lessons-learned-report - Regulatory sandbox lessons learned report - Financial Conduct Authority, UK.

Regulatory sandbox toolkit (EN) - A Comprehensive Guide for Regulators to Establish and Manage Regulatory Sandboxes Effectively – OECD.

https://www.sciencedirect.com/science/article/pii/S2199853122004383?via%3Dihub - The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation - Jayoung James Goo, Joo-Yeun Heo.

https://www.cambridge.org/core/services/aop-cambridge-core/content/view/3EE71CEEB3BC22E57A1BF08023073A6F/S1867299X20000082a.pdf/regulating-fintech-in-the-eu-the-case-for-a-guided-sandbox.pdf - Regulating Fintech in the EU: the Case for a Guided Sandbox - Wolf-Georg RINGE and Christopher RUOF.

https://2024-isola.isola-conference.org/wp-content/uploads/2024/11/141290313-paper.pdf - Thinking Outside the Box? Regulatory Sandboxes as a Tool for AI Regulation - Hannah Ruschemeier.

https://iris.imtlucca.it/handle/20.500.11771/34339 - Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders - F. Bagni, F. Seferi, N. Brinker.

Martini, Mario (Hrsg.) / Wendehorst, Christiane (Hrsg.), KI-VO: Verordnung über Künstliche Intelligenz, Kommentar, 1. Auflage, München, C.H.Beck, 2024.

Quelle Grafik Titelseite: erstellt mit ChatGPT.