JOANNEUM RESEARCH POLICIES
Institut für Wirtschafts- und Innovationsforschung

Regulatory Sandboxes für KI in Österreich

Endbericht

Auftraggeber: Wirtschaftskammer Österreich

JOANNEUM RESEARCH Forschungsgesellschaft mbH
Zentrum für Wirtschafts- und Innovationsforschung

Büro Graz
Leonhardstraße 59
8010 Graz, Austria
Tel.: +43-316-876 1488
E-Mail: policies@joanneum.at

Büro Wien
Haus der Forschung, Sensengasse 1
1090 Wien, Austria
Tel.: +43-1-581 7520
E-Mail: policies@joanneum.at

David Walker, Christian Hartmann, Marlies Schütz

Wien, Februar 2026

THE INNOVATION COMPANY

Inhaltsverzeichnis

1 Executive Summary

„**Regulatory Sandbox**“ (kurz: Sandbox) bezeichnet ein von **staatlichen Stellen autorisiertes Testumfeld**, in dem ausgewählte Unternehmen neue Produkte oder Dienstleistungen unter realen Marktbedingungen austesten können – bei **gleichzeitiger temporärer Anpassung oder Flexibilisierung regulatorischer Anforderungen**. Im Zentrum steht nicht die technologische Innovation selbst, sondern deren Interaktion mit normativen Vorgaben wie Finanzmarktregeln, Datenschutz oder Produktsicherheit. In der internationalen Praxis kristallisieren sich **drei zentrale Zielkategorien** heraus: **Technologieerprobung**, **Politiklernen** und **Normweiterentwicklung**. Ihren Wert entfalten Sandboxes dann, wenn ihre Ergebnisse über den konkreten Testfall hinauswirken. Der entscheidende Schritt liegt in der Überführung erfolgreicher Experimente in den regulären Rechts- und Verwaltungsrahmen. Es lassen sich **zwei Grundtypen** unterscheiden: (1) Sandboxes mit temporären Regulierungsausnahmen und (2) innovationsbezogene Beobachtungsräume ohne rechtliche Abweichung vom Status quo.

Sandboxes sind in **Österreich kein neues Konzept**, sondern ein sich entwickelndes Instrument mit bereits sichtbaren institutionellen Bezugspunkten. Um ihr Potenzial vollständig zu entfalten, braucht es **koordinierte Strukturen**, verlässliche Zuständigkeiten und **sektorübergreifende Rahmenbedingungen**. Die institutionelle Ausgangslage ist differenziert, aber prinzipiell anschlussfähig – und bildet eine belastbare Grundlage für weiterführende Pilotierung und strategische Verankerung. Erfolgreiche Initiativen verfügten über klare Steuerungsstrukturen, multidisziplinäre Konsortien und transparente Zieldefinitionen. Wichtig ist die Rolle der **Forschungsförderung als Ermöglichungsstruktur**. Die Unterstützung durch FFG, Klima- und Energiefonds oder aws hat sich als wichtiger Hebel erwiesen, um experimentelle Vorhaben überhaupt initiieren zu können.

Die **rechtliche Kodifikation von KI-Sandboxes** erfolgt durch die **Europäische KI-Verordnung** (KI-VO) (Art. 57 bis 62), die zukünftig **ergänzt um EU-Durchführungsrechtsakte** einen risikobasierten und sektorenübergreifenden Rahmen für KI-Anwendungen schafft. Im Fokus stehen Hochrisiko-KI-Systeme; verbotene Anwendungen (z. B. Social Scoring, manipulative Verhaltensbeeinflussung oder biometrische Massenüberwachung) sind explizit ausgeschlossen. Die **KI-VO** lässt **keine inhaltliche Ausnahme** von ihren Anforderungen innerhalb der Sandbox zu, diese sind nur als Unterstützung bei der Umsetzung und Konformitätsprüfung vorgesehen. Sie ermöglichen etwa eine **begleitete Testphase**, bieten aber **keinen Freiraum zur Abweichung von materiellen Anforderungen**. Damit sind sie formal eher als unterstützendes Prüf- und Dialoginstrument angelegt, nicht als normative Ausnahmeregelung im engeren Sinne.

Zugleich gilt es, **bestehende institutionelle Strukturen und Infrastrukturen gezielt zu nutzen**. Synergien mit bestehenden europäischen Infrastrukturen wie (European) Digital Innovation Hubs, Testing and Experimentation Facilities (TEFs) oder sektoralen EU-Projekten müssen angestrebt werden. Die **Governance** von KI-Sandboxes muss sich an Prinzipien der Praktikabilität, Effizienz und Zugänglichkeit orientieren. Nur so kann das Instrument selbst innovationsfreundlich wirken – nicht nur technisch, sondern auch institutionell. Vor diesem Hintergrund erscheint es zielführend, die WKO als institutionelle Vertreterin der Unternehmen systematisch in die Ausgestaltung, Steuerung und begleitende Bewertung zukünftiger Sandbox-Modelle einzubinden. KI Regulatory Sandboxes benötigen eine **leistungsfähige**

Infrastruktur für die technologische Umsetzung sowie die rechtliche Begleitung, die Evaluierung und den Zugang zu Testressourcen.

2 Einleitung

Die rasante Entwicklung von Künstlicher Intelligenz (KI) stellt regulatorische Systeme weltweit vor neue Herausforderungen. Während KI-basierte Technologien enorme Innovations- und Wertschöpfungspotenziale bieten, werfen sie zugleich grundlegende rechtliche und sozio-technologische Fragen auf. Regulierungsbehörden, Unternehmen und gesellschaftliche Akteure stehen vor der Aufgabe, innovationsfreundliche Rahmenbedingungen zu schaffen, ohne zentrale ethische und rechtliche Standards zu unterlaufen.

Ein möglicher Lösungsansatz sind sogenannte **Regulatory Sandboxes**[1] – kontrollierte Umgebungen, in denen KI-Systeme entwickelt, getestet und validiert werden können, bevor sie auf den Markt gebracht werden. Ziel ist es, Innovationen zu fördern und gleichzeitig Risiken zu erkennen und abzumildern, beispielsweise in Bezug auf Grundrechte, Gesundheit und Sicherheit.

Mit der **Europäischen KI-Verordnung** wird dieser Ansatz auf europäischer Ebene institutionalisiert: Alle Mitgliedstaaten werden verpflichtet, nationale KI Regulatory Sandboxes einzurichten, um die Entwicklung und Erprobung vertrauenswürdiger KI-Anwendungen insbesondere für Start-ups und Klein- und Mittelunternehmen (KMU) zu erleichtern. Für Österreich bedeutet dies nicht nur eine rechtliche Umsetzungspflicht, sondern auch eine strategische Chance zur Positionierung als innovationsfreundlicher Standort für verantwortungsvolle KI.

Vor diesem Hintergrund verfolgt das vorliegende Projekt das Ziel, eine evidenzbasierte Grundlage für die Ausgestaltung von KI Regulatory Sandboxes in Österreich zu schaffen. Im Fokus stehen dabei die Analyse regulatorischer Rahmenbedingungen, die Auswertung internationaler Good Practices, die Berücksichtigung sektoraler Besonderheiten sowie die Entwicklung eines Governance- und Umsetzungsmodells. Der Bericht dokumentiert die Ergebnisse der ersten Projektphase, in der eine systematische, KI-gestützte Desk Research durchgeführt wurde.

Diese bildet die analytische Basis für nachgelagerte Interviews, Workshops und strategische Empfehlungen, mit denen die Wirtschaftskammerorganisation (WKO) den Aufbau und die Gestaltung von KI-Sandboxes in Österreich aktiv mitgestalten kann.

2.1 ZIELSETZUNG UND KONZEPTIONELLER ANSATZ DER STUDIE

Im Rahmen der Studie wurden folgende übergeordnete Ziele verfolgt:

- Wissensaufbau zum Thema Bedarfe, Potenziale und Nutzen von Regulatory Sandboxes unter besonderer Berücksichtigung des KI-Bereichs
- Sammlung relevanter Praxisbeispiele aus dem nationalen wie internationalen Kontext zum Thema Regulatory Sandboxes, deren rechtliche Rahmenbedingungen, inhaltliche Ausrichtung und Governance

[1] „Regulatory Sandboxes“, „Sandboxes" oder „KI-Sandboxes”

- Erarbeitung von relevanten Use Cases für Regulatory Sandboxes im Bereich KI
- Sensibilisierung und Mobilisierung von Stakeholdern zum Thema Regulatory Sandboxes
- Unterstützung beim Netzwerkaufbau mit Stakeholdern und Expert:innen

Um die definierten Ziele im zur Verfügung stehenden Zeitraum effizient als auch empirisch fundiert erreichen zu können, war ein differenziertes methodisches Vorgehen notwendig, das aus aufeinander abgestimmten wie ineinandergreifenden Arbeitsschritten besteht. Das methodische Vorgehen verbindet etablierte Methoden der empirischen Sozialforschung (KI-gestützte Literatur- und Dokumentenanalyse sowie Expert:innen-Interviews) mit partizipativen, co-kreativen Workshops. Dadurch konnte nicht nur das bereits vorhandene Wissen zu Regulatory Sandboxes in Hinblick auf die relevanten Fragestellungen der Studie in einer synthetischen Weise zusammengefasst und entsprechend dem Bedarf des Auftraggebers aufbereitet werden, sondern es konnten auch Aufgabenstellungen bearbeitet werden, die einen stärker explorativen, in die Zukunft gerichteten Charakter haben. Gleichzeitig haben es die co-kreativen Workshops ermöglicht, nicht nur die Zwischen- wie Endergebnisse der Studie zu reflektieren und zu verfeinern, sondern boten auch die Möglichkeit, zur Bewusstseinsbildung und Mobilisierung von internen wie externen Stakeholdern hinsichtlich der zentralen Fragestellungen der Studie beizutragen.

2.2 METHODISCHES VORGEHEN

Desk Research

Ziel der Desk Research war es, eine fundierte Wissensgrundlage für die strategische Gestaltung von Regulatory Sandboxes im Bereich KI in Österreich zu schaffen. Im Fokus stand die Kombination von wissenschaftlicher Evidenz, regulatorischer Analyse und praxisnahen Fallbeispielen. Folgende Teilziele standen im Vordergrund:

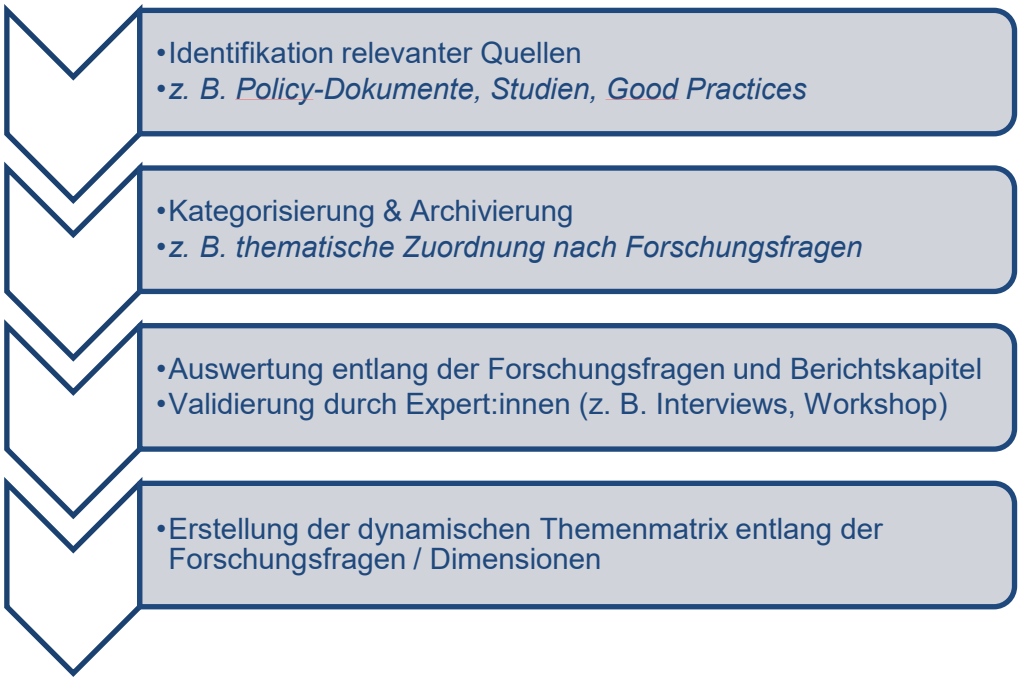
1. **Erhebung des Status quo bestehender regulatorischer Sandboxes** in Österreich und deren rechtliche, institutionelle und sektorale Einbettung.
2. **Analyse der Anforderungen der europäischen KI-Verordnung** mit Blick auf die nationale Umsetzungspflicht für KI Regulatory Sandboxes.
3. **Systematische Darstellung internationaler Good Practices** – einschließlich rechtlicher Rahmenbedingungen, Governance-Modelle und sektoraler Besonderheiten.
4. **Identifikation branchenspezifischer Bedarfe und Herausforderungen** in Form explorativer Use Cases (z. B. Medizintechnik, Industrie, Medien, Mobilität).
5. **Entwicklung einer dynamischen Themenmatrix** als zentrales Werkzeug für Analyse, Priorisierung und Diskussion von Fragestellungen.
6. **Unterstützung der Wirtschaftskammerorganisation (WKO)** beim Aufbau von Know-how und der Mobilisierung zum Thema KI Regulatory Sandboxes.

Die Desk Research diente somit nicht nur der Analyse, sondern fungierte auch als Transfer- und Orientierungsinstrument für Entscheidungsträger:innen im Spannungsfeld zwischen Regulierung und Innovation.

Konkrete Schritte

Die KI-unterstützte Desk Research bildete das methodische Rückgrat der ersten Projektphase. Sie kombiniert bewährte Literatur- und Dokumentenanalyse mit modernen KI-Tools und folgt einem modularen, mehrstufigen Ablauf. Dabei kommen **Large Language Models (LLMs)** zum Einsatz, deren Ergebnisse durchgehend durch Expert:innen des Projektteams kontextualisiert und validiert werden (Human-in-the-loop-Prinzip). Der Desk-Research-Prozess umfasste vier Schritte (*siehe Abbildung 1*)**.**

Abbildung 1: Vier Schritte der Desk Research



Quelle: Eigener Entwurf

1. Identifikation relevanter Quellen

Dieser Schritt umfasste die gezielte Sammlung einschlägiger Dokumente zu rechtlichen, technischen und politischen Aspekten von Regulatory Sandboxes – national wie international. Der Fokus lag einerseits auf der europäischen KI-Verordnung, der DSGVO sowie weiteren nationalen Gesetzgebungen. Andererseits wurden Informationen zu Anwendungsfeldern wie z. B. Medizintechnik, Industrie, Mobilität, Medien, internationalen Sandbox-Beispielen (z. B. Deutschland, Spanien, Schweiz) und Governance-Modellen und sektoralen Bedarfen gesammelt. Die Ergebnisse wurden in einem Literaturverwaltungsprogramm (Zotero) archiviert und thematisch verschlagwortet – als Grundlage für die inhaltliche Analyse.

2. Systematische Kategorisierung und Archivierung der Quellen

Die Dokumente wurden entlang eines festen Kriterienrasters verschlagwortet, u. a.: regulatorische Rahmenbedingungen, technologische Einsatzfelder, wirtschaftliche Perspektiven, Governance- und Steuerungsmodelle, internationale Good Practices und Stakeholderstrukturen. Für jedes Dokument wurden ein Abstract erstellt und relevante

Textpassagen für die KI-Auswertung vorbereitet, um Vergleichbarkeit und Tiefe der Analyse sicherzustellen.

3. KI-unterstützte Inhaltsanalyse und Auswertung

Die Auswertung erfolgte KI-gestützt mit ChatGPT (GPT-4o), unter Anwendung eines standardisierten Prompting-Verfahrens. Dabei wurde jeder Quellentext entlang eines konsistenten Analyseprofils durchleuchtet, wobei zentrale Aussagen extrahiert und einem Raster zugeordnet wurden. Alle Ergebnisse wurden durch das Projektteam validiert und inhaltlich eingeordnet (Human-in-the-loop-Prinzip). Die inhaltliche Erschließung orientierte sich an einem strukturierten **Fragenkatalog** (siehe Anhang), der direkt aus den Forschungsfragen abgeleitet wurde. Die zentralen Analyseachsen lauten:

- **Konzeption & Typen von Regulatory Sandboxes**: z. B. Unterschiede zu Reallaboren, Varianten mit/ohne Experimentierklausel, Ziele wie Politiklernen oder Technologietests
- **Rechtlich-institutionelle Rahmenbedingungen**: z. B. bestehende Gesetzeslagen in Österreich, Lücken und Vergleich zu Deutschland/Spanien/Schweiz
- **Internationale Good Practices**: z. B. Governance-Modelle, übertragbare Lessons Learned
- **KI-spezifische Herausforderungen und Chancen**: z. B. Blackbox-Problematik, Hochrisikoanwendungen, sektorspezifische Potenziale in Industrie, MedTech, Medien, Mobilität
- **Gestaltungsoptionen von Sandboxes**: z. B. Struktur, Ablauf, Risikomanagement, Lernprozesse, Skalierbarkeit
- **Governance und Stakeholder**: z. B. Rollen von Verwaltung, Wirtschaft, Forschung, funktionale Governance-Strukturen für eine nationale KI Sandbox
- **EU-rechtlicher Rahmen und Koordination**: z. B. Anforderungen aus der europäischen KI-Verordnung, Möglichkeiten der Anbindung an EU-Projekte
- **Handlungsoptionen und strategische Modelle**: z. B. Idealtypen von Sandboxes, Empfehlungen für Österreich

Die Analyse erfolgte pro Dokument, wobei je Quelle entlang der genannten Kategorien zentrale Inhalte extrahiert wurden. Die Ergebnisse wurden in einem tabellarischen Auswertungsformat festgehalten. So entstand ein inhaltlich vergleichbares und durchsuchbares Wissensraster mit direktem Bezug zu den Forschungsfragen. Durch die standardisierte Auswertung war es möglich, übergreifende Muster und Differenzen zu erkennen. Diese Muster bildeten die empirische Basis für die Themenmatrix und späteren Handlungsempfehlungen. Die KI-Auswertung wurde kontinuierlich durch das Projektteam überprüft, ergänzt und kontextualisiert. Dabei erfolgte eine Bewertung hinsichtlich der Validität der Aussagen (z. B. rechtliche Aussagen oder technische Details), der Relevanz im Hinblick auf das österreichische Innovations- und Regulierungssystem und der Anschlussfähigkeit an die Projektziele.

Am Ende dieses Schritts lag ein qualitätsgesicherter, systematisch gegliederter Wissenspool vor, der zentrale Erkenntnisse je Forschungsfrage aufbereitet, die Grundlage für die **Themenmatrix** liefert und gezielte Rückfragen für die **Expert:innen-Interviews** und **Co-Creation-Workshops** ermöglicht.

4. Strukturierte Synthese in der Themenmatrix

Im vierten Schritt wurden die Ergebnisse der KI-gestützten Inhaltsanalyse in einer systematischen **Themenmatrix** gebündelt. Diese Matrix diente als zentrales Analyse-, Kommunikations- und Steuerungsinstrument innerhalb des Projekts. Sie verknüpfte die Forschungsfragen mit empirischen Evidenzen, internationalen Beispielen und branchenspezifischen Herausforderungen – und bildete die Grundlage für Workshops, Interviews und Handlungsempfehlungen. Die Themenmatrix verfolgte mehrere Ziele: erstens die **analytische Strukturierung** der gewonnenen Erkenntnisse entlang definierter Themenkategorien und Forschungsfragen, zweitens die **Vergleichbarkeit** von Inhalten über Dokumente, Sektoren und Länder hinweg und drittens die **Identifikation von Handlungserfordernissen** in Österreich (z. B. gesetzliche Lücken, Governance-Defizite, Innovationshemmnisse) und die **Vorbereitung für die Validierung** im Rahmen von Workshops und Interviews mit Stakeholdern.

Die Matrix wurde als mehrdimensionale Tabelle angelegt, deren Einträge entlang folgender Hauptachsen (vorläufig) strukturiert sind:

1. **Themenfeld / Forschungsfrage:** z. B. „Welche regulatorischen Lücken bestehen in Österreich?“ oder „Welche Sandbox-Typen existieren international?“
2. **Kernaussagen / Evidenzbasis:** extrahierte Ergebnisse aus den analysierten Dokumenten (KI-gestützt und validiert)
3. **Branchenbezug / sektorale Relevanz:** Zuordnung zu Sektoren wie Medizintechnik, Industrie, Mobilität, Medien
4. **Regulatorischer Kontext:** Einordnung in nationale Gesetzeslage, europäische KI-Verordnung, DSGVO etc.
5. **Internationale Bezugspunkte:** Verweise auf relevante Länderbeispiele, Good Practices und Lessons Learned
6. **Stakeholder-Relevanz:** Einschätzung, welche Akteursgruppen jeweils betroffen oder verantwortlich sind (z. B. Ministerien, WKO, Unternehmen)
7. **Implikationen / Diskussionsbedarf:** Hinweise für Workshops, Interviews oder strategische Entscheidungen

Die Themenmatrix wurde als **„Living Document“** angelegt – sie wurde im Verlauf des Projekts iterativ erweitert und verfeinert:

- **Nach jeder Analysewelle** (Literatur, Interviews, Workshops) erfolgt eine Fortschreibung.
- **Rückmeldungen aus Workshops** (v. a. WS1 und WS2) fließen systematisch ein.
- **Identifizierte Lücken oder Diskussionsbedarfe** werden vermerkt und dienen als Input für nachfolgende Arbeitsschritte (z. B. Interviewleitfäden).

Die strukturierte Darstellung in der Matrix ermöglichte es, komplexe Informationen zielgruppenorientiert aufzubereiten. Sie diente sowohl als **Diskussionsgrundlage** für Co-Creation-Formate und als **Dokumentationsinstrument** für Entscheidungsprozesse als auch als **Grundlage für Empfehlungen** im Abschlussbericht und als **Brücke zur nationalen Umsetzung** der europäischen KI-Verordnung.

Expert:innen-Interviews und Co-Creation

Im Rahmen der Studie wurden 20 semi-strukturierte Expert:innen-Interviews mit unterschiedlichen Zielgruppen in Österreich sowie in EU-Mitgliedstaaten bzw. der Schweiz durchgeführt. So konnten einerseits vertiefende Erkenntnisse zu ausgewählten internationalen und gegebenenfalls nationalen Good-Practice-Beispielen gesammelt und andererseits die regulatorischen Herausforderungen und Bedarfe sowie die Potenziale und der Nutzen von Regulatory Sandboxes für österreichische Unternehmen aus unterschiedlichen Branchen unter besonderer Berücksichtigung von KI-Unternehmen erhoben werden.

Tabelle 1: Gespräche mit nationalen Expert:innen

Organisation
Austrian Society for Artificial Intelligence (ASAI)
Software Competence Center Hagenberg
AI Factory Austria AI:AT
DIH SÜD GmbH
Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)
Bundeskanzleramt (BKA)
Women in AI / TechMeetsLegal
Finanzmarktaufsicht (FMA)
Austrian Institute of Technology (AIT)
IDea_Lab Universität Graz
Probando GmbH
Joanneum Research Forschungsgesellschaft mbH

Quelle: Eigene Zusammenstellung

Tabelle 2 bietet einen komplementären Überblick über jene Institutionen aus anderen EU-Staaten bzw. der Schweiz, mit denen Interviews geführt wurden.

Tabelle 2: Gespräche mit internationalen Expert:innen

Organisation	Land
Innovation-Sandbox für Künstliche Intelligenz	Schweiz
AppliedAI Initiative	Deutschland
Katholische Universität Löwen	Belgien
European DIGITAL SME Alliance	Belgien

Reallabor zum Transfer digitaler Gesundheitsanwendungen und KI ins Gesundheitswesen	Deutschland
Wirtschaftsförderung Region Stuttgart GmbH	Deutschland
Projektträger Jülich / DigiSandbox NRW	Deutschland
Legal Department of the Luxembourg Chamber of Commerce	Luxemburg

Quelle: Eigene Zusammenstellung

Im Projekt wurde ein umfassender Open-Innovation-Prozess umgesetzt, der zwei zentrale Ziele verfolgt. Zum einen sollte unter den relevanten Stakeholdern in Österreich ein Bewusstsein für das Thema Reallabore und Regulatory Sandboxes geschaffen werden und zum anderen konnten Herausforderungen und Lösungsansätze in einer Co-Creation-Umgebung gemeinsam identifiziert und reflektiert werden.

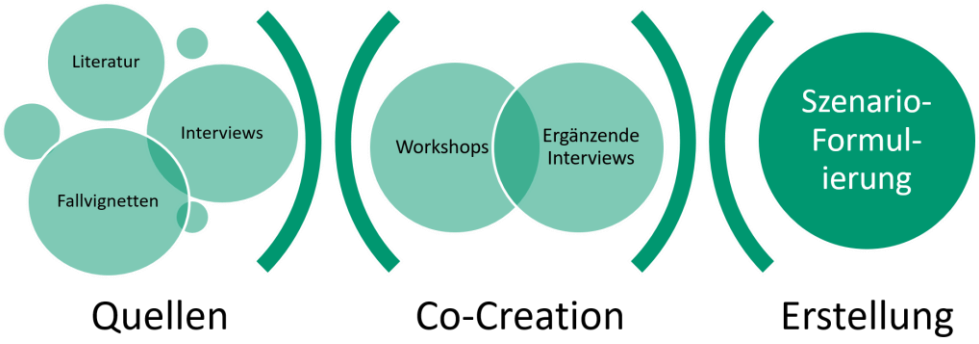
Von Mai bis Ende Juni 2025 wurden insgesamt drei Workshops durchgeführt; Details zu Zielen und dem Ablauf finden sich im Anhang.

Entwicklung von Implementierungsszenarien

Aufbauend auf den Ergebnissen der Desk Research, den Expert:innen-Interviews und Co-Creation-Workshops wurden vom Projektteam mögliche Implementierungsszenarien für eine KI-Sandbox in Österreich entworfen. Abbildung 2 bietet einen schematisierten Überblick über die relevanten Schritte und ihre jeweilige Interaktion.

Als Quellen für die Formulierung der Szenarien wurden vor allem die im Rahmen der Desk Research analysierte Literatur, die Erhebungen zu den internationalen Good-Practice-Beispielen und die Expert:innen-Interviews herangezogen.

Abbildung 2: Quellen und Prozess der Szenarioerstellung



Quelle: Eigener Entwurf

Ergänzend wurden die Ergebnisse der Co-Creation-Workshops und zusätzlicher fokussierter Expert:innen-Interviews in Österreich angereichert in die Szenarien eingepflegt. Das World-Café am 26.06.2025 war ausschließlich der Reflexion und Ergänzung der entwickelten vier Szenario-Hypothesen (horizontale Bundessandbox, sektorale Bundesandbox) gewidmet. Die

Ergebnisse des World-Cafés sowie ergänzender Interviews haben dann zur abschließenden Formulierung der Szenarien (siehe Kapitel 9) geführt.

3 Begriffliche und konzeptionelle Grundlagen

3.1 EINLEITUNG

Um Regulatory Sandboxes strategisch gestalten zu können, braucht es ein präzises Verständnis ihrer begrifflichen, konzeptionellen und institutionellen Grundlagen. Dieses Kapitel schafft die **theoretische Basis für die weitere Analyse**, indem es das Konzept der Sandbox systematisch erläutert, von verwandten Formaten abgrenzt, Rollen und Governance-Strukturen beschreibt sowie die Offenheit des Instruments in seiner kontextuellen Vielfalt darstellt.

3.2 REGULATORY SANDBOXES – ÜBERBLICK UND VARIANTEN

Als Reaktion auf die Beschleunigung technologischer Innovationen wurde das Instrument der „Regulatory Sandbox“ entwickelt, um das Spannungsverhältnis zwischen Innovationsförderung und Rechtskonformität aufzulösen (Kaal, 2017). Regulatory Sandboxes ermöglichen die befristete Erprobung innovativer Lösungen unter realen Bedingungen innerhalb eines kontrollierten und teilweise flexibilisierten regulatorischen Rahmens (Jenik & Lauer, 2017). Der prototypische Anwendungsfall war der Finanzsektor. Im Jahr 2015 implementierte die britische Financial Conduct Authority (FCA) im Rahmen ihres „Project Innovate“ das erste Sandbox-Modell (Financial Conduct Authority, 2015). Ihr Ziel: Unternehmen den Marktzugang erleichtern, ohne grundlegende aufsichtsrechtliche Prinzipien wie Konsumentenschutz oder Systemstabilität zu kompromittieren. Parallel sollten Regulierungsbehörden frühzeitig Erkenntnisse über neue Technologien und deren Risiken gewinnen (World Bank, 2020). In der Folge wurden weltweit über 70 Sandbox-Programme initiiert – u. a. in Singapur, Australien, den Niederlanden, Mexiko oder den Vereinigten Arabischen Emiraten (Cambridge Centre for Alternative Finance, 2019; UNSGSA, 2020).

Neben regulatorischen Vorteilen zeigen empirische Studien zudem ökonomische Wirkungen: Cornelli et al. (2020) konnten in einer quantitativen Analyse für Großbritannien nachweisen, dass die Teilnahme an einer Sandbox mit einer erhöhten Wahrscheinlichkeit für Folgeinvestitionen in Verbindung steht. Gleiches gilt für Asien: Goo und Heo (2020) dokumentieren, dass Sandbox-Teilnehmer in Südkorea *signifikant mehr Wagniskapital* erhielten als vergleichbare Kontrollunternehmen.

Regulatory Sandboxes sind heute fester Bestandteil moderner Innovationspolitik als gezielte Interventionsform, die Lernen und Governance miteinander verbindet (Allen, 2019; APEC, 2021).

Überblick: Allgemeines Verständnis und Varianten

Im engeren Sinn bezeichnet eine Regulatory Sandbox ein (staatlich) autorisiertes Testfeld, in dem innovative Produkte oder Dienstleistungen unter zeitlich und räumlich begrenzten Bedingungen sowie unter der Aufsicht bzw. Begleitung zuständiger Regulierungsbehörden ausprobiert werden können (Zetzsche et al., 2017; Jenik & Lauer, 2017). Dabei werden einzelne regulatorische Anforderungen temporär ausgesetzt oder angepasst, um Experimentierräume zu eröffnen, ohne den normativen Grundrahmen auszuhebeln (Arner et al., 2017; Fenwick, Vermeulen & Corrales Compagnucci, 2024). Darüber hinaus sind Regulatory Sandboxes typischerweise durch folgende **Kernelemente** gekennzeichnet:

- **Begrenzter Zugang:** Teilnehmen dürfen nur ausgewählte Akteure, häufig nach einem kompetitiven Auswahlverfahren (Cambridge Centre for Alternative Finance, 2019).
- **Transparenzpflichten:** Die Dokumentation von Fortschritt und Risiken ist zentral, um systematische Lerneffekte zu erzielen (World Bank, 2020).

Neben diesen strukturellen Aspekten ist das Zielprofil zentral. Regulatory Sandboxes können sich auf die Technologieerprobung, das Politiklernen oder die Vorbereitung einer normativen Weiterentwicklung richten (Kaal, 2017; Allen, 2019). In jüngster Zeit entstehen zunehmend thematische Sandboxes, etwa im Bereich nachhaltiger Technologien, digitaler Identitäten oder KI (UNSGSA, 2020; ECLAC, 2024). Schließlich sind Sandboxes auch als Baustein dynamischer Regulierung zu verstehen – als institutionelle Antwort auf das Spannungsverhältnis zwischen der Geschwindigkeit von Innovation und der Trägheit regulativer Prozesse (Zetzsche et al., 2017; Fenwick et al., 2024). Regulatory Sandboxes sind kein einheitliches Format, sondern ein Sammelbegriff für eine Vielzahl von institutionellen, regulatorischen und organisatorischen Testumgebungen (Jenik & Lauer, 2017).

Die Unterscheidung erfolgt erstens entlang des **Grades formaler Absicherung**. Während einige Sandboxes lediglich auf Memoranden oder Verwaltungspraxis beruhen (z. B. die early-stage Sandbox Singapur), sind andere rechtlich ausdrücklich normiert – etwa durch sektorale Experimentierklauseln oder eigenständige Sandbox-Gesetze (BMWK, 2024; Zetzsche et al., 2017).

Zweitens lassen sich Sandboxes nach ihrer **Zielsetzung differenzieren**. Manche dienen primär der **Technologieerprobung** (etwa bei neuartigen Zahlungssystemen), andere legen den Fokus auf **Regulationslernen** – also der institutionellen Reflexion bestehender Normen unter neuen technologischen Bedingungen (Arner et al., 2017; Allen, 2019). Ein drittes Modell zielt auf die **Vorbereitung normativer Änderungen**, indem empirische Evidenz gesammelt wird, um Regulierungsinstrumente ex-ante zu verbessern (Kaal, 2017; World Bank, 2020).

Eine weitere Typologie bezieht sich auf die **sektorale Ausrichtung**: Während erste Sandboxes vor allem im Finanzbereich etabliert wurden (z. B. FCA UK, MAS Singapur), entstehen zunehmend sektorübergreifende Modelle, etwa im Energierecht, im Gesundheitswesen oder für KI-Anwendungen (UNSGSA, 2020; ECLAC, 2024). In Frankreich beispielsweise wurde eine KI-Sandbox mit Fokus auf Gesundheitsdaten geschaffen, in Spanien agiert die Comisión Nacional del Mercado de Valores im Rahmen eines strukturierten Testprogramms für FinTechs (European Commission, 2023; OECD, 2021).

Neben der sektoralen Differenzierung lassen sich Regulatory Sandboxes auch nach ihrem **institutionellen Verankerungsniveau** typologisieren. So existieren **zentralstaatliche Sandboxes**, die auf Bundesebene angesiedelt sind (z. B. UK Financial Conduct Authority), ebenso wie **dezentrale Modelle** auf Ebene einzelner Bundesländer oder Regionen – etwa in Deutschland oder Kanada, wo föderale Strukturen regionale Testfelder ermöglichen (BMWK, 2024; SECO, 2022).

Transnationale Sandboxes gewinnen im Kontext europäischer Regulierung zunehmend an Bedeutung. Hierbei handelt es sich um koordinierte Testumgebungen zwischen mehreren Staaten – etwa im Rahmen des Global Financial Innovation Network (GFIN) oder von EU-Initiativen zur sektorübergreifenden KI-Erprobung (OECD, 2021; European Commission, 2023). Auch sogenannte **Meta-Sandboxes** zeichnen sich ab: strukturierte Rahmenwerke,

unter denen mehrere thematisch oder geografisch definierte Testfelder koordiniert werden – etwa durch gemeinsame Governance-Standards, Monitoring-Protokolle oder Evaluationsformate (Leimüller et al., 2024).

Diese internationale Vielfalt legt nahe, dass Regulatory Sandboxes nicht als starres Format, sondern als **Governance-Infrastruktur mit kontextsensibler Ausgestaltung** verstanden werden müssen (Zetzsche et al., 2017; Allen, 2019; OECD, 2021).

Vorteile, Nutzen, Herausforderungen und Grenzen

Die wesentliche Funktion von Regulatory Sandboxes besteht darin, einen strukturierten Lernraum für Innovation und Regulierung zu schaffen – bei gleichzeitiger Wahrung grundlegender Prinzipien wie Sicherheit, Transparenz und Verbraucherschutz (Financial Conduct Authority, 2015; World Bank, 2020).

Aus Unternehmenssicht bieten Sandboxes die Möglichkeit, **innovative Technologien unter klar definierten Bedingungen zu testen**, ohne unmittelbar dem vollen regulatorischen Rahmen zu unterliegen. Dies erleichtert Marktzugänge, reduziert Transaktionskosten und beschleunigt Entwicklungszyklen (Cornelli et al., 2020; Goo & Heo, 2020). Für Regulierungsbehörden wiederum eröffnen Sandboxes eine Plattform, um neue Technologien frühzeitig kennenzulernen, deren Risiken besser einzuschätzen und durch gezielte Beobachtung **datengestützte Evidenz für zukünftige Regulierungen** zu generieren (Kaal, 2017; OECD, 2021). Diese Interaktion reduziert nicht nur Informationsasymmetrien, sondern stärkt auch das Vertrauen zwischen regulatorischer Aufsicht und Wirtschaft (Jenik & Lauer, 2017). Ein dritter Nutzen liegt in der **Reputationseffizienz**: Staaten oder Regionen, die Sandboxes anbieten, signalisieren Offenheit für technologische Innovation und können sich dadurch als zukunftsorientierte Standorte positionieren – ein Argument, das etwa in Dubai oder Litauen strategisch eingesetzt wurde (UNSGSA, 2020; ECLAC, 2024; OECD, 2021).

Nicht zuletzt zeigen Studien eine positive Korrelation zwischen Sandbox-Teilnahme und **Zugang zu Wagniskapital** (Cornelli et al., 2020; FSB, 2020). Diese finanzielle Hebelwirkung kann insbesondere für KMU ein entscheidender Vorteil sein, um innovative Ideen über die Pilotphase hinaus zu skalieren.

Allerdings ist der Nutzen von Sandboxes **nicht automatisch gegeben**: Ohne klare Zieldefinition, ausreichende Ressourcen und eine ordentliche rechtliche Einbettung besteht die Gefahr, dass die Form über den Inhalt siegt (Allen, 2019; OECD, 2021).

Trotz ihrer Attraktivität als innovationspolitisches Instrument stehen Regulatory Sandboxes vor mehreren strukturellen und normativen Herausforderungen. Ein zentrales Problem betrifft die **Rechtsstaatlichkeit und Gleichbehandlung**: Wenn einzelnen Unternehmen temporär Ausnahmen gewährt werden, kann dies als Wettbewerbsverzerrung wahrgenommen werden – insbesondere, wenn die Zugangskriterien unklar oder die Auswahlverfahren intransparent sind (Allen, 2019; Zetzsche et al., 2017; OECD, 2021). Darüber hinaus bestehen **haushalts- und ressourcenbezogene Engpässe**: Die Durchführung und Begleitung eines Sandbox-Prozesses erfordert erhebliche personelle, technische und juristische Kapazitäten – sowohl bei den Behörden als auch bei den teilnehmenden Unternehmen (Cambridge Centre for Alternative Finance, 2019; UNSGSA, 2020). Länder mit begrenzten

Verwaltungskapazitäten laufen Gefahr, Sandboxes als symbolische Innovationspolitik zu etablieren, ohne nachhaltige Lerneffekte zu generieren (APEC, 2021).

Ein weiteres Risiko besteht im **Regulatory Capture** und damit verbundenen **Verzerrungen des marktlichen Wettbewerbs**: Wenn Sandbox-Prozesse zu stark von wirtschaftlichen Interessen dominiert werden, besteht die Gefahr, dass einzelne Unternehmen zu intensiv ohne ein Gegengewicht durch unabhängige Expertise auf mögliche Regulierungen einwirken könnten (Kaal, 2017; Allen, 2019; OECD, 2021).

Zudem bleibt der **Transfer in das reguläre System** häufig ungeklärt: Studien zeigen, dass viele Sandbox-Projekte am Übergang vom Experiment zur Verstetigung scheitern oder regulatorisch „versanden". Das Scheitern am Übergang von Experiment zu Verstetigung resultiert meist aus einem Zusammenspiel von unzureichender Planung, fehlenden Ressourcen, regulatorischer Starrheit und mangelnder Einbindung der relevanten Akteure. Um diesen Herausforderungen zu begegnen, ist eine frühzeitige und systematische Übergangsplanung sowie eine enge Zusammenarbeit mit Regulierungsbehörden und Stakeholdern entscheidend. (Zetzsche et al., 2017; Fenwick et al., 2024) Dieses sogenannte „scaling gap" limitiert den langfristigen Impact.

Nicht zuletzt existieren **ethische und datenschutzrechtliche Unsicherheiten**, etwa wenn Tests auf personenbezogene Daten oder algorithmische Entscheidungsfindung zurückgreifen – wie es bei KI-Anwendungen der Fall ist (European Commission, 2023; ECLAC, 2024).

Begriffserklärung: Sandbox, Reallabor, Experimentierklausel, Testumgebung

Die Diskussion um Regulatory Sandboxes wird häufig durch eine unscharfe oder gleichsetzende Verwendung verwandter Begriffe erschwert. Konzepte wie „Reallabor", „Experimentierklausel" oder „Testumgebung" werden teils synonym zur Sandbox verwendet, obwohl sie unterschiedliche institutionelle, normative und operationale Implikationen aufweisen (Bogner, Kuhlmann & Schubert, 2014; Gellert & Oertel, 2022). Diese Unschärfe birgt Risiken: Einerseits kann es zu überhöhten oder unangemessenen Erwartungen an Sandbox-Instrumente kommen, andererseits zu falschen regulatorischen Rückschlüssen. Eine präzise Abgrenzung der Begrifflichkeiten ist daher grundlegend – nicht nur aus wissenschaftlicher Perspektive, sondern auch für die Praxis der Rechtsgestaltung und Innovationspolitik (Zetzsche et al., 2017; OECD, 2021).

„Regulatory Sandbox" im engeren Sinne: Der Begriff „Regulatory Sandbox" bezeichnet ein von staatlichen Stellen autorisiertes Testumfeld, in dem ausgewählte Unternehmen neue Produkte oder Dienstleistungen unter realen Marktbedingungen austesten können – bei gleichzeitiger temporärer Anpassung oder Flexibilisierung regulatorischer Anforderungen (Financial Conduct Authority, 2015; World Bank, 2020). Im Zentrum steht nicht primär die technologische Innovation selbst, sondern deren Interaktion mit normativen Vorgaben wie Finanzmarktregeln, Datenschutz oder Produktsicherheit (Arner et al., 2017; Kaal, 2017). Im Gegensatz zu klassischen Innovationsförderprogrammen operieren Sandboxes im institutionellen Grenzbereich zwischen regulatorischer Aufsicht und Markt, und ermöglichen unter Aufsicht eine partielle Entgrenzung rechtlicher Vorgaben – jedoch stets auf Zeit, unter Auflagen und mit Rückkopplungspflicht (Jenik & Lauer, 2017; Allen, 2019). Entscheidend ist,

dass Sandbox-Teilnehmer sich nicht „außerhalb“ der Regulierung bewegen, sondern in einem formal definierten Experimentierraum innerhalb des Systems (Cambridge Centre for Alternative Finance, 2019).

Reallabor: Das Konzept des Reallabors stammt ursprünglich aus der transdisziplinären Nachhaltigkeitsforschung und betont die Co-Produktion von Wissen durch Wissenschaft, Gesellschaft und Politik (Schneidewind, 2014; Wanner et al., 2022). Im Vordergrund stehen partizipative Prozesse, gesellschaftliche Transformation und eine experimentelle Praxis jenseits rein technischer Lösungen. Anders als Sandboxes sind Reallabore meist nicht regulatorisch flankiert, sondern **freiwillig**, **dialogisch** und **langfristig angelegt**. Es ist zugleich darauf hinzuweisen, dass in der offiziellen deutschen Übersetzung der europäischen KI-Verordnung der Begriff der Regulatory Sandbox mit Reallabor übersetzt worden ist.

Experimentierklausel: Hierbei handelt es sich um ein juristisches Instrument, das es erlaubt, **explizit im Gesetz verankerte Ausnahmen vom geltenden Recht** zu erproben (Gellert & Oertel, 2022). Anders als bei Sandboxes, wo Aufsichtsbehörden flexibel agieren, ist bei Experimentierklauseln die Möglichkeit zur Abweichung **gesetzlich normiert und meist eng befristet**. Der Fokus liegt stärker auf rechtspolitischer Erkenntnisgewinnung als auf marktlicher Innovation (BMWK, 2024).

Testumgebung: Dieser Begriff wird häufig techniknah verwendet und bezeichnet die **praktische Erprobung von Produkten oder Verfahren**, etwa in der Software- oder Medizintechnik. Sie verfügen in der Regel **nicht über eine regulatorische Ausnahmestellung**, sondern erfolgen innerhalb bestehender rechtlicher Rahmenbedingungen (OECD, 2021; UNSGSA, 2020). Während eine Sandbox auch rechtliche Komponenten umfasst, bleibt eine technische Testumgebung regulatorisch neutral.

Tabelle 3: Gemeinsamkeiten und Unterschiede von Regulatory Sandboxes und verwandten Konzepten

Dimension	**Rechtl. Grundlage**	**Zielsetzung**	**Beteiligung**	**Fokus**
Regulatory Sandbox	Behördlich / regulatorisch	Regulierung u. Innovation	Unternehmen, Aufsicht	Normumgang u. Anwendung
Reallabor	Projektbasiert	Gesellschaftl. Lernen	Wissenschaft, Bürger, Behörden	Soziale Transformation
Experimentier-klausel	Gesetzlich normiert	Normänderung vorbereiten	Gesetzgeber, Verwaltung	Rechtliche Evaluation
Testumgebung	Technisch definiert	Funktionstestung	Technikent-wicklung	System- u. Produkttests

Quelle: Eigene Zusammenstellung

Obwohl die Begriffe „Regulatory Sandbox“, „Reallabor“, „Experimentierklausel“ und „Testumgebung“ teils überlappende Ziele wie Innovationsförderung oder Wissensgenerierung verfolgen, unterscheiden sie sich systematisch entlang mehrerer Dimensionen: rechtliche Verankerung, institutionelle Trägerschaft, zeitliche Struktur, Partizipationslogik und normativer Anspruch. Tabelle 3 bietet einen entsprechenden Überblick.

Relevanz dieser Unterscheidung für den österreichischen Kontext

Für die strategische Entwicklung von Regulatory Sandboxes in Österreich ist eine präzise begriffliche Trennschärfe entscheidend. In der politischen und medialen Debatte besteht die Tendenz, verschiedene Formate unter dem Etikett „Reallabor" oder „Sandbox" zu subsumieren – ungeachtet der normativen, juristischen und institutionellen Unterschiede (Buchinger, 2021; Gellert & Oertel, 2022). Dies birgt die Gefahr, dass **falsche Erwartungshaltungen** erzeugt und regulatorische Instrumente entweder überfrachtet oder unterkomplex gestaltet werden.

Besonders relevant ist diese Unterscheidung im Hinblick auf die kommende Umsetzung der KI-Verordnung der EU, in der ausdrücklich von „regulatorischen Sandboxes" im Sinne temporärer Aufsichtsexperimente die Rede ist – nicht von Reallaboren oder rein technischen Tests (European Commission, 2023). Fehlende begriffliche Differenzierung könnte dazu führen, dass Österreich entweder zu zögerlich agiert oder Formate etabliert, die die europäischen Anforderungen nicht erfüllen.

Zudem bedingt die juristische Praxis eine klare Differenzierung zwischen normativ verankerten Experimenten (z. B. via Gesetz) und verwaltungspraktischen Pilotierungen. Nur so lassen sich **Rechtssicherheit und Innovationsfreiheit** effektiv verbinden (Hoffmann-Riem, 2008).

3.3 ROLLENVERSTÄNDNIS: GOVERNANCE, BETEILIGTE, RISIKOMANAGEMENT

Regulatory Sandboxes erfordern ein differenziertes Verständnis der beteiligten Akteure und ihrer Verantwortlichkeiten. Dieses Kapitel analysiert, **wie Governance strukturiert ist, wer welche Rolle im Sandbox-Prozess übernimmt und wie Risiken verteilt und gesteuert werden** – zentrale Fragen für Legitimität, Effizienz und Vertrauen in regulatorische Experimente.

Regulatory Sandboxes fungieren nicht als technokratische Innovationsräume, sondern als **politisch und institutionell orchestrierte Regulierungsinstrumente**. Ihr Erfolg hängt entscheidend davon ab, wie klar die Rollen und Verantwortlichkeiten zwischen staatlichen Akteuren, Unternehmen und weiteren Anspruchsgruppen verteilt sind. Eine Sandbox kann nur dann ihren doppelten Zweck – Innovationsförderung und Risikobewältigung – erfüllen, wenn Governance-Strukturen nicht nachgelagert, sondern integraler Bestandteil des Designs sind (Black & Murray, 2019).

Die internationale Erfahrung zeigt: Unklare Zuständigkeiten, fehlende Leitprinzipien oder übermäßiger Einfluss einzelner Akteursgruppen führen zu Legitimitäts- und Effizienzdefiziten (Goslinga & Grünewald, 2021). Gerade im Hinblick auf die gesellschaftliche Akzeptanz regulatorischer Experimente wie etwa bei KI-Systemen, ist transparente und differenzierte Governance unabdingbar (Floridi et al., 2018).

Die zentrale Steuerungsrolle in Sandboxes liegt bei staatlichen Einrichtungen – typischerweise bei **Regulierungs- oder Aufsichtsbehörden**, seltener bei Ministerien oder Regierungen selbst (OECD, 2021; World Bank, 2020). Diese übernehmen unterschiedliche Funktionen: sie initiieren die Sandbox, definieren Auswahl- und Evaluierungskriterien, begleiten den

Testbetrieb und sichern gegebenenfalls eine Reintegration in den regulären Rechtsrahmen (Black & Murray, 2019). Dabei sind drei Rollen zu unterscheiden:

1. **Initiator**: Oft agieren Behörden (z. B. Finanzmarktaufsichten oder Datenschutzbehörden) als Gestalter des Formats. Sie definieren Ziel und Reichweite der Sandbox.
2. **Moderator**: In laufenden Projekten sind sie Vermittler zwischen Interessen, z. B. bei Konflikten zwischen Unternehmen und betroffenen Dritten.
3. **Aufseher**: Im Sinne des Rechtsstaatsprinzips bleibt die Behörde für die Einhaltung zentraler Schutzpflichten verantwortlich (auch bei temporären Ausnahmen).

Die genaue institutionelle Verankerung variiert international stark. Während beispielsweise in UK oder Singapur spezialisierte Sandbox-Einheiten innerhalb der Finanzaufsicht bestehen, setzen andere Länder auf interministerielle Plattformen oder Kooperationen mit Innovationsagenturen (APEC, 2021).

Ein zunehmender Trend ist die Delegation bestimmter operativer Aufgaben an halbstaatliche oder intermediäre Organisationen, zum Beispiel zur **technischen Begleitung oder zur Schnittstelle mit Unternehmen** (Schuetz et al., 2023). Dies birgt Chancen für Effizienz, verlangt jedoch klare Steuerungs- und Haftungsregeln.

Private Akteure und insbesondere Start-ups, KMU, aber auch große Technologiekonzerne sind zentrale Teilnehmer an Sandboxes. Sie bringen die Innovation ein, übernehmen die technische Implementierung und sind im Erfolgsfall Nutznießer des regulatorischen Experiments (Cornelli et al., 2020; Allen, 2019). Zugleich tragen sie Verantwortung für **Compliance innerhalb des Sandbox-Rahmens**, etwa hinsichtlich des Verbraucherschutzes oder der Datensicherheit.

Die Teilnahme an einer Sandbox ist in der Regel an bestimmte Bedingungen geknüpft: **Innovationshöhe, regulatorische Relevanz, potenzieller Nutzen für die Allgemeinheit oder Lernpotenzial für die Behörde** (OECD, 2021; Auer & Claessens, 2018). Hierbei besteht die Herausforderung, Antragsverfahren weder zu überregulieren noch so offen zu gestalten, dass Beliebigkeit droht.

Ein wesentliches Spannungsfeld ergibt sich zwischen **kleinen, experimentellen Akteuren und großen Marktteilnehmern**. Während Sandboxes ursprünglich insbesondere Start-ups adressierten, nehmen zunehmend auch etablierte Unternehmen teil. Hier gibt es ungleiche Ressourcen und Einflussmöglichkeiten (Zetzsche et al., 2017; Black & Murray, 2019). Dies wirft Fragen der Fairness und Zugänglichkeit im Hinblick auf technische Unterstützung oder rechtliche Beratung auf.

Auch strategisch motivierte Sandbox-Teilnahmen („Regulatory Arbitrage“) sind nicht auszuschließen. Unternehmen könnten primär auf einen erleichterten Marktzugang spekulieren, ohne ernsthafte Innovationsambitionen zu verfolgen (Buchinger, 2021). Eine **klare Rollenzuweisung, transparente Kriterien und begleitende Evaluierung** sind deshalb essenziell.

Während staatliche Akteure und Unternehmen die institutionelle Hauptachse von Regulatory Sandboxes bilden, wird die Einbindung gesellschaftlicher Akteure und wissenschaftlicher Expertise zunehmend als Erfolgsfaktor erkannt. In vielen Ländern zeigte sich, dass **fehlende Partizipation externer Anspruchsgruppen** (z. B. Forschungseinrichtungen, Vertreter:innen

der Zivilgesellschaft, Ethikräte) zu Legitimitätsdefiziten und Vertrauenserosion führen kann (Goslinga & Grünewald, 2021; OECD, 2021).

Zivilgesellschaftliche Organisationen können frühzeitig auf soziale, ethische oder ökologische Risiken hinweisen und so zur normativen Fundierung des Sandbox-Designs beitragen. Besonders relevant wird dies im Kontext von Technologien wie künstlicher Intelligenz, der Verarbeitung von Gesundheitsdaten oder automatisierter Entscheidungsfindung (Floridi et al., 2018; Mantelero, 2022). Dennoch sind sie bislang nur selten institutionell im Rahmen von Begleitgremien oder Beratungskommissionen verankert (European Commission, 2023; van den Broek et al., 2021).

Auch **wissenschaftliche Akteure** können mehrfache Funktionen erfüllen: Sie generieren begleitende Evidenz, evaluieren Wirksamkeit und helfen bei der Übertragbarkeit erfolgreicher Sandbox-Ergebnisse auf andere Kontexte (Hofmann et al., 2020). Ihre Beteiligung sichert epistemische Vielfalt und verringert die Gefahr einseitiger Technologieförderung.

Einige Länder (z. B. Niederlande, Finnland oder Kanada) binden Hochschulen oder Think Tanks systematisch in die Konzeption und Auswertung von Sandboxes ein (Wagner et al., 2021).

Da Regulatory Sandboxes an der Schnittstelle zwischen Regulierungsausnahme und Markterprobung operieren, ist ein strukturiertes Risikomanagement unabdingbar. Fehlende Definitionen von Haftung, Verantwortlichkeit und Exit-Mechanismen führen nicht nur zu praktischen Problemen, sondern untergraben die normative Glaubwürdigkeit des Instruments (Black & Murray, 2019; Lindholm, 2022).

Zentral ist die **Verteilung regulatorischer Verantwortung**:

- Wer haftet im Schadensfall?
- Wie wird mit Zwischenfällen umgegangen?
- Was passiert bei Projektausfall?

Während Unternehmen für technische Fehler verantwortlich sind, liegt die politische Verantwortung für das Setting zumeist bei den Behörden (OECD, 2021). Diese duale Struktur verlangt klare Governance-Mechanismen in Form von Memoranda of Understanding (MoUs), Risikoklassifikationen und Eskalationsroutinen (World Bank, 2020; Schuetz et al., 2023).

Zudem bedarf es klarer **Kriterien für den Abbruch („Kill Switch“) oder Abschluss** eines Sandbox-Projekts. Diese betreffen nicht nur technische Indikatoren, sondern auch normative Benchmarks, etwa zu Datenschutz oder Diskriminierungsvermeidung (Floridi et al., 2018; Mantelero, 2022), die insbesondere im Bereich KI zum Tragen kommen könnten. Ohne diese Exit-Pfade droht ein „regulatorischer Zwischenraum“, der Unsicherheit erzeugt.

Innovative Ansätze gehen mittlerweile über klassische Risikoanalysen hinaus: In Singapur etwa wurde ein **„Ethics-by-Design“-Ansatz** entwickelt, der schon in der Konzeption von Sandbox-Projekten ethische Risikofolgenabschätzung integriert (Wagner et al., 2021).

Insgesamt gilt: Ohne strukturiertes Risikomanagement wird aus der Sandbox schnell ein „Regulatory Blind Spot“ mit entsprechendem Reputations- und Vertrauensverlust für die beteiligten Institutionen (Lindholm, 2022; Hofmann et al., 2020).

3.4 OFFENHEIT DES KONZEPTS: DIFFERENZIERUNG STATT FIXIERUNG

Regulatory Sandboxes sind per Definition **keine standardisierten Instrumente**, sondern offene Governance-Formate, deren konkrete Ausgestaltung stark vom jeweiligen politischen, regulatorischen und sektoralen Kontext abhängt (Sabel & Zeitlin, 2012). Die internationale Praxis zeigt: Der Erfolg von Sandboxes hängt nicht von einer normativen Einheitslösung, sondern von ihrer **Anpassungsfähigkeit** an lokale institutionelle Bedingungen ab (OECD, 2021; Wagner, Eiden & Müller, 2021).

Im Gegensatz zu klassischen Regulierungsinstrumenten, wie technischen Normen oder Verwaltungsverordnungen, basieren Sandboxes auf **prozeduraler Offenheit und iterativer Justierung**. Sie sind keine „one size fits all"-Lösungen, sondern dynamische Settings, die durch Feedback und Lernprozesse stetig weiterentwickelt werden (Sabel & Simon, 2018). Diese Offenheit betrifft nicht nur das Design, sondern auch die Zieldefinition: Manche Sandboxes sind explizit auf Marktintegration ausgerichtet, andere verfolgen vorrangig explorative oder politische Lernziele (Black & Lodge, 2022).

Gerade in Europa gibt es eine große Heterogenität von Rechtssystemen, Innovationskulturen und Verwaltungstraditionen. Es hat sich gezeigt, dass **adaptive Sandbox-Modelle erfolgreicher sind** als starre Blaupausen (Bürgin, 2023). So basiert die französische „Régulation Sandbox IA Santé" auf einer engen Kooperation zwischen Gesundheitsaufsicht, der Commission Nationale de l'Informatique et des Libertés (CNIL) und Ministerien und verfolgt explizit das Ziel, KI-Systeme mit Gesundheitsbezug unter DSGVO-Bedingungen zu testen (CNIL & Health Data Hub, 2022). Die finnische Digital-Health-Sandbox hingegen wird von Sitra (Finnish Innovation Fund) und THL (Finnish Institute for Health and Welfare) getragen und zielt stärker auf sektorale Interoperabilität ab (Sitra, 2023). In den verschiedenen Sandboxes, die in den Good-Practice-Beispielen dargestellt sind, kam es auch zu Anpassungen bzgl. der Einbindung neuer Anspruchsgruppen, der Ausweitung auf weitere Sektoren in verschiedenen Phasenmodellen und zu kontinuierlichen Lernprozessen. Gerade in dieser prozessoralen Offenheit liegt die Stärke des Konzepts.

Zugleich birgt diese Offenheit auch Risiken: Ohne klare Mindeststandards besteht die Gefahr **semantischer Verwässerung** oder **politischer Instrumentalisierung** (Wagner et al., 2021). Daher ist es sinnvoll, ein Set an *funktionalen Kernelementen* zu identifizieren, wie beispielsweise Transparenz, Reversibilität oder regulatorische Einbettung, die als Qualitätskriterien unabhängig vom konkreten Kontext dienen (UNSGSA, 2020; Black & Lodge, 2022).

Für Österreich bedeutet das: **Internationale Modelle** müssen gesichtet und evaluiert werden, jedoch nicht exakt repliziert. Es ist nötig, die internationalen Modelle kontextuell unter Einbezug österreichischer Verwaltungs-, Rechts- und Innovationskultur zu übersetzen. Die Offenheit des Sandbox-Konzepts ist keine Schwäche, sondern eine Voraussetzung für Wirksamkeit und Legitimität – vorausgesetzt, sie wird unter Einbeziehung diverser Anspruchsgruppen **steuerungspolitisch bewusst gestaltet**.

3.5 KONZEPTUELLE EINORDNUNG UND OFFENLEGUNG MÖGLICHER AUSPRÄGUNGEN

Regulatory Sandboxes lassen sich nicht nur operational als Testumgebungen beschreiben, sondern erfordern eine **konzeptuelle Einordnung innerhalb der Innovations- und**

Regulierungstheorie. Dabei stehen sie an der Schnittstelle zwischen klassischen Steuerungsinstrumenten des Staates und neuen Formen adaptiver, lernorientierter Governance (Black & Lodge, 2022; Sabel & Zeitlin, 2012). Sie sind weniger ein normatives Endprodukt als vielmehr eine **prozessuale Infrastruktur zur kooperativen Problemlösung unter Unsicherheit** (Gerlach & Lösch, 2020).

Aus der institutionentheoretischen Perspektive stellen Sandboxes ein **instrumentelles Experimentierformat** dar, welches in Situationen eingesetzt wird, in denen weder technologische Entwicklungen vollständig verstanden, noch deren regulatorische Implikationen abschließend geklärt sind (Kuhlmann, Stegmaier & Konrad, 2019). Es ist somit kein Zufall, dass die Europäische Kommission mit der europäischen KI-Verordnung gerade künstliche Intelligenz als Anwendungsbereich gewählt hat – ein Bereich, der durch die Innovationsgeschwindigkeit dynamischen Veränderungen unterworfen ist. Damit unterscheiden sich diese Situationen sowohl von klassischen Innovationsförderinstrumenten (wie Cluster-Programmen oder Subventionen) als auch von rein normsetzenden Verfahren (wie Gesetzesnovellen oder Richtlinien).

Sie fungieren als **regelgeleitete Erprobungszonen**, in denen Innovationen mit regulatorischem Potenzial getestet werden, ohne sofort eine Systementscheidung zu erzwingen (Lindholm, 2022). Diese Versuchsarchitektur erlaubt es politischen und administrativen Systemen, ‚probeweise zu regeln', bevor irreversible Entscheidungen getroffen werden – ein Prinzip, das in der experimentellen Governance (Sabel & Simon, 2018) und im Konzept der „regulativen Vortestung" (Gerlach & Lösch, 2020) theoretisch verankert ist.

Zudem lassen sich Sandboxes als **„reflexive Governance-Arrangements"** einordnen. Sie erzeugen nicht nur empirische Daten, sondern auch institutionelle Reflexivität: Behörden lernen über die Tauglichkeit ihrer Regeln, Unternehmen über regulatorische Erwartungen und die Öffentlichkeit über systemische Risiken (Kuhlmann et al., 2019; Hofmann & Weyer, 2021)

Im Hinblick auf mögliche **Ausprägungen** lassen sich mehrere Dimensionen identifizieren:

- **Normativer Einschlag**: Von rein beobachtenden Formaten bis hin zu Experimentierklauseln mit echter Rechtswirkung.
- **Akteursstruktur**: Von exklusiven B2G-Testumgebungen bis zu partizipativen, multistakeholder-orientierten Settings.
- **Funktionaler Fokus**: Von technologiegetriebener Validierung über regulatorisches Lernen bis zu politisch-strategischer Systemgestaltung.

Diese Vielfalt ist kein Nachteil, sondern ein **Gestaltungsspielraum**: Die Wahl der Ausprägung sollte sich an konkreten Zielsetzungen, sektoralen Spezifika und institutionellen Kapazitäten orientieren wie etwa in Hinblick auf Datenschutz, Marktstruktur oder Innovationsreife (Bürgin, 2023).

Ein zentraler Vorteil der konzeptionellen Offenheit liegt darin, dass sie **Verknüpfungen mit anderen Governance-Formaten** erlaubt – etwa Reallaboren, Forschungsprogrammen oder normativen Deliberationsprozessen. Gerade in technologieintensiven Feldern wie KI, Biotechnologie oder Klimainnovation kann sich so ein hybrides Geflecht zwischen Regulierung, Exploration und Strategiebildung entwickeln (Jasanoff, 2018; Kuhlmann et al., 2019).

4 Funktionen, Formate und zentrale Gestaltungsmerkmale

4.1 EINLEITUNG

Regulatory Sandboxes sind vielfältig in ihrer Zielsetzung und Ausgestaltung. Dieses Kapitel untersucht, wie sie als **regulatorische Instrumente praktisch funktionieren**, welche Ziele sie verfolgen und welche strukturellen Voraussetzungen für ihre Wirksamkeit notwendig sind. Im Fokus stehen dabei **Regelungsansätze, institutionelle Designs und Skalierungsperspektiven**, die internationalen Erfahrungen folgend als zentrale Stellschrauben erfolgreicher Sandbox-Formate gelten.

4.2 TEMPORÄRE REGULIERUNGSAUSNAHMEN VS. INNOVATIONSRÄUME MIT BEOBACHTUNG

Regulatory Sandboxes lassen sich hinsichtlich ihrer **Rechtswirkung und Eingriffsintensität** grundlegend unterscheiden. Zwei Grundtypen stehen sich dabei gegenüber: (1) Sandboxes mit temporären Regulierungsausnahmen und (2) innovationsbezogene Beobachtungsräume ohne rechtliche Abweichung vom Status quo (Black & Lodge, 2022; Lindholm, 2022).

Sandboxes mit temporären Regulierungsausnahmen: Diese Form beruht auf der bewussten und rechtlich abgesicherten Möglichkeit, geltende Normen **zeitlich begrenzt außer Kraft zu setzen oder zu flexibilisieren**. Sie ermöglichen damit echten regulatorischen Spielraum wie beispielsweise durch **Experimentierklauseln**, befristete Ausnahmeregeln oder angepasste Genehmigungsverfahren (OECD, 2021; BMWK, 2024).
Ein konkretes Beispiel hierfür ist das deutsche Reallaborgesetz, das explizit vorsieht, dass für bestimmte Vorhaben der gesetzliche Rahmen im Sinne eines Experiments angepasst werden kann – allerdings stets unter Einbindung der Legislative (BMWK, 2024). Auch das britische Sandbox-Modell (FCA) sieht die Möglichkeit vor, in enger Abstimmung mit der Aufsicht regulatorische Anforderungen befristet zu lockern (FCA, 2015).
Solche Sandboxes stellen hohe Anforderungen an **Transparenz, Rechtsklarheit und Exit-Regelungen**, da sie mit dem Grundprinzip der Rechtssicherheit kollidieren können. Die Legitimität solcher Ausnahmen hängt stark von ihrer Begründung, ihrer Zweckbindung und der flankierenden Evaluation ab (Lindholm, 2022; Hofmann & Weyer, 2021).

Innovationsräume mit Beobachtung: Demgegenüber stehen Sandboxes, die **keine rechtliche Ausnahme gewähren**, sondern als **instrumentelle Beobachtungs- und Lernräume** ausgestaltet sind. Hier werden innovative Produkte oder Prozesse unter bestehenden Normen getestet. Dies geschieht allerdings nur unter besonderer Aufsicht, intensiver Kommunikation mit Behörden und mit vereinfachten Melde- und Feedbackstrukturen (APEC, 2021; Wagner et al., 2021).
Der Vorteil dieses Modells liegt in seiner **geringeren rechtlichen Komplexität**. Gleichzeitig können substanzielle Lerneffekte entstehen. Zu diesen Lerneffekten zählt beispielsweise ein besseres Verständnis technischer Innovationen, der Aufbau interner Kompetenz bei Behörden oder die Erprobung neuer Formen der Risikobewertung (Black & Murray, 2019). Das finnische Digital-Health-Sandbox-Modell ist ein typisches Beispiel: Es operiert vollständig im geltenden Rechtsrahmen, bietet aber strukturierte Dialogformate und begleitende wissenschaftliche Evaluation (Sitra, 2023).
Diese zweite Kategorie ist besonders geeignet für Kontexte mit hohem Rechtsbindungsgrad wie etwa dem Datenschutzrecht oder sicherheitskritischen Sektoren. Gleichzeitig kann sie als

Vorstufe für spätere echte Regulierungsanpassungen dienen, indem sie empirische Evidenz für Reformvorschläge generiert (Gerlach & Lösch, 2020).

Hybride Ansätze und Übergänge: In der Praxis verschwimmen diese beiden Idealtypen zunehmend. Viele Sandboxes starten als reine Beobachtungsräume, entwickeln sich jedoch im Laufe des Prozesses zu Regulierungstestfeldern durch präzedenzbildende Entscheidungen oder informelle Normanpassungen (Bürgin, 2023; Sabel & Zeitlin, 2012). Umgekehrt können auch formal ausnahmesensitive Sandboxes faktisch nur geringe normative Auswirkungen haben, wenn politische Rückkopplung oder rechtliche Umsetzung fehlen.

Für Österreich bedeutet dies, dass bei der Einführung einer Sandbox-Struktur **von Beginn an Klarheit über den intendierten Grad der Regulierungswirkung** bestehen muss und dass diese Entscheidung mit Blick auf Rechtsstaatlichkeit, Wirkungserwartung und politische Akzeptanz **explizit kommuniziert und dokumentiert** wird (OECD, 2021; UNSGSA, 2020).

4.3 ZIELE: TECHNOLOGIEERPROBUNG, POLITIKLERNEN, NORMWEITERENTWICKLUNG

Regulatory Sandboxes sind keine Selbstzweckformate. Ihre Legitimität und Wirkung hängen wesentlich davon ab, ob sie klar definierte, überprüfbare und realistische **Zielsetzungen** verfolgen. In der internationalen Praxis kristallisieren sich drei zentrale Zielkategorien heraus: **Technologieerprobung**, **Politiklernen** und **Normweiterentwicklung** (Black & Lodge, 2022; OECD, 2021). Diese Ziele sind nicht immer trennscharf, überschneiden sich aber funktional und können je nach Sektor oder regulatorischem Umfeld unterschiedlich gewichtet sein.

Technologieerprobung unter Realbedingungen: Ein zentrales Ziel vieler Sandboxes ist es, neue Technologien, Prozesse oder Geschäftsmodelle unter realen Marktbedingungen in einem kontrollierten und begleiteten Umfeld zu testen. Diese Erprobung ermöglicht es, funktionale Eigenschaften, Nutzerverhalten und mögliche Risiken frühzeitig zu erkennen und empirisch zu dokumentieren (Cornelli et al., 2020; Baker McKenzie, 2020). Dies ist insbesondere bei Technologien mit unsicherer gesellschaftlicher oder regulatorischer Bewertung sinnvoll wie etwa bei KI-gestützten Entscheidungsprozessen, datenintensiven Plattformmodellen oder neuartigen Interaktionen zwischen Menschen und Maschine (Fenwick et al., 2024). Die Sandbox dient als Raum zwischen Labor und Markt, als eine Art „transitional space“, der risikoarmes Lernen erlaubt (Wagner et al., 2021). Technologieerprobung kann zudem helfen, technologische Reife (TRL), Schnittstellenprobleme oder Interoperabilitätsfragen zu identifizieren. Dies schafft Grundlagen für künftige Standards oder Zertifizierungsmodelle (Sitra, 2023).

Politiklernen und regulatorische Reflexion: Ein zweites, oft unterschätztes Ziel von Sandboxes ist das **organisierte Lernen von Behörden und politischen Institutionen**. In dynamischen Technologiefeldern stoßen klassische Regulierungsinstrumente oft an ihre Grenzen: Sie sind entweder zu langsam, zu technikfern oder zu fragmentiert (Sabel & Zeitlin, 2012; Hofmann & Weyer, 2021). Sandboxes ermöglichen es Regulierungsbehörden, im engen Austausch mit Unternehmen, Forschungseinrichtungen und ggf. der Zivilgesellschaft **regulationsrelevante Erkenntnisse** über Risikoprofile, Marktpotenziale oder Lücken in bestehenden Regelwerken zu gewinnen (Black & Murray, 2019). Dadurch wird Regulierung nicht nur reaktiv, sondern reflexiv gestaltet: Wissen entsteht im Prozess und nicht vorab. Dieses Politiklernen kann sich auch auf institutionelle Praktiken erstrecken, z. B. durch neue

Formen der Kooperation zwischen Ressorts, ressortübergreifende Datenpools oder neue Evaluationsformate (UNSGSA, 2020; Gerlach & Lösch, 2020).

Normweiterentwicklung und evidenzbasierte Regelgestaltung: Langfristig zielen viele Sandbox-Initiativen darauf ab, Impulse für eine **Anpassung oder Weiterentwicklung des Rechtsrahmens** zu liefern. Die Erprobung unter kontrollierten Bedingungen erlaubt es, konkrete Erfahrungen in die Legislative zurückzuspielen. Dies findet etwa bei der Ausgestaltung technikneutraler Begriffe, beim Umgang mit Innovationsausnahmen oder bei sektorübergreifenden Regelungslücken statt (Lindholm, 2022). Dieser Weg von der Sandbox zum Gesetz ist keineswegs automatisch, sondern erfordert institutionalisierte Feedbackmechanismen. Beispiele hierfür sind Stellungnahmen, wissenschaftliche Gutachten oder begleitende Wirkungsanalysen (OECD, 2021). Ziel ist nicht die Deregulierung per Ausnahme, sondern die Regulierung auf Basis besserer Evidenz.

Erfolgreiche Beispiele zeigen, dass Sandbox-Erfahrungen genutzt wurden, um **gesetzliche Pilotklauseln zu verstetigen**, neue Aufsichtsformate zu etablieren oder sektorale Regeln zu harmonisieren wie etwa im Finanzsektor oder bei Datenzugangsrechten (Bürgin, 2023).

4.4 STRUKTUR- UND DESIGNOPTIONEN

Regulatory Sandboxes sind nicht nur regulatorische Testfelder, sondern auch **institutionelle Innovationsarchitekturen**, deren Wirkung maßgeblich von ihrer Gestaltung abhängt. Die internationale Praxis zeigt: Es reicht nicht aus, ein Sandbox-Modell zu „erlauben“ – es muss **gestaltet, legitimiert und operationalisiert** werden (OECD, 2021; Wagner et al., 2021). In diesem Sinne kommt der strukturellen Ausgestaltung zentrale Bedeutung zu: Sie beeinflusst sowohl die Qualität der Lernprozesse als auch die Chancen auf Verstetigung und Systemwirkung (Bason & Austin, 2021).

Dabei variieren Sandbox-Designs erheblich hinsichtlich ihrer Governance-Formen, rechtlichen Einbettung, Partizipationsarchitektur oder Skalierungsfähigkeit (Black & Lodge, 2022). Diese Unterschiede spiegeln nicht nur technische oder sektorale Eigenheiten wider, sondern auch **unterschiedliche regulatorische Kulturen, Innovationsstrategien und institutionelle Kapazitäten** (Bürgin, 2023).

Governance und Verantwortung

Die Governance-Struktur von Regulatory Sandboxes ist ein **entscheidender Erfolgsfaktor für deren Wirksamkeit, Legitimität und Lerneffizienz**. Während Kapitel 3.3 auf die beteiligten Akteure fokussiert, geht es hier um die Frage, wie institutionelle Verantwortung im Rahmen einer Sandbox **formalisiert und operationalisiert** wird – also: *Wer steuert? Wer kontrolliert? Wer trägt Verantwortung?*

Internationale Erfahrungen zeigen, dass es keine einheitliche Governance-Lösung gibt, wohl aber wiederkehrende **Strukturmuster**, die sich in vier zentralen Dimensionen unterscheiden lassen (Wagner et al., 2021; OECD, 2021).

Trägerschaft und Steuerungseinheit

Zunächst stellt sich die Frage, **wer organisatorisch und rechtlich Träger der Sandbox ist**. Die Bandbreite reicht von ministeriellen Abteilungen (z. B. BM für Digitales in Spanien) über

unabhängige Regulierungsbehörden (z. B. FCA UK) bis hin zu spezialisierten Innovationseinheiten innerhalb der Verwaltung oder in Form von Public-Private-Partnerships (Sitra, 2023; APEC, 2021)[2]. Eine übliche Praxis ist die Einrichtung eines **dedizierten Sandbox-Boards** oder einer **interdisziplinären Koordinierungsstelle**, die das operative Management übernimmt, Antragstellungen prüft, das Monitoring verantwortet und als Schnittstelle zwischen Politik, Verwaltung und Teilnehmern fungiert (Wagner et al., 2021).

Aufsicht, Begleitung und Interaktion

Ein zentrales Element erfolgreicher Governance ist die **aktive, begleitende Aufsicht** durch die zuständige Regulierungsstelle – nicht als Kontrolle im klassischen Sinne, sondern als kooperativer Interaktionsrahmen. Die Behörde agiert hier als „lernende Instanz", die im Austausch mit den Unternehmen regulatorische Handlungsfähigkeit aufbaut (Black & Lodge, 2022; Hofmann & Weyer, 2021). Einige Länder setzen zudem auf **externe Panels oder Beiräte**, die unabhängige Expertise einbringen und eine „Checks & Balances"-Funktion übernehmen – etwa zu ethischen, datenschutzrechtlichen oder gesellschaftlichen Fragen (van den Broek et al., 2021).

Entscheidungslogik und Auswahlverfahren

Die Auswahl von Projekten zur Teilnahme an einer Sandbox erfolgt in der Regel **nicht automatisch**, sondern auf Basis transparenter, mehrstufiger Verfahren. Zentrale Kriterien sind Innovationsgrad, regulatorische Relevanz, erwartbare Lerneffekte und gesellschaftlicher Nutzen (UNSGSA, 2020; Lindholm, 2022).

Wichtig ist, dass diese Verfahren **rechtsstaatlich nachvollziehbar**, fair und inklusiv gestaltet sind. Das ist besonders bedeutend, wenn nur begrenzte Teilnahmeplätze zur Verfügung stehen. In mehreren Ländern wurden hierfür **punktesystembasierte Scoring-Modelle** und **multidisziplinäre Auswahlgremien** etabliert (Bürgin, 2023).

Dokumentation, Evaluation und Exit

Ein häufig unterschätzter Bestandteil von Sandbox-Governance ist die **strukturelle Verankerung von Evaluations- und Exit-Mechanismen**. Dazu zählen:

- **transparente Dokumentationspflichten** für Teilnehmer:innen,
- **laufende Wirkungsanalysen** (z. B. durch externe Forschungseinrichtungen),
- sowie **klare Kriterien für den Abschluss oder Abbruch** eines Projekts (Black & Murray, 2019).

In besonders erfolgreichen Fällen wurden die Ergebnisse von Sandbox-Vorhaben in **öffentlich zugänglichen Abschlussberichten** dokumentiert und enthalten Handlungsempfehlungen für Gesetzgeber und Verwaltung (Sitra, 2023; World Bank, 2020). Ein Beispiel hierfür ist die

[2] Siehe hierzu auch Punkt 3.3.2

ausführliche Dokumentation und Begleitevaluierung der spanischen KI-Sandbox (siehe Fallvignette).

Rechtsrahmen und institutionelle Verankerung

Die rechtliche und institutionelle Verankerung von Regulatory Sandboxes ist zentral für ihre **Rechtsstaatlichkeit, Handlungsfähigkeit und Legitimität**. Sie definiert, *was eine Sandbox darf*, *unter welchen Voraussetzungen sie betrieben werden kann* und *welche institutionellen Ressourcen ihr zur Verfügung stehen* (Lindholm, 2022; OECD, 2021). Unzureichend geregelte oder institutionell isolierte Sandboxes laufen Gefahr, zu informellen Pilotvorhaben ohne rechtliche Wirkung oder systemische Anschlussfähigkeit zu verkommen (Black & Lodge, 2022).

Der Rechtsrahmen von Sandboxes kann von **unverbindlichen Verwaltungserlassen** bis zu **gesetzlich normierten Experimentierklauseln** reichen. Viele frühe Sandbox-Modelle (z. B. UK, Singapur oder Litauen) basierten auf einer **behördlichen Ermessensermächtigung**, bei der geltende Regeln flexibel interpretiert wurden, ohne dass formelle Ausnahmen gesetzlich vorgesehen waren (FCA, 2015; UNSGSA, 2020).

Inzwischen setzt sich zunehmend die Erkenntnis durch, dass strukturell relevante Sandboxes eine **formalisierte rechtliche Grundlage** benötigen – etwa in Form sektorspezifischer Klauseln (z. B. im Finanzmarkt- oder Energierecht), übergreifender „Reallabor-Gesetze“ (wie in Deutschland, vgl. BMWK, 2024) oder horizontaler Regelungen innerhalb eines Digital- oder Innovationsgesetzes (Bürgin, 2023).

Für eine solche gesetzliche Verankerung sprechen vor allem vier Argumente:

1. **Rechtssicherheit für Unternehmen**, insbesondere im Hinblick auf Haftung und Datenverarbeitung,
2. **Rechtsklarheit für Verwaltung und Aufsicht**, insbesondere bei Risikobewertungen,
3. **Verlässlichkeit für politische Rückkopplung** und Gesetzesfolgenabschätzung,
4. **Normative Transparenz gegenüber der Öffentlichkeit**.

Neben der rechtlichen Basis ist entscheidend, wie die Sandbox **institutionell eingebettet** ist, also welche Verbindung sie zu bestehenden Verwaltungsstrukturen, Aufsichtsbehörden oder politischen Entscheidungsprozessen aufweist (Wagner et al., 2021; World Bank, 2020).

Bewährt haben sich Modelle, in denen die Sandbox **weder völlig unabhängig noch vollständig integriert** ist, sondern über eine **semiautonome Struktur mit klaren Koordinationsschnittstellen** verfügt. So kann Innovationsfreiheit mit verwaltungspraktischer Kohärenz verbunden werden (Black & Murray, 2019).

Ein prominentes Beispiel hierfür ist die dänische „Digital Tech Sandbox“, die operativ durch ein Innovation Lab geführt, aber eng an das Wirtschaftsministerium angebunden ist, hier Reporting-Pflichten hat und politiknahe Evaluationen durchführen muss (OECD, 2021). Auch in Estland wurde eine technikoffene Sandbox-Struktur in ein bestehendes e-Governance-Modell eingebettet, um Synergien mit Digitalstrategie, Verwaltungstransformation und Gesetzgebung herzustellen (UNSGSA, 2020).

Für eine nachhaltige Wirkung sollte die institutionelle Verankerung einer Sandbox nicht isoliert erfolgen, sondern **systematisch mit politischen, legislativen und evaluativen Prozessen** verbunden sein. Dies betrifft unter anderem:

- **Zugänge zum Gesetzgebungsprozess** (z. B. via Berichtspflichten oder Vorab-Konsultationen),
- **Verknüpfungen mit Digital- oder Innovationsstrategien**,
- **Institutionalisierte Feedback-Schleifen** (z. B. zu Gesetzesfolgenabschätzungen, Folgenutzung von Ergebnissen, Scoping-Prozesse).

Ohne diese Einbettung besteht das Risiko, dass Sandbox-Ergebnisse **entkoppelt vom Regelsystem bleiben** und damit ihren strategischen Wert verlieren (Gerlach & Lösch, 2020; Hofmann & Weyer, 2021).

Stakeholder-Beteiligung: Staat, Unternehmen, Gesellschaft

Die Gestaltung der Stakeholder-Beteiligung zählt zu den zentralen Designfragen bei der Entwicklung von Regulatory Sandboxes. Im Unterschied zur funktionalen Rollenverteilung (vgl. Kapitel 3.3) steht hier nicht im Fokus, *wer* beteiligt ist, sondern **wie Partizipation inhaltlich, institutionell und prozedural gestaltet werden kann**. Beteiligung wird damit zur strategischen Komponente: Sie beeinflusst nicht nur Legitimität und Akzeptanz, sondern auch Lernfähigkeit und Governance-Qualität (Stirling, 2008; Wagner, Eiden & Müller, 2021).

Internationale Beispiele zeigen, dass sich Beteiligungsarchitekturen entlang dreier Achsen unterscheiden lassen: **Reichweite der Beteiligung**, **Form der Interaktion** und **Stellung im Entscheidungsprozess** (OECD, 2021; van den Broek et al., 2021).

Staatliche Stellen sind integraler Bestandteil jeder Sandbox. Gestalterisch entscheidend ist jedoch, ob sie lediglich als Aufsichtsinstanz agieren, als koordinierende Kraft oder als **aktiv gestaltender Governance-Akteur**. In neueren Sandbox-Designs sind ministerielle oder behördliche Stellen nicht nur für die Genehmigung zuständig, sondern aktiv in die Prozessbegleitung und Ergebnisverwertung eingebunden (APEC, 2021; OECD, 2021).

In Finnland etwa ist die Beteiligung mehrerer Verwaltungsressorts in der operativen Steuerung ausdrücklich vorgesehen. Es handelt sich hierbei um ein „multi-agency governance model“, das sektorübergreifende Abstimmung und Kompetenzbündelung ermöglicht (Sitra, 2023).

Private Unternehmen sind in der Regel die unmittelbaren Teilnehmer an Sandbox-Prozessen. Doch auch im Designprozess selbst ist ihre frühe und transparente Einbindung zentral. Die Einbindung findet etwa über **Branchenanhörungen, Auswahlbeiräte oder dialogische Vorbereitungsformate** statt (Floridi et al., 2018; UNSGSA, 2020).

Eine wichtige Designentscheidung betrifft die **Zugangsstruktur**: Sind Sandboxes exklusiv für innovative Start-ups geöffnet oder auch für etablierte Akteure? Offenheit kann zu breiterer Wirkung führen, verlangt aber differenzierte Unterstützungsstrukturen, damit kleinere Akteure nicht systematisch benachteiligt werden (Bürgin, 2023).

Eine zunehmend relevante Perspektive ist die **aktive Einbindung zivilgesellschaftlicher und wissenschaftlicher Akteure**. Diese Beteiligung erweitert die Perspektiven auf gesellschaftliche, ethische oder ökologische Aspekte. Gerade im Bereich KI berücksichtigen

sie Datenschutz, algorithmische Transparenz oder Zugänglichkeit und können entsprechend Druck ausüben (van den Broek et al., 2021; Wagner et al., 2021).

Beteiligungstypen: Von Konsultation bis Co-Kreation

Je nach Tiefe der Einbindung lassen sich verschiedene **Beteiligungsformen** unterscheiden (siehe Tabelle 4):

Tabelle 4: Beteiligungsformen bei Sandboxes

Typ	Beschreibung	Rolle
Konsultativ	Rückmeldung auf vorgegebene Entwürfe	Informationsgewinn
Deliberativ	Dialogischer Austausch auf Augenhöhe	Perspektivenerweiterung
Co-kreativ	Gemeinsame Entwicklung von Zielen und Kriterien	Mitgestaltung

Quelle: Eigene Zusammenstellung

Während viele Sandboxes bislang vor allem auf konsultative Formate setzen, zeigt sich ein Trend hin zu **deliberativen und co-kreativen Ansätzen**, insbesondere bei komplexen Themen wie Gesundheitsdaten oder automatisierter Entscheidungsfindung (Felt, 2017; Stirling, 2008). Partizipation ist nur dann wirksam, wenn sie durch **Transparenz flankiert** wird. Durch öffentlich zugängliche Ausschreibungen, nachvollziehbare Auswahlprozesse, sowie verständlich aufbereitete, aggregierte Berichte und Evaluationsergebnisse von Sandbox-Projekten kann Transparenz gewährleistet werden (World Bank, 2020; Wagner et al., 2021). Gerade bei heiklen Technologien entscheidet sich die gesellschaftliche Tragfähigkeit regulatorischer Experimente häufig mit der Frage, ob Beteiligung *sichtbar, nachvollziehbar und ernstgemeint* ist.

Skalierungsperspektive: Vom Pilotprojekt zur Regelintegration

Regulatory Sandboxes entfalten ihren strukturellen Wert nur dann, wenn ihre Ergebnisse über den konkreten Testfall hinauswirken. Der entscheidende Schritt liegt in der **Überführung erfolgreicher Experimente in den regulären Rechts- und Verwaltungsrahmen**. Dieser Übergang von der temporären Ausnahme zum dauerhaften Systemelement ist jedoch selten automatisiert und erfordert **institutionell abgesicherte Skalierungsprozesse** (Bason & Austin, 2021; Gerlach & Lösch, 2020).

Viele Sandbox-Projekte erzeugen interessante Einzelerkenntnisse, scheitern jedoch an der **systemischen Anschlussfähigkeit**. Das liegt häufig an fehlenden Feedbackkanälen zwischen Sandbox-Verantwortlichen und Legislativ- oder Verwaltungsprozessen (Willems & Van Dooren, 2021). Verstetigung erfordert daher frühzeitig definierte **„Transferpfade“**, zum Beispiel in Form von normativen Empfehlungen, standardisierbaren Verfahren oder Anstößen für Rechtsfortbildung (OECD, 2021; van Twist & Scherpenisse, 2011). Dabei geht es nicht nur um die technische oder rechtliche Verstetigung, sondern auch um den **kulturellen Transfer** von Innovationsbereitschaft und Adaptionsfähigkeit in Verwaltungen (Ansell et al., 2021).

Aus internationaler Perspektive lassen sich mehrere Bedingungen identifizieren, die eine erfolgreiche Skalierung fördern:

- **Frühzeitige Zielklärung:** Sandbox-Formate mit explizit definiertem Skalierungshorizont (z. B. „if-then"-Kriterien) erzielen häufiger systemische Wirkung (World Bank, 2020).
- **Verrechtlichung von Ergebnissen:** Einbindung der Legislative, etwa über Berichtspflichten, Petitionsverfahren oder Verordnungsermächtigungen (Lindholm, 2022).
- **Evaluation mit Reformfokus:** Wirkungsanalysen sollten nicht nur Projektziele bewerten, sondern gezielt **gesetzgeberisch nutzbare Evidenz** generieren (Jansen, 2022).
- **Verwaltungsfähige Anschlussformate:** Ergebnisse müssen in Regelverfahren überführbar sein, etwa durch Standardisierung, Musterverträge oder Umsetzungshandbücher (Gerlach & Lösch, 2020).

Ein zentrales Risiko besteht im sogenannten **„Pilotismus"** – der Tendenz, Innovation auf ewige Pilotphasen zu beschränken, ohne strukturelle Reformen umzusetzen (Jasanoff, 2018; Felt, 2017). Dieses Phänomen entsteht oft dann, wenn Sandboxes **politisch als Innovationsalibi** fungieren, aber keine institutionelle Bereitschaft zur Regelintegration besteht. Hinzu kommt das Problem der **Skalierungsfragmentierung**: Wenn unterschiedliche Behörden, Ressorts oder Regionen parallele Sandbox-Erkenntnisse ohne horizontale Koordination generieren, droht regulatorische Inkonsistenz (Gaskell et al., 2022).

Statt auf spontane Verstetigung zu hoffen, empfehlen sich **strukturierte Skalierungsarchitekturen**:

- **Policy Windows definieren:** z. B. Verknüpfung mit Legislaturzyklen oder Strategieprozessen.
- **Integration in Wirkungsfolgenabschätzung:** gezielte Verwertung in Regulierungsfolgenanalysen oder Normprüfverfahren (OECD, 2021).
- **Übergabemechanismen etablieren:** z. B. institutionelle Übergabe an Standardisierungsgremien, Fachministerien oder Aufsichtsbehörden.
- **Institutionelle Gedächtnisformate schaffen:** wie Wissensdatenbanken, Lernberichte oder Erfahrungsworkshops (Willems & Van Dooren, 2021; Wagner et al., 2021).

5 Regulatory Sandboxes in der EU

5.1 EINLEITUNG

Die Einführung regulatorischer Sandboxes in der Europäischen Union ist Ausdruck eines strategischen Wandels hin zu einem neuen, innovationsfreundlichen, evidenzbasierten und zugleich grundrechtskonformen Regulierungsrahmen. Dabei spielt die Europäische Kommission eine zentrale Rolle bei der Initiierung und normativen Rahmensetzung solcher Instrumente. In diesem Kapitel erfolgt sowohl eine Diskussion der politischen und rechtlichen Grundlagen als auch von Designprinzipien und der institutionellen Ausgestaltung von Sandboxes. In Ergänzung dazu werden Pilotprojekte und Good Practices in der EU und die Bedeutung des Instruments für den europäischen Rechts- und Innovationsraum betrachtet.

5.2 POLITISCHE UND RECHTLICHE GRUNDLAGEN

Die Einführung regulatorischer Sandboxes in der Europäischen Union ist Ausdruck eines strategischen Wandels hin zu einem neuen, innovationsfreundlichen, evidenzbasierten und zugleich grundrechtskonformen Regulierungsrahmen. Dabei spielt die Europäische Kommission eine zentrale Rolle bei der Initiierung und normativen Rahmensetzung solcher Instrumente. Bereits in den Schlussfolgerungen des Rates der Europäischen Union vom November 2020 wurde festgehalten, dass regulatorische Sandboxes und sogenannte „Experimentierklauseln“ zentrale Elemente eines zukunftsfähigen regulatorischen Ökosystems darstellen. Ziel ist es, „*disruptive Innovationen kontrolliert zu erproben*, *regulatorisches Lernen zu fördern* und gleichzeitig *technologische Souveränität* sowie eine *innovationsförderliche Wettbewerbsordnung sicherzustellen“* (Rat der Europäischen Union, 2020).

EU-weite Rahmensetzung: Die strategische Verankerung von Sandboxes ergibt sich aus einer Reihe politischer Programme, etwa der EU-Digitalstrategie, der SME Strategy for a Sustainable and Digital Europe (European Commission, 2020) und der europäischen KI-Verordnung, die als erstes supranationales Gesetz explizit regulatorische Sandboxes vorsieht. Die europäische KI-Verordnung verpflichtet die Mitgliedstaaten in Art. 57 ff. zur Einrichtung mindestens einer koordinierten KI-Sandbox bis spätestens 2. August 2026, (Europäische Kommission, 2021a). Dabei sollen Start-ups, KMU sowie öffentliche Stellen gleichermaßen von einem klar definierten Rechtsrahmen profitieren.
Gleichzeitig verweist die „Better Regulation Toolbox“ der Kommission (Tool #21) auf die Rolle von Sandboxes als Teil dynamischer Regulierung, die unter dem „Innovation Principle“ insbesondere im digitalen Kontext gestärkt werden sollen (European Commission, 2021b). Die Anwendung solcher experimenteller Regulierungsformen wird dabei als notwendige Reaktion auf technologische Komplexität und regulatorische Unsicherheit verstanden.

Rechtsgrundlage und Verordnungen: Die rechtliche Kodifikation von KI-Sandboxes erfolgt primär durch die europäische KI-Verordnung (Art. 57 bis 62), die einen risikobasierten und sektorenübergreifenden Rahmen für KI-Anwendungen schafft. Im Fokus stehen insbesondere sogenannte Hochrisiko-KI-Systeme, für die im Rahmen einer Sandbox vorübergehende Abweichungen von bestimmten Rechtsnormen erlaubt werden können, ohne jedoch grundlegende Schutzgüter wie Datenschutz, Verbraucherschutz oder Diskriminierungsfreiheit zu unterlaufen (European Commission, 2021a).
Die Sandboxes fungieren in diesem Kontext als „regulierte Ausnahmen“ im Sinne strukturierter Experimentierräume. Dabei betont die europäische KI-Verordnung ausdrücklich die Einhaltung

von Art. 16 und Art. 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), um sowohl Grundrechte zu schützen als auch den Binnenmarkt zu fördern (European Commission, 2021a).

EU-Durchführungsrechtsakte und subsidiäre Umsetzungsfreiräume: Die praktische Implementierung obliegt den Mitgliedstaaten, wobei die Kommission Durchführungsrechtsakte zur Festlegung der detaillierten Modalitäten für die Einrichtung, Entwicklung, Durchführung, den Betrieb und die Beaufsichtigung der KI Regulatory Sandboxes erlassen wird. Der Entwurf der Durchführungsverordnung der Kommission zu KI-Regulierungssandkästen legt den operativen Rahmen für die Einrichtung, Verwaltung und Überwachung gemäß der EU-KI-VO fest. Zu den wichtigsten Elementen des Verordnungsentwurfs gehören die Festlegung der Teilnahmebedingungen, wobei KMU und Start-ups, die kostenlosen Zugang zu den Sandboxes erhalten, Vorrang eingeräumt wird, während größere Unternehmen möglicherweise mit Kostendeckungsgebühren konfrontiert werden. Der Entwurf enthält detaillierte Angaben zum Antrags- und Auswahlverfahren und beschränkt die Teilnahmeberechtigung auf KI-Systeme, die noch nicht auf dem Markt sind oder derzeit erheblich modifiziert werden. Die zuständigen Behörden müssen sich mit den Teilnehmern auf einen detaillierten Sandbox-Plan einigen, der Ziele, Zeitpläne, Methoden und Maßnahmen zur Risikominderung umfasst. Die Behörden sind verpflichtet, Sandbox-Aktivitäten zu dokumentieren, Compliance-Tools zu veröffentlichen, einen schriftlichen Nachweis über die Teilnahme bei Beendigung vorzulegen und Jahresberichte zu erstellen, um Transparenz und regulatorisches Lernen zu fördern. Der Entwurf sieht auch die Aussetzung von Projekten vor, die Bedenken hinsichtlich der Sicherheit oder der Grundrechte aufwerfen. Die Teilnahme befreit die Anbieter nicht von der Haftung für Schäden, die durch KI-Experimente verursacht werden, schützt sie jedoch vor Verwaltungsstrafen, wenn sie in gutem Glauben gemäß den Sandbox-Richtlinien handeln.

Eine vergleichende Analyse zeigt, dass zwölf Mitgliedstaaten (darunter AT, BE, DK, ES, FR, IT) bereits explizite Rechtsgrundlagen für Sandboxes geschaffen haben (entweder in Form von Rahmengesetzen oder durch Experimentierklauseln), während sieben weitere (z. B. DE, FI, PL) entsprechende Gesetzesvorhaben prüfen (Fraunhofer ISI & Trinomics, 2023). Die rechtliche Voraussetzung für die Schaffung von Sandboxes ist dabei in vielen Fällen eine sektorale Gesetzesnovelle oder eine delegierte Rechtsverordnung. Die Harmonisierung wird auf EU-Ebene durch Rahmenbedingungen in der europäischen KI-Verordnung unterstützt, gleichzeitig bleibt Raum für nationale Diversität im Design, der Zielgruppe und den Testbereichen der Sandboxes.

Es lässt sich beobachten, dass regulatorische Sandboxes innerhalb der EU eine hybride Struktur aufweisen: Sie sind gleichzeitig ein zentral gelenktes Innovationsinstrument (Top-down) und ein Ermöglichungsrahmen für nationale Regulierungsinnovationen (Bottom-up). Diese Doppelrolle erfordert eine koordinierte europäische Governance-Struktur, wie sie etwa mit dem „AI Board“ im Rahmen der europäischen KI-Verordnung angestrebt wird. Das AI Board in der europäischen KI-Verordnung ist ein Gremium, das sich aus einem Vertreter jedes EU-Mitgliedstaats zusammensetzt und dazu dient, die Kohärenz und Koordinierung der Umsetzung der europäischen KI-Verordnung zwischen den nationalen zuständigen Behörden sicherzustellen.

5.3 DESIGNPRINZIPIEN UND INSTITUTIONELLE AUSGESTALTUNG

Die Gestaltung regulatorischer Sandboxes in der EU folgt keinem einheitlichen Modell, sondern kann eine Vielzahl von Ausprägungen annehmen. Dies reflektiert sowohl die sektorale Vielfalt als auch die unterschiedliche regulatorische Kultur in den Mitgliedstaaten. Gleichwohl lassen sich zentrale Gestaltungsprinzipien und institutionelle Grundmuster identifizieren, die für die EU-weit kohärente Ausgestaltung dieser Instrumente von Relevanz sind.

Formate, Funktionen und Governance-Modelle: Regulatorische Sandboxes lassen sich grob in zwei Typen unterscheiden: **policy-oriented** und **innovator-oriented** Sandboxes (ETIP SNET, 2023). Erstere werden von Behörden initiiert, um gezielte politische Ziele wie etwa die Förderung von Nachhaltigkeit oder Digitalisierung zu erreichen. Letztere hingegen entstehen durch Nachfrage von Unternehmen, insbesondere Start-ups, um neue Technologien schneller zur Marktreife zu bringen.

Auch in der **institutionellen Verankerung** bestehen Unterschiede. Einige Länder setzen auf **zentralisierte Sandbox-Strukturen** (z. B. Spanien, Litauen), während andere **dezentrale, sektorale Formate** bevorzugen (z. B. Deutschland mit Energie- und Mobilitäts-Sandboxes). Die Organisation erfolgt entweder über bereits bestehende Regulierungsbehörden, wie Datenschutz- oder Wettbewerbsbehörden, oder über neu geschaffene Governance-Einheiten, etwa beim spanischen KI-Sandbox-Pilotprojekt, das mit zwei interministeriellen Fokusgruppen (FG1/FG2) operiert (Gobierno de España, 2023).

Darüber hinaus werden unterschiedliche regulatorische Rollen wahrgenommen: von bloßer „Beobachtung“ (supervisory by design) über „Mitgestaltung“ (co-regulatory) bis hin zu „temporären regulatorischen Ausnahmen“ (regulatory relief). Dabei ist stets die Balance zwischen Innovationsoffenheit und regulatorischem Schutzbedürfnis zentral.

Teilnahmekriterien, Rechtsklarheit und Transparenz: Für die Aufnahme in eine Sandbox gelten meist klar definierte Zugangskriterien. Diese umfassen typischerweise: Innovationsgrad des Vorhabens, potenzielle gesellschaftliche Relevanz, regulatorischer Klärungsbedarf sowie Durchführbarkeit und Risikobeherrschbarkeit im Sandbox-Kontext (OECD, 2023; World Bank, 2020).
Ein zentrales Gestaltungsmerkmal ist die befristete Natur der Teilnahme. Die **Laufzeiten** variieren meist **zwischen sechs Monaten und zwei Jahren** (ETIP SNET, 2023), wobei Verlängerungen möglich sind. In diesem Zeitraum wird der regulatorische Rahmen „probeweise“ angepasst, etwa durch Erlass einer Ausnahme. Entscheidend ist, dass dies in einem formalisierten Verfahren erfolgt, etwa über öffentlich dokumentierte Bedingungen und Berichtspflichten, um Transparenz und Revisionsfähigkeit zu gewährleisten (UNSGSA & CCAF, 2019).
Die Transparenz der Teilnahmebedingungen sowie der Ergebnisse der Sandbox-Projekte ist essenziell, nicht nur für das Vertrauen der Marktteilnehmer, sondern auch zur Legitimation des Instruments gegenüber der Öffentlichkeit und dem Gesetzgeber.

5.4 PILOTPROJEKTE UND GOOD PRACTICES IN DER EU

Innerhalb der EU sind in den vergangenen Jahren mehrere exemplarische Sandbox-Initiativen auf nationaler sowie supranationaler Ebene realisiert worden. Diese Pilotprojekte dienen als empirische Grundlage für zukünftige europäische Koordinationsmechanismen und illustrieren verschiedene sektorale Anwendungsbereiche, etwa im Bereich künstliche Intelligenz, Energie,

Finanzen oder Blockchain. Die Projekte sind in Zielsetzung, Design und Implementierungsgrad unterschiedlich, liefern aber wertvolle Einsichten hinsichtlich Machbarkeit, Governance, Erfolgsfaktoren und Transferpotenzial.

Neben nationalen Initiativen (z. B. Spanien oder Luxemburg[3]) existieren sektorale EU-weite Sandbox-Projekte, etwa im Energiebereich. Hierzu zählt das Forschungsprogramm „EnTEC – Energy Transition Expertise Centre", das im Auftrag von DG ENER 2023 eine vergleichende Analyse regulatorischer Bedingungen in 19 Mitgliedstaaten vorlegte. Die Studie zeigt auf, dass insbesondere im Energiesektor ein erheblicher Bedarf an rechtlich abgesicherten Experimentierräumen besteht, u. a. zur Förderung dezentraler Versorgung, Smart Grids und innovativer Speichertechnologien (Fraunhofer ISI & Trinomics, 2023).

Ein weiteres Format ist die **ETIP SNET** Sandbox-Plattform, welche Best Practices im Energienetzbereich sammelt und der EU-Kommission Empfehlungen für einheitliche Standards und Erfolgskriterien vorlegt. Ein besonderer Fokus liegt hier auf Anreizmodellen, Dateninteroperabilität und Verbraucherintegration (ETIP SNET, 2023).

Auch im Bereich der Blockchain-Technologien fördert die Europäische Kommission eine grenzüberschreitende Sandbox („EU Blockchain Regulatory Sandbox"), die insbesondere der Evaluierung rechtlicher Anforderungen an DLT-basierte Geschäftsmodelle dient und eine enge Abstimmung mit den jeweiligen nationalen Behörden vorsieht (European Commission, 2023b).

Innerhalb der EU zeigen sich unterschiedliche nationale Ausprägungen regulatorischer Sandboxes, sowohl inhaltlich als auch institutionell. Während beispielsweise Litauen ein besonders unternehmensnahes, niederschwelliges Modell für FinTechs etabliert hat, verfolgt Deutschland einen stärker wissenschaftlich-technisch orientierten Ansatz im Energiebereich (z. B. „Forschungsprogramm Schaufenster intelligente Energie – Digitale Agenda für die Energiewende" oder „Reallabore der Energiewende").

Österreich implementierte mit seiner FMA-Sandbox ein formalisiertes Zulassungsverfahren für FinTechs, das auf enge regulatorische Begleitung und gezielte Marktintegration abzielt (FMA, 2023). Frankreich wiederum nutzt sektorübergreifende Innovation Hubs, um regulatorische Fragen frühzeitig bilateral zu klären.

Die Vielzahl an Ansätzen veranschaulicht das Innovationspotenzial, macht aber auch deutlich, dass ohne EU-weite Mindeststandards eine Fragmentierung droht. Die Förderung von Koordinationsinstrumenten wie etwa über den Europäischen Ausschuss für künstliche Intelligenz (AI Board) erscheint daher essenziell, um Lerneffekte zu bündeln und Rechtsunsicherheit zu minimieren.

5.5 BEDEUTUNG FÜR DEN EUROPÄISCHEN RECHTS- UND INNOVATIONSRAUM

Die Etablierung regulatorischer Sandboxes markiert einen bedeutenden Paradigmenwechsel in der europäischen Innovations- und Regulierungspolitik. Sie stehen exemplarisch für den Übergang von statischen Rechtsrahmen hin zu flexiblen, lernorientierten Steuerungsmodellen, die auf technologische Dynamiken ebenso reagieren wie auf die Notwendigkeit, gesellschaftliche Werte – insbesondere Grundrechte, Nachhaltigkeit und Datenschutz –

[3] Eine detaillierte Darstellung der Projekte findet sich im Anhang 1.

abzusichern. In diesem Kontext entfalten regulatorische Sandboxes sowohl **innenpolitische Steuerungswirkungen** als auch **außenpolitische Hebelwirkungen** in Richtung globaler Normsetzung.

EU als Standardsetzer – globaler Einfluss

Die Europäische Union versteht sich zunehmend als „global regulatory power" (Bradford, 2020), insbesondere in digital- und innovationspolitischen Feldern. Mit der verrechtlichten Verankerung regulatorischer Sandboxes in der europäischen KI-Verordnung setzt die EU weltweit ein Signal: Sie gestaltet Innovation nicht nur technologisch, sondern auch rechtlich.

Das zeigt sich exemplarisch daran, dass sich andere internationale Organisationen wie die OECD, die Weltbank oder der Sonderbeauftragte des Generalsekretärs der Vereinten Nationen für inklusive Finanzdienstleistungen (UNSGSA) explizit auf europäische Erfahrungen und Modelle beziehen (OECD, 2023; World Bank, 2020; UNSGSA & CCAF, 2019). So betont die OECD die Notwendigkeit international interoperabler Sandbox-Standards, um Fragmentierung und regulatorisches Arbitrage-Verhalten zu verhindern.

Die EU-eigenen Initiativen wie die geplante „AI-Sandbox-Interoperabilität" oder die „Blockchain-Sandbox" sollen künftig auch Drittstaaten einbinden und über technische Äquivalenzabkommen eine regelbasierte Innovationskooperation ermöglichen (OECD, 2023, S. 20). Hier lässt sich die Tendenz zur Ausweitung über die Grenzen der Europäischen Union hinweg erkennen.

Risiken von Fragmentierung vs. Chancen der Koordinierung

Trotz des supranationalen Rahmens verbleibt ein erheblicher Handlungsspielraum auf nationaler Ebene. Diese Flexibilität ist demokratietheoretisch wünschenswert, birgt jedoch das Risiko eines regulatorischen Fleckenteppichs. Das gilt insbesondere, wenn divergente Praxisformen ohne Rückkopplung zur EU-Ebene implementiert werden (Fraunhofer ISI & Trinomics, 2023).

Um dem zu begegnen, sieht die europäische KI-Verordnung die Einrichtung eines „European Artificial Intelligence Board" vor, das die Harmonisierung, Evaluation und Weiterentwicklung nationaler Sandbox-Ansätze koordinieren soll (European Commission, 2021). Dabei geht es nicht nur um formale Mindeststandards, sondern auch um eine europäische Feedback-Architektur: Sandbox-Ergebnisse sollen systematisch zur Evidenzgewinnung für Gesetzgebungsprozesse genutzt werden. Es handelt sich um ein zentrales Element „smarter Regulierung" (Zetzsche et al., 2017).

Ferner zeigen Pilotprojekte wie das spanische KI-Sandbox-Modell, dass durch strukturierte Kooperation zwischen Mitgliedstaaten und Kommission wertvolle Lernprozesse generiert werden können, die über technische Details hinaus auch Vertrauen in das europäische Innovationsmodell stärken (Gobierno de España, 2023). Es bleibt abzuwarten, ob verstärkt auf derartige Beteiligungsformate gesetzt wird.

6 Der österreichische Kontext

6.1 EINLEITUNG

Angesichts der bevorstehenden Umsetzung der **europäischen KI-Verordnung** ergibt sich jedoch ein konkreter politischer Handlungsbedarf: Die Artikel 57 bis 59 der KI-VO sehen verpflichtende nationale KI-Sandboxes vor, um insbesondere KMU bei der Entwicklung konformer KI-Systeme zu unterstützen (European Commission, 2023). Österreich steht somit vor der Aufgabe, ein entsprechendes institutionelles Modell zu entwickeln. Dabei zeigen internationale Beispiele – etwa Frankreichs „AI for Health"-Sandbox oder die spanische „Sandbox Financiera" –, wie nationale Sandbox-Modelle regulatorische Lernprozesse stimulieren können, ohne rechtsstaatliche Standards aufzuweichen (OECD, 2021; European Commission, 2023).

6.2 RECHTLICHE RAHMENBEDINGUNGEN UND INSTITUTIONELLE AUSGANGSLAGE

Österreich verfügt bislang über **keine Rahmengesetzgebung**, welche die Einrichtung von Regulatory Sandboxes oder deren Durchführung strukturell und sektorübergreifend absichert. Es existieren in verschiedenen Rechtsbereichen aber einzelne Normen, Ermessensspielräume oder Förderinstrumente, diese sind jedoch **auf spezifische sektorielle Gegebenheiten** (z. B. autonomes Fahren, lokale Energiemärkte) **ausgelegt**. Auch institutionell fehlt es an einer übergreifenden Koordination, die adaptive Regulierung als strategisches Steuerungsinstrument etablieren könnte. Dies verunmöglicht nicht prinzipiell die Einführung von z. B. sektoralen Sandboxes, könnte aber in bestimmten Bereichen für Schwierigkeiten sorgen.

Das **Datenschutzgesetz (DSG)**, BGBl. I Nr. 165/1999 idgF, ergänzt die unmittelbar anwendbare **Datenschutz-Grundverordnung (DSGVO)** (VO [EU] 2016/679). Beide zusammen regeln die Zulässigkeit der Verarbeitung personenbezogener Daten in Österreich. Die DSGVO kennt keine explizite Öffnungsklausel für regulatorisches Experimentieren; selbst die **Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO** erlaubt lediglich risikobasierte Evaluierung, jedoch **keine formale Ausnahme vom geltenden Schutzstandard**.

Der österreichische Gesetzgeber hat von den in Art. 6 Abs. 2 und 3 DSGVO vorgesehenen Öffnungsklauseln nur eingeschränkt Gebrauch gemacht. So erlaubt etwa § 7 DSG i. V. m. § 1 DSG im öffentlichen Interesse Datenverarbeitungen bei wissenschaftlicher Forschung – doch dies gilt **nicht für Sandbox-Szenarien im privatwirtschaftlichen Kontext**. Somit stellt der Datenschutz derzeit eine substanzielle Hürde für Sandbox-Vorhaben dar, insbesondere wenn KI-Systeme mit sensiblen Daten getestet werden sollen (Mantelero, 2022; EDPB, 2020).

Das **AVG 1991** (BGBl. Nr. 51/1991 idgF) ist das zentrale Regelwerk für verwaltungsrechtliche Verfahren in Österreich. Es basiert auf den Prinzipien der **Gesetzesbindung, Rechtsstaatlichkeit und Gleichbehandlung** (vgl. §§ 1 und 7 AVG). Die Behörden sind verpflichtet, Entscheidungen ausschließlich auf Grundlage des geltenden Rechts zu treffen.

Eine behördliche **Experimentierpraxis ohne formale gesetzliche Grundlage** ist daher nicht möglich. Auch § 57 AVG (Selbstbindung der Verwaltung) erlaubt keine rechtsverbindlichen Ausnahmen im Sinne eines „Testregimes". Die Anwendung von Ermessen (§ 5 AVG) unterliegt

der Nachvollziehbarkeit und Bindung an den Zweck des Gesetzes – und kann **nicht als Hebel für regulatorische Flexibilität** in Sandbox-Vorhaben interpretiert werden (Lindholm, 2022).

Im Gegensatz zu Ländern wie Deutschland oder Estland verfügt Österreich derzeit über **keine gesetzlich verankerten Experimentierklauseln**, die sektorübergreifend den Betrieb regulatorischer Reallabore oder Sandboxes ermöglichen würden. Weder im **Bundes-Verfassungsgesetz (B-VG)** noch in einfachen Gesetzen (z. B. E-Government-Gesetz, Digitalsteuergesetz, Forschungsorganisationsgesetz) sind temporäre Abweichungen vom geltenden Recht zu Zwecken der Innovation ausdrücklich vorgesehen. Auch die aktuelle **„Strategie für Forschung, Technologie und Innovation 2030“** (BMBWF/BMK 2021) erwähnt regulatorisches Testen oder Sandboxes nicht. Damit fehlt eine **strategische und gesetzgeberische Verankerung** im österreichischen Innovationssystem.

Das **aktuelle Regierungsprogramm** spricht Sandboxes in den Bereichen Arbeitszeit, Anerkennung von Arbeit in den Tagesstrukturen für Menschen mit Behinderungen, Digitalisierung für Unternehmen und in der Forschung und Entwicklung explizit als Themen an. Darüber hinaus gibt es **branchenspezifische Ausnahmen** und Pilotrahmen, auf denen aufgebaut werden kann. Beispielsweise wurden im Energiebereich im Rahmen des Erneuerbaren-Ausbau-Gesetzespaket befristete Ausnahmen von Systemnutzungsentgelten für Forschungs- und Demonstrationsprojekte (§ 58a ElWOG, § 78a GWG) verankert. Auch die Regulatory Sandbox im FinTech-Bereich, die seit 2020 existiert und von der Finanzmarktaufsicht angeboten wird, ist eine derartige branchenspezifische Lösung.

Die Zuständigkeit für innovations- und digitalisierungsbezogene Regulierungsfragen ist gemäß Bundesministeriengesetz (BMG) u. a. auf folgende Ressorts verteilt:

- **Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET)** – zuständig für Wirtschafts- und Standortfragen,
- **Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)** – zuständig für arbeitsmarktpolitische Themen,
- **Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)** – zuständig für Forschungs- und Innovationspolitik,
- **Bundeskanzleramt (BKA)** – die Sektion VII (Digitalisierung und E-Government) ist federführend zuständig für KI Regulatory Sandboxes,
- **Bundesministerium für Frauen, Wissenschaft und Forschung (BMFWF)** – zuständig für Wissenschaftskoordination und -förderung und strategische Entwicklung des österreichischen Forschungs- und Hochschulsektors; Digitalisierung im Wissenschaftsbereich,
- **Bundesministerium für Bildung –** zuständig für KI im österreichischen Schulwesen.

Diese Verteilung führt zu komplexer Koordination. Eine Entscheidung, wo Regulatory Sandboxes in Österreich angesiedelt sein werden, wurde noch nicht getroffen.

Vergleich: Reallabore-Gesetz in Deutschland

Deutschland hat mit dem **Reallabore-Gesetz** (BMWK, 2024) einen sektorübergreifenden gesetzlichen Rahmen für befristete Abweichungen vom geltenden Recht zum Zweck der Innovation geschaffen. Das Gesetz verpflichtet zu Beteiligung, Evaluation und Rückkopplung in den Gesetzgebungsprozess. Ein solches Modell gibt es im österreichischen Rechtsrahmen bislang nicht (Bürgin, 2023), weswegen bisherige Sandbox-Modelle innerhalb des bestehenden Rechtsrahmens oder durch sektorale Adaptierungen umgesetzt werden mussten. Ein solches allgemeines Reallabor-Gesetz kann zwar hilfreich für den Aufbau einer nationalen KI Regulatory Sandbox wirken, ist aber keine notwendige oder verpflichtende Grundlage für die Einrichtung von Sandboxes in Österreich.

6.3 BISHERIGE PILOTINITIATIVEN UND FORMATE

In Österreich wurden in den letzten Jahren verschiedene Initiativen gestartet, die als mit Regulatory Sandboxes vergleichbare Formate betrachtet werden können. Diese Projekte bieten wertvolle Erkenntnisse für die Entwicklung zukünftiger regulatorischer Experimentierräume.

Die **Regulatory Sandbox der Finanzmarktaufsicht Österreich** (FMA) wurde am 1. September 2020 eingeführt, um innovativen FinTech-Geschäftsmodellen den Weg zur Aufsicht und Marktreife zu erleichtern (§ 23a FMABG). Dabei dürfen Unternehmen ihr Geschäftsmodell in einer Testphase mit einer vorläufigen Lizenz unter enger Aufsicht der FMA erproben, ohne dass dabei die hohen Aufsichtsstandards gesenkt werden. Die Teilnahme setzt eine positive Bewertung durch den Regulatory Sandbox Beirat voraus, der volkswirtschaftliches Interesse, Innovationsgrad und Testreife prüft. Ziel ist es, durch gezielten Support und enge Betreuung junge FinTechs und etablierte Unternehmen bei der regulatorischen Marktreife zu unterstützen. Erfolgreiche Sandboxteilnehmer verlassen die Sandbox und treten in die reguläre Aufsicht ein, wodurch Innovationen die Finanzmarktaufsicht bereichern (FMA 2020). Die FMA versteht das Modell als „kooperativ und prüfend“ – mit Fokus auf frühes regulatorisches Lernen. Bis Ende 2023 nahmen acht Unternehmen teil; erste Sandbox-Teilnehmer konnten bereits Zulassungen bzw. Konzessionen erhalten, was zeigt, dass die Sandbox den Weg zur regulären Marktreife beschleunigt.

Energie.Frei.Raum – Regulatory Sandbox im Energiebereich: Mit der Novellierung des Elektrizitätswirtschafts- und -organisationsgesetzes (ElWOG 2010) und des Gaswirtschaftsgesetzes (GWG 2011) im Jahr 2021 wurden in Österreich gesetzliche Grundlagen für Regulatory Sandboxes im Energiebereich geschaffen. Diese ermöglichen es, im Rahmen von Forschungs- und Demonstrationsprojekten temporäre Ausnahmen von bestimmten regulatorischen Vorgaben zu erhalten, insbesondere im Bereich der Systemnutzungsentgelte. Ziel ist es, innovative Technologien und Geschäftsmodelle unter realen Bedingungen zu testen und deren Auswirkungen auf das Energiesystem zu evaluieren (Energieinstitut an der Johannes Kepler Universität Linz, 2024). Das vormals vom Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (jetzt BMIMI) initiierte Programm „Energie.Frei.Raum" dient als Plattform für solche Experimente. Die FFG übernahm dabei die Rolle einer begleitenden Koordinations- und Förderstruktur und schuf ein abgestimmtes Verfahren, das auch regulatorisches Lernen ermöglichte. Der Begriff „Sandbox“ wurde zwar nicht explizit verwendet, das zugrundeliegende Prinzip des kontrollierten Testens unter Mitwirkung der Aufsicht ist jedoch vergleichbar. Die

Begleitforschung wird im Rahmen des Projekts „RE-FRESCH“ durchgeführt, das von B.A.U.M. Consult GmbH, dem Energieinstitut an der Johannes Kepler Universität Linz und dem Institut für Klimaschutz, Energie und Mobilität (IKEM) umgesetzt wird (BMK, 2024).

Reallabore für 100 % erneuerbare Energie: Die Initiative „100 % Erneuerbare-Energie-Reallabore" verfolgt das Ziel, in sechs österreichischen Regionen prototypische Systemlösungen für integrierte, regionale Energiesysteme zu entwickeln und zu testen. Jedes Reallabor besteht aus einem Innovationslabor, das neue Ideen entwickelt, und einem Leitprojekt, das diese unter realen Bedingungen umsetzt. Diese Reallabore dienen als Testumgebungen für innovative Technologien und Geschäftsmodelle im Energiebereich und liefern wichtige Erkenntnisse für die Weiterentwicklung des regulatorischen Rahmens (BMK, 2024).

Green SandboxBuilder – Bedarfserhebung für Regulatory Sandboxes im Bausektor: Ein weiteres Beispiel für eine Regulatory Sandbox betrifft den Bausektor: Das Projekt „Green SandboxBuilder" (2022–2024) untersuchte systematisch den Bedarf an Regulatory Sandboxes im Bereich des nachhaltigen Bauens und Sanierens in Österreich. Ein interdisziplinäres Konsortium, bestehend aus der Innovationsberatung winnovation, der Technischen Universität Wien, der FH Campus Wien und der Initiative „For Forest Forever“, analysierte, in welchen Bereichen regulatorische Experimentierräume den größten Impact haben könnten. Das Projekt identifizierte vier Typen von Regulatory Sandboxes und entwickelte 14 thematische Vorschläge für deren Anwendung im Bausektor. Ziel ist es, die Einführung von technologischen, prozessualen und sozialen Innovationen zu beschleunigen und somit die Nachhaltigkeitsziele zu erreichen (TU Wien, 2024).

Innovationslabore für Bildung: Ein weiteres experimentelles Vorhaben mit regulatorischem Lernen betrifft den Bildungsbereich. Die **Innovationsstiftung für Bildung** fördert seit Herbst 2021 fünf Innovationslabore, die neue Lehr- und Lernmethoden sowie EdTech-Lösungen in realen Schulumgebungen testen. Diese Labore bieten Raum für die Erprobung innovativer Bildungsformate und tragen zur evidenzbasierten Weiterentwicklung des österreichischen Bildungssystems bei. Die Projekte werden wissenschaftlich begleitet, um ihre Wirksamkeit zu evaluieren und potenzielle Skalierungsmöglichkeiten zu identifizieren (Innovationsstiftung für Bildung, 2021).

GRÜNSTATTGRAU: Innovationslabor für Bauwerksbegrünung: Es handelt sich hierbei um eine ganzheitliche Kompetenzstelle für Bauwerksbegrünung in Österreich. Das Innovationslabor vernetzt innovative Produkte und Projekte, liefert Know-how und Analysen für die Praxis und begleitet urbane und partizipative Entwicklungsstrategien bis zur Umsetzung. Es dient als Plattform für die Entwicklung und Umsetzung von Lösungen zur Verbesserung der urbanen Lebensqualität durch Begrünungsmaßnahmen (GRÜNSTATTGRAU, 2024). Das Innovationslabor wurde im Rahmen des Programms „Stadt der Zukunft" des vormaligen Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (jetzt BMIMI) initiiert und wird von der FFG gemeinsam mit der Austria Wirtschaftsservice Gesellschaft mbH und der Österreichischen Gesellschaft für Umwelt und Technik (ÖGUT) abgewickelt (GRÜNSTATTGRAU, 2024).

Ein weiteres Beispiel für experimentelles Lernen ist die **future.lab Innovationswerkstatt** der Technischen Universität Wien. Sie bietet eine zentrale Anlaufstelle für soziale Innovation und nachhaltige Transformation in der Stadt- und Quartiersentwicklung. Im Fokus stehen

methodische Zugänge, offene Formen des Wissenstransfers und die co-produktive Zusammenarbeit zwischen Praxis und Wissenschaft. Das Labor fördert soziale Innovationen als Schlüssel einer transformativen Innovationspolitik (future.lab TU Wien, 2024). Seit März 2022 wird die Innovationswerkstatt durch Mittel des Klima- und Energiefonds gefördert. Diese Förderung ermöglicht dem future.lab den Ausbau und die Weiterentwicklung seiner Formate, unterstützt den Dialog, die Zusammenarbeit und das gemeinsame Lernen mit anderen wissenschaftlichen Akteuren und der Stadtentwicklungspraxis (future.lab TU Wien, 2024).

Lehren aus bisherigen Projekten

Die bisherigen Pilot- und Innovationsprojekte in Österreich, die Regulatory Sandboxes sind oder in Ansätzen sandboxähnliche Strukturen aufweisen, liefern wichtige Hinweise für die Ausgestaltung zukünftiger regulatorischer Experimentierräume. Eine zentrale Lehre betrifft die **frühzeitige und aktive Einbindung von Behörden**: Sowohl im Projekt *Energie.Frei.Raum* als auch in den Reallaboren für erneuerbare Energie hat sich gezeigt, dass die Beteiligung von Vollzugs- und Aufsichtsbehörden nicht nur die rechtliche Machbarkeit verbessert, sondern auch die institutionelle Akzeptanz erhöht (BMK, 2023).

Ein zweiter zentraler Aspekt ist die **funktionale Unterscheidung zwischen technischen Tests und regulatorischem Lernen**. In vielen bisherigen Vorhaben lag der Fokus auf der Demonstration technologischer Lösungen (z. B. Energiezellen, Smart Grids oder Holzbauverfahren), weniger jedoch auf der gezielten Reflexion und Modifikation regulatorischer Rahmenbedingungen. Dies zeigt, dass ein strukturiertes Learning-Design – etwa durch begleitende Evaluation, Indikatorensysteme oder Policy-Workshops – eine Voraussetzung dafür ist, dass Pilotprojekte tatsächlich in Regelsetzung oder -anpassung münden können (FFG, 2022; ZSI, 2021). Es ließe sich problemlos auf bisherigen Initiativen aufbauen, um regulatorisches Lernen zu stärken.

Darüber hinaus lassen sich aus mehreren Projekten Lehren zur **Governance und Prozessgestaltung** ableiten: Erfolgreiche Initiativen verfügten in der Regel über klare Steuerungsstrukturen, multidisziplinäre Konsortien und transparente Zieldefinitionen. Beispielsweise war im Projekt *Green SandboxBuilder* die Entwicklung eines Typenrasters hilfreich, um mögliche Sandbox-Formate systematisch voneinander abzugrenzen – etwa hinsichtlich Rechtsrelevanz, Skalierbarkeit und sektoraler Einbettung (BMK, 2023).

Positiv hervorzuheben ist die **Rolle der Forschungsförderung** als Ermöglichungsstruktur. Die Unterstützung durch FFG, Klima- und Energiefonds oder aws hat sich als wichtiger Hebel erwiesen, um experimentelle Vorhaben initiieren zu können – gerade dort, wo Rechtsgrundlagen fehlen oder regulatorische Unsicherheit besteht. Förderorganisationen können somit auch für Regulatory Sandboxes eine wichtige Position einnehmen, z. B. durch die Förderung von Begleitevaluationen oder Forschungsprojekten.

Gleichzeitig wurde deutlich, dass **Kooperation allein keine Wirksamkeit garantiert**. Ohne Rückbindung an strategische Politikebenen und ohne Mechanismen zur Überführung von Erkenntnissen in dauerhafte institutionelle Strukturen verbleiben viele Pilotprojekte isoliert. Die Lehren aus der bisherigen Praxis zeigen somit klar: Regulatory Sandboxes müssen nicht nur technisch machbar, sondern **strategisch gewollt, normativ abgesichert und prozessual**

lernfähig gestaltet werden. Bei der Förderung und Umsetzung derartiger Projekte könnte das „Sandbox-Potenzial“ bewertet und berücksichtigt werden.

6.4 HEMMNISSE UND GESTALTUNGSSPIELRÄUME

Rechtliche und politische Barrieren

Die Einrichtung von Regulatory Sandboxes in Österreich steht derzeit vor mehreren strukturellen Hürden. Diese betreffen sowohl die **gesetzliche Ausgestaltung** als auch das **politisch-administrative Umfeld**, in dem regulatorisches Experimentieren verhandelt wird. Wie oben dargestellt, existiert im österreichischen Recht (anders als z. B. in Deutschland) **kein Rahmengesetz**, das temporäre Abweichungen vom geltenden Regulierungsrahmen – etwa im Datenschutz- oder Verwaltungsverfahrensrecht – sektorübergreifend erlaubt. Darüber hinaus fehlt eine **übergeordnete rechtliche Definition** von Regulatory Sandboxes, wie sie etwa in Deutschland im Reallabore-Gesetz vorgeschlagen wurde (BMWK, 2024). Dies erschwert die normierte Implementierung, etwa in Bezug auf Zulassungskriterien, Aufsichtsbefugnisse oder Evaluationspflichten.
Obwohl einzelne Initiativen (z. B. Energie.Frei.Raum) Impulse gesetzt haben, fehlt bislang eine **klar priorisierte politische Strategie zur Umsetzung von Regulatory Sandboxes** auf Bundesebene. Weder die geltende Digital- noch die FTI-Strategie benennen regulatorisches Experimentieren als explizites Politikziel (BMBWF/BMK, 2025).
Zugleich ist das Thema in der Praxis bislang **stark sektoralisiert**: So bestehen etwa im Energiebereich oder im Bereich Finanzdienstleistungen Sandboxes für die rechtliche Erprobung neuer Anwendungen, während die Sektion III des Bundeskanzleramts Sandboxes zur Verwaltungstransformation betreibt, die als Lernumgebung für Organisationen der öffentlichen Verwaltung fungieren, um KI-Projekte und andere Innovationen zu entwickeln und zu testen. Diese Fragmentierung geht mit einem **Mangel an ressortübergreifender Steuerung** einher (OECD, 2021). Die Möglichkeit über sektorale Sandboxes hinauszugehen, bedingt ein politisches Umdenken, Priorisierung und, wie man beispielsweise in der nationalen Sandbox für KI in Spanien oder der Sandbox für Digitalisierung in Malta beobachten kann, erhebliche Ressourcen.
Da das hoheitliche Verwaltungshandeln in Österreich vom Legalitätsprinzip bestimmt wird, kann ein Spannungsverhältnis zu regulatorischen Werkzeugen wie Sandboxes, in denen temporär vom Rechtsrahmen abgewichen wird, entstehen (Gerlach & Lösch, 2020).

Rechtliche und politische Barrieren

Auch wenn Österreich derzeit über keinen allgemeinen Gesetzesrahmen für sektorübergreifende Regulatory Sandboxes verfügt (vgl. 5.1), lassen sich im bestehenden Rechtsrahmen **Spielräume identifizieren**, die unter bestimmten Bedingungen für innovationsorientiertes Experimentieren genutzt werden könnten. Diese betreffen insbesondere **Verwaltungspraxis, Förderinstrumente und sektorale Spezialgesetze**.

Verwaltetes Ermessen und Pilotierung unter Aufsicht: Im einfachen Verwaltungsverfahren besteht grundsätzlich dort ein **gewisser Handlungsspielraum**, wo der Gesetzgeber **Ermessen** zulässt. So kann beispielsweise im Rahmen von **Pilotierungen** unter Aufsicht eine neue Verfahrensweise getestet werden, solange sie nicht gegen geltendes Recht verstößt und im Sinne der Verwaltungsökonomie sachlich gerechtfertigt ist.

In Bereichen wie dem **Datenschutz** ist das zwar stark eingeschränkt – in anderen Bereichen, etwa bei **Förderrichtlinien** oder internen Abläufen im Bereich Service Design, kann dieser Weg jedoch genutzt werden. Hier ist nicht von „Sandbox" im engeren Sinne zu sprechen, sondern von **testfähiger Verwaltungspraxis**.
Forschungsförderung als indirekter Sandbox-Hebel: Programme der **FFG** oder des **Klima- und Energiefonds** ermöglichen es, **praxisnahe Forschung und Demonstrationsprojekte mit dem Charakter** von **Regulatory Sandboxes** zu fördern. Zwar handelt es sich meist **nicht um regulierungsverändernde Formate**, doch durch begleitende Evaluation, multidisziplinäre Kooperationen und institutionelle Einbindung (z. B. Behördenbeteiligung) können **Erkenntnisse generiert werden**, die später regulatorisch nutzbar gemacht werden (OECD, 2021; Gerlach & Lösch, 2020).

Öffnung über sektorale Gesetzgebung: Einzelne sektorale Gesetze enthalten **schon heute Regelungen**, die sich punktuell für regulatorisches Experimentieren nutzen lassen – etwa:

- im **Energiewirtschaftsrecht** (ElWOG, GWG): temporäre Ausnahmeregelungen für innovative Netz- oder Marktmodelle (siehe 7.2.1),
- im **Forschungsorganisationsgesetz (FOG)**: Förderstrukturen, die Pilotierung und Reallabore unterstützen,
- im **Telekommunikationsgesetz (TKG 2021)**: gewisse Spielräume zur Flexibilisierung von Frequenznutzungsmodellen in Pilotprojekten.

Diese Hebel sind **sektoral begrenzt**, könnten aber als Vorbild für zukünftige sandboxfähige Öffnungsklauseln dienen.
Soft-Law und informelle Koordination: Ein ergänzender Ansatz liegt in der Nutzung von **Soft-Law-Instrumenten**, wie etwa **Memoranda of Understanding (MoUs)**, **Kooperationsvereinbarungen** oder **Modellprojekten mit wissenschaftlicher Begleitung**. Diese Instrumente schaffen **Erwartungssicherheit**, ohne rechtlich verbindlich zu sein, und können das Vertrauen in regulatorisch sensible Innovationen fördern – etwa im Bereich algorithmischer Systeme oder sensibler Datennutzung (Black & Lodge, 2022).

Strategische Lücken

Über die sektoral zersplitterten rechtlichen Grundlagen und die institutionelle Fragmentierung hinaus bestehen in Österreich auf der Umsetzungsebene **koordinative Verbesserungspotenziale** für die Entwicklung und Implementierung von Regulatory Sandboxes. Diese Verbesserungspotenziale betreffen insbesondere die **Verknüpfung innovationspolitischer Ziele mit regulatorischen Instrumenten**, die **Ressortkoordination**, das **Politiklernen** sowie die **Verankerung von Testkultur im Verwaltungshandeln**.
Übersetzungsstrategien zwischen Innovation und Regulierung: Obwohl sich Österreich in verschiedenen Strategiedokumenten zur Förderung von technologischer und gesellschaftlicher Innovation bekennt (z. B. FTI-Strategie 2030, Digital Austria Agenda), fehlt es bislang an einer **übergeordneten Strategie**, um Innovationsimpulse in regulatorisches Lernen zu überführen. Es bedarf strukturierter Mechanismen, die Erkenntnisse aus Pilotprojekten oder technologischen Tests in **gesetzgeberische oder administrative Veränderungsprozesse** rückbinden (Kuhlmann, Stegmaier & Konrad, 2019). Derzeit besteht ein **Strategiedefizit an der Schnittstelle von Technologieentwicklung und**

Normsetzung – ein zentrales Element für das Funktionieren von Sandboxes als lernorientierte Regulierungsform.

Mangelnde ressortübergreifende Abstimmung von regulatorischem Experimentieren: Anders als in Ländern mit strukturierter Sandbox-Praxis (z. B. UK, Frankreich, Singapur) fehlt in Österreich ein **explizites Mandat**, das Innovations- und Regulierungsressorts systematisch miteinander verknüpft. Die Folge ist ein **Verlust an strategischer Steuerungskompetenz**: Pilotvorhaben entstehen isoliert, ohne Governance-Struktur, in der Innovations-, Rechts-, Markt- und Gesellschaftsperspektiven integriert werden.
Unzureichende Nutzung von Evaluationswissen: In zahlreichen innovationspolitischen Programmen (z. B. Reallabore, Energie.Frei.Raum, Smart Cities) wird zwar projektbezogen evaluiert – jedoch fehlt es an Mechanismen, um dieses Wissen **systematisch auf Regelsetzung zurückzuführen**. Es gibt keine etablierte Praxis, Ergebnisse aus Feldtests in legislative Entscheidungsprozesse zu übersetzen (Willems & Van Dooren, 2021). Ohne strukturelle Feedbackschleifen bleibt Lernen zufällig statt strategisch organisiert.
Fehlende politische Symbolik und Narrative: Regulatorisches Experimentieren ist in Österreich **nicht als positives Innovationsnarrativ verankert**. Anders als etwa im Vereinigten Königreich, wo die Financial Conduct Authority mit ihrer Sandbox-Praxis aktiv Innovationsbereitschaft signalisiert, fehlt es in Österreich an politischen Repräsentationen, die adaptive Regulierung aktiv kommunizieren. Dies trägt zur **Zurückhaltung in Verwaltung und Öffentlichkeit** bei und verhindert, dass Regulatory Sandboxes als Teil einer zukunftsorientierten Governance verstanden werden (Sabel & Zeitlin, 2012). Hier könnte es aktuell beispielsweise durch die Vorgabe der EU, im Rahmen der europäischen KI-Verordnung Sandboxes im Bereich KI umzusetzen, zu einem Umdenken kommen.

6.5 KOORDINATION UND HERAUSFORDERUNGEN IM FÖDERALEN SYSTEM

Österreich ist ein bundesstaatlich organisierter Rechtsstaat, in dem die Gesetzgebung und Vollziehung zwischen Bund und Ländern aufgeteilt ist (vgl. Art. 10–15 B-VG). Diese Struktur schafft spezifische Herausforderungen für die Einführung und Steuerung von lokalen oder regionalen Regulatory Sandboxes (KI-VO Art. 57 (2)), da sie sowohl **vertikale Koordination zwischen Bund und Ländern** als auch **horizontale Abstimmung zwischen Ressorts und Politikfeldern** erfordert.

Viele gesetzliche Regelungen, die für sandboxbezogene Experimente relevant wären – etwa aus dem Bau-, Raumordnungs-, Veranstaltungs- oder Naturschutzrecht – fallen in den **Zuständigkeitsbereich der Länder**. Das bedeutet, dass für ein und dasselbe Innovationsvorhaben potenziell **neun unterschiedliche Vollzugsregime** gelten – mit jeweils eigenen Behörden, Verfahren und politischen Bewertungsmaßstäben (Gamper, 2014). Ohne gemeinsame Standards oder föderale Vereinbarungen kann ein Projekt, das in einem Bundesland rechtlich möglich ist, im nächsten faktisch blockiert sein. Einzelne Länder könnten hier Vorreiter sein und Sandbox-Modelle umsetzen und ggf. zu einem Umdenken und Anpassungen in anderen Ländern führen.

Zudem fehlt in Österreich eine **ressortübergreifende Koordination**, die Regulierungs-, Innovations- und Digitalpolitik systematisch integriert. Während beispielsweise das BMIMI für innovationsbezogene Agenden (z. B. FTI-Strategie) zuständig ist, liegt die Regulierungshoheit meist bei Fachministerien und die strategische Digitalpolitik beim Bundeskanzleramt. Diese

Aufteilung führt zu **strukturellen Koordinationsproblemen**, wenn innovationspolitische Ziele in rechtliche Gestaltungsräume übersetzt werden sollen (Kattel et al., 2022). In der Praxis zeigt sich, dass innovative Pilotprojekte oft auf persönliches Engagement einzelner Akteur:innen angewiesen sind – etwa im Bereich Stadtentwicklung oder regionaler Energielösungen (Wagner et al., 2021).

Diese Abhängigkeit von Einzelfalllösungen verhindert eine **strukturierte und skalierbare Sandbox-Politik**. Es könnten Mechanismen entwickelt werden, um **Regeldivergenzen zu minimieren** und **Interoperabilität föderaler Regime zu ermöglichen**, z. B. durch Mustersatzungen, Rahmenerlasse oder kooperative Gesetzgebung.

Aktuell fehlen zudem **rechtliche Instrumente**, um ein Sandbox-Vorhaben verbindlich zwischen mehreren Gebietskörperschaften zu koordinieren. Selbst wenn auf allen Ebenen Zustimmung besteht, existieren **keine klaren Regelungen für Zuständigkeitsübertragung, Evaluationsverantwortung oder gemeinsames Risikomanagement**. Internationale Beispiele zeigen, dass etwa durch Mustersatzungen, ressortübergreifende Verwaltungsvereinbarungen oder projektbasierte Kooperationsverordnungen gezielt Abhilfe geschaffen werden kann (Kostka & Schmidthuber, 2022).

6.6 ANSPRUCHSGRUPPENPERSPEKTIVEN UND INSTITUTIONELLE POSITIONEN

Die Einführung von Regulatory Sandboxes in Österreich berührt eine Vielzahl institutioneller Akteure – aus Verwaltung, Politik, Regulierung, Wirtschaft, Sozialpartnerschaft, Zivilgesellschaft und Forschung. Ihre Positionen sind entscheidend dafür, ob und wie Sandbox-Formate entstehen, ausgestaltet oder gar blockiert werden. Dieses Kapitel beleuchtet systematisch die institutionellen Einschätzungen, Erwartungen und Vorbehalte, die in der öffentlichen Diskussion bislang dokumentiert oder ableitbar sind.

Im Zentrum steht dabei die Frage, **wie verschiedene Anspruchsgruppen regulatorisches Experimentieren bewerten, welche Funktionen sie ihm zuschreiben und unter welchen Bedingungen sie zur Mitwirkung bereit wären**. Die folgenden Abschnitte basieren auf öffentlich zugänglichen Stellungnahmen, Strategiepapieren, Projektberichten und Expert:innen-Interviews und gliedern sich in drei Perspektivlinien: (1) institutionelle Positionen, (2) wahrgenommene Chancen und Risiken, sowie (3) konkrete Mitgestaltungs- und Pilotierungsmöglichkeiten.

Gemeinsam bieten sie ein differenziertes Bild institutioneller Erwartungshaltungen und damit eine wichtige Grundlage für die Entwicklung eines tragfähigen, konsensfähigen und handlungsorientierten Modells von Regulatory Sandboxes in Österreich.

Institutionelle Perspektiven für Regulatory Sandboxes in Österreich

Dieser Abschnitt beleuchtet die Perspektiven zentraler Institutionen in Österreich, die durch ihre gesetzliche Zuständigkeit, strategische Position oder soziale Repräsentativität eine Rolle bei der Entwicklung, Steuerung oder Bewertung von Sandbox-Modellen einnehmen können. Neben Ministerien und Aufsichtsbehörden werden auch Kammern, Sozialpartner und Organisationen mit Schnittstellenfunktion berücksichtigt. Die Analyse stützt sich auf offizielle

Dokumente, Stellungnahmen und Interviews sowie aktuelle Entwicklungen im institutionellen Feld.

Die Diskussion um Regulatory Sandboxes in Österreich ist von vielfältigen Einschätzungen, institutionellen Hintergründen und normativen Zielsetzungen geprägt. Während einige Akteur:innen das Format als innovatives Regulierungsinstrument betrachten, überwiegt bei anderen die Sorge vor einer möglichen Aushöhlung bestehender Schutzstandards. Die Spannungsfelder betreffen vor allem Fragen der Rechtsklarheit, gesellschaftlichen Verantwortung und sektorspezifischen Umsetzbarkeit.

Das **Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)** hat sich im Kontext von Nachhaltigkeits- und Innovationspolitik mehrfach zur Rolle regulatorischer Experimentierräume geäußert. Im Rahmen des vom BMIMI unterstützten Projekts „Green SandboxBuilder“ wird Regulatory Sandboxes eine hohe Bedeutung für die Ermöglichung transformativer Innovationen im Baubereich zugeschrieben. In der begleitenden Studie heißt es: „*Regulatory Sandboxes können als innovationsfördernde Zwischenräume fungieren, in denen bestehende Normen kritisch geprüft und neue Lösungen risikobegrenzt getestet werden*“ (Leimüller et al., 2024, S. 7).
Damit signalisiert das BMIMI Offenheit gegenüber sandboxartigen Formaten, auch wenn diese bislang vorwiegend sektorale Schwerpunkte verfolgen und konzeptionell in bestehende Nachhaltigkeitsprogramme integriert sind. Das gilt nicht nur für den Green SandboxBuilder, sondern auch für das Programm „Energie.Frei.Raum“, das auf die Erprobung dezentraler Energie- und Klimasysteme abzielt.
Eine eigenständige Positionierung des BMIMI im Hinblick auf KI-spezifische Regulatory Sandboxes liegt nicht vor. Dennoch lässt sich ein grundsätzliches Interesse an experimentellen Innovationsformaten erkennen. Vor allem im Bereich klimabezogener Digitalisierung und nachhaltiger Mobilität eröffnen sich potenzielle Anknüpfungspunkte für sektorübergreifende Sandbox-Modelle, auch im Zusammenspiel mit weiteren Ressorts.

Das **Bundeskanzleramt (BKA)** in Österreich hat eine zentrale Rolle beim Aufbau der KI-Sandbox. Insbesondere die für die nationale Umsetzung der europäischen KI-Verordnung zuständige Digitalisierungssektion sei hierbei erwähnt. Dazu gehört die Benennung von Behörden, die die KI-Sandbox beaufsichtigen und für die Überwachung von Hochrisiko-KI-Systemen verantwortlich sind. Das Bundeskanzleramt wirkt somit an der Schaffung eines rechtlichen und organisatorischen Rahmens mit, der notwendig ist, um KI-Sandboxes hierzulande einzurichten und zu betreiben. Außerdem spielt das Bundeskanzleramt eine treibende Rolle bei der digitalen Strategie Österreichs, indem es den verantwortungsvollen Einsatz von KI in der öffentlichen Verwaltung fördert, die Effizienz steigert und die Transparenz erhöht. Es koordiniert außerdem gemeinsam mit dem BMIMI eine nationale Governance-Struktur zum Thema KI, einschließlich des AI Policy Forums[4]. Die genaue Organisation umfasst zudem interministerielle Zusammenarbeit sowie Beratung durch den KI-Beirat und die KI-Servicestelle (RTR). Diese Initiativen verfolgen zwar primär regulatorische Umsetzungs- und Aufklärungsziele, könnten jedoch mittelfristig in eine umfassendere Architektur von KI Regulatory Sandboxes eingebettet werden.

[4] Das AI Policy Forum ist ein zentrales Koordinations- und Austauschformat in Österreich, das die Umsetzung von KI-Strategien steuert, regulatorische und ethische Fragen behandelt und den Dialog zwischen Staat, Wirtschaft und Wissenschaft zur verantwortungsvollen KI-Nutzung fördert.

Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK): Im Zuge der Ministerienreform 2025 wurden die arbeits- und sozialpolitischen Agenden des früheren Bundesministeriums für Arbeit und Wirtschaft (BMAW) in das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK) integriert. Seither verantwortet das BMSGPK unter anderem Fragen der Arbeitsmarktpolitik, der Pflege- und Gesundheitsversorgung sowie des Konsumentenschutzes. Es handelt sich hier um Bereiche, in denen der Einsatz von KI-Systemen und algorithmischer Entscheidungsunterstützung besonders grundrechtsrelevant ist. Obwohl das BMSGPK bislang keine eigene Initiative im Bereich von Regulatory Sandboxes verfolgt hat, kommt dem Ressort eine zentrale Rolle in der Entwicklung solcher Formate zu. Das gilt insbesondere dort, wo KI-Anwendungen in sensible soziale Infrastrukturen eingreifen – etwa in der Pflegeplanung, bei der Verteilung von Sozialleistungen oder im Bereich digitaler Gesundheitsanwendungen. In diesen Kontexten ist eine regulierte Erprobung neuer Technologien unter ethischer, datenschutzrechtlicher und sozialpolitischer Aufsicht von besonderer Bedeutung. Vor diesem Hintergrund erscheint die Einbindung des BMSGPK in künftige Sandbox-Prozesse sinnvoll. Als zuständige Stelle für Grundsatzfragen des Konsumentenschutzes und der sozialen Absicherung kann das Ministerium dazu beitragen, Risiken für betroffene Gruppen frühzeitig zu erkennen, Schutzmechanismen einfließen zu lassen und die Legitimität von KI-Erprobungen zu stärken. Auch mit Blick auf die Umsetzung der europäischen KI-Verordnung, insbesondere in Anwendungsfeldern mit hohem Risiko, könnte das BMSGPK an der Ausgestaltung von Governance-Strukturen, Aufsichtsprozessen und ethischer Begleitung beteiligt werden.

Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET): Im Zuge der Regierungsumbildung im Frühjahr 2025 wurden die wirtschaftspolitischen Agenden des früheren Bundesministeriums für Arbeit und Wirtschaft (BMAW) in das neu geschaffene Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET) überführt. Das BMWET ist seither für standortrelevante Wirtschaftspolitik, Wettbewerbsfähigkeit, Unternehmensförderung sowie energie- und tourismuspolitische Fragen zuständig.
Für die Weiterentwicklung eines wirtschaftsnahen Sandbox-Modells erscheint das BMWET als naheliegender Kooperationspartner, insbesondere in Bezug auf die Verzahnung von Innovationsförderung **und** Standortpolitik. Zudem war das Wirtschaftsressort in der jüngsten Vergangenheit in die Entwicklung der Experimentierklausel und einer Support-Plattform eingebunden. Eine enge Koordination mit anderen zuständigen Ressorts, etwa in den Bereichen Soziales, Konsumentenschutz oder Forschung, wäre dabei zentral.

Das Bundesministerium für Frauen, Wissenschaft und Forschung (BMFWF) ist für die strategische Steuerung und Förderung des österreichischen Forschungs- und Bildungssystems zuständig. Auch wenn das BMBWF bislang keine spezifische Position zu Regulatory Sandboxes im Bereich künstlicher Intelligenz veröffentlicht hat, ergibt sich aus seinen Zuständigkeiten eine mögliche Rolle im Kontext forschungsnaher oder öffentlich geförderter Sandbox-Modelle.
In der gemeinsamen „Strategie für Forschung, Technologie und Innovation 2030“ (BMBWF/BMK, 2021) bekennen sich die zuständigen Ressorts zur Förderung transdisziplinärer und verantwortungsvoller Technologieentwicklung. Experimentierformate wie Reallabore oder Regulatory Sandboxes werden dort jedoch nicht ausdrücklich adressiert. In Anbetracht der Anforderungen der europäischen KI-Verordnung – insbesondere der

Einbindung von Forschungseinrichtungen, ethischen Gremien und Fachöffentlichkeit – könnte dem BMBWF dennoch eine Schlüsselrolle zukommen: etwa bei der Konzeption von Begleitforschung, der Koordination universitärer Beiträge oder der Qualitätssicherung evidenzbasierter Regulierung.
Zudem könnten Bildungsbereiche selbst – etwa im Rahmen digital gestützter Lernsysteme oder algorithmischer Entscheidungshilfen im Schulkontext – Gegenstand zukünftiger Sandbox-Projekte werden. Dabei wären die didaktischen, datenschutzrechtlichen und ethischen Implikationen besonders sensibel zu gestalten. Auch aus diesem Grund erscheint eine strukturierte Einbindung des BMBWF in nationale Sandbox-Initiativen als strategisch vorteilhaft.

Das **Bundesministerium für Finanzen (BMF)** spielt eine zentrale Rolle bei der Umsetzung der regulatorischen Sandbox im Finanzmarktbereich. Mit der Novelle des Finanzmarktaufsichtsbehördengesetzes (FMABG) im Jahr 2020 wurde die rechtliche Grundlage für eine sektorale Sandbox unter Aufsicht der FMA geschaffen. Das BMF ist über die Einrichtung und Koordination des sogenannten Regulatory Sandbox Beirats formell eingebunden. Dieser Beirat beurteilt im Zulassungsverfahren unter anderem das volkswirtschaftliche Interesse, die Innovationshöhe und die Testreife der eingereichten Geschäftsmodelle und spricht eine Stellungnahme aus, auf deren Basis die FMA über die Aufnahme entscheidet (BMF, 2023).
Im Zusammenhang mit digitalen Technologien wie Blockchain, Krypto-Assets oder automatisierter Finanzberatung hat das BMF mehrfach auf die Notwendigkeit innovationsfreundlicher und zugleich rechtsklarer Rahmenbedingungen verwiesen. In einem juristischen Fachbeitrag zur Ausgestaltung der Finanzmarkt-Sandbox wird betont, dass der geschaffene Rechtsrahmen ein strukturiertes, risikobasiertes Prüfregime ermögliche, das sowohl Innovation als auch Anlegerschutz und Finanzmarktstabilität berücksichtige (Potacs & Kircher, 2021).
Eine explizite Positionierung des BMF zu KI-spezifischen Sandbox-Formaten außerhalb des Finanzsektors liegt nicht vor. Angesichts der zunehmenden Verknüpfung von Finanztechnologie und künstlicher Intelligenz bei algorithmischer Risikoanalyse oder automatisierten Kundeninteraktionen erscheint eine Ausweitung bestehender Formate auf KI-basierte Anwendungsfälle jedoch mittelfristig plausibel. Im Rahmen nationaler Umsetzungsmaßnahmen der europäischen KI-Verordnung könnte dem BMF daher eine Rolle bei der regulatorischen Einbettung von KI-Innovationen im Finanzbereich zukommen.

Die **Österreichische Forschungsförderungsgesellschaft (FFG)** ist die nationale Förderagentur für anwendungsorientierte Forschung und Entwicklung. Sie spielt eine zentrale Rolle im österreichischen Innovationssystem. Sie fördert kooperative Forschungsprojekte, Sondierungen, Reallabore und sektoraler Pilotprogramme. Auch wenn die FFG bislang nicht an einer Regulatory Sandbox im engeren Sinne beteiligt ist, greift sie in mehreren Förderformaten das Prinzip regulierter Erprobung unter realen Bedingungen auf.

Im Zuge der laufenden Diskussion um KI-Sandboxes erscheint die FFG als potenzieller Implementierungspartner: sowohl für den Aufbau strukturierter Förderpfade als auch für die Begleitung sektoraler oder themenspezifischer Testumgebungen. Ihre Nähe zu anwendungsorientierter Forschung, ihre Erfahrung in der Koordination öffentlicher Mittel und ihre Kontakte zu Unternehmen und Hochschulen machen sie zu einer möglichen Infrastrukturträgerin für innovationsfreundliche Sandbox-Modelle. Besonders relevant wäre die

FFG auch für die Integration von Evaluationsprozessen, Wirkungsmonitoring und den Erfahrungsaustausch, wie im Kontext der europäischen KI-Verordnung zunehmend gefordert. Eine enge Zusammenarbeit mit anderen Stellen – etwa BMWET, BMIMI oder BMBWF – sowie der Einbezug bestehender Strukturen wie COMET-Zentren, Digital Innovation Hubs (DIHs) oder European Digital Innovation Hubs (EDIHs) könnte helfen, Synergien zu nutzen und sektorübergreifende Testformate effizient umzusetzen.

Die **Austria Wirtschaftsservice GmbH (aws)** ist die Förderbank des Bundes für unternehmensbezogene Wirtschaftsförderung. Sie unterstützt Start-ups, KMU und wachstumsorientierte Unternehmen mit Zuschüssen, Garantien, Beteiligungen und begleitenden Services. Im Kontext von KI spielt die aws eine maßgebliche Rolle bei der Umsetzung innovationspolitischer Förderstrategien.

Auch wenn die aws bislang keine eigene Regulatory Sandbox im engeren Sinne betreibt, führen einige ihrer Programme Unternehmen gezielt an neue regulatorische Rahmenbedingungen heran – zumeist in der Kombination aus technischer Begleitung, Zugang zu Testinfrastrukturen und vorbereitender Konformitätsberatung.

Die aws gilt als naheliegender Umsetzungspartner für zukünftige Sandbox-Modelle, vor allem im anwendungsorientierten Bereich. Sie verfügt über institutionelle Erfahrung in der Projektförderung, breites Know-how im Risikomanagement und ein bestehendes Netzwerk zu Start-ups, Deep-Tech-Teams und förderfähigen KMU. Besonders in frühen Innovationsphasen kann die aws dabei unterstützen, Unternehmen in die Lage zu versetzen, regulatorische Anforderungen zu erkennen und Testformate mitzugestalten.

Vor diesem Hintergrund erscheint die strukturierte Einbindung der aws zum Beispiel über den Aufbau koordinierter Förderlinien für Sandbox-Teilnehmer als strategisch sinnvoll. Sie könnte eine Brückenfunktion zwischen Förderung, Regulierung und Markteintritt einnehmen und zur praktischen Umsetzung eines österreichischen Sandbox-Ökosystems beitragen.

Finanzmarktaufsicht (FMA): Ein institutionalisierter Bezug zu Regulatory Sandboxes besteht derzeit ausschließlich im Finanzmarktbereich. Im Jahr 2020 wurde durch § 23a des Finanzmarktaufsichtsbehördengesetzes (FMABG) die gesetzliche Grundlage für die Einrichtung einer Sandbox bei der FMA geschaffen. Ziel ist es, innovativen Geschäftsmodellen mit potenziell hoher Markt- oder Verbraucherschutzrelevanz eine temporäre Testumgebung unter regulatorischer Aufsicht zu bieten.
Die FMA führt das Format nach eigenen Angaben mit einem kooperativen Prüfcharakter. Es soll dazu dienen, neuartige Modelle frühzeitig zu verstehen, regulatorisch einzuordnen und gegebenenfalls Anpassungsbedarf im geltenden Aufsichtsrahmen zu identifizieren. Ein interministerieller Beirat begleitet das Verfahren und gibt Stellungnahmen zur volkswirtschaftlichen Relevanz, Testreife und Marktfähigkeit der eingereichten Projekte ab.

In der Praxis blieb die Zahl der Teilnehmer:innen bislang überschaubar. Ende 2023 befanden sich drei Unternehmen in der aktiven Testphase. Die Öffnung auf weitere Sektoren, etwa in Richtung KI, Energie oder Gesundheitswesen, wurde bislang weder gesetzlich noch organisatorisch vorgesehen bzw. kommuniziert. Damit bleibt das österreichische Sandbox-Modell im Finanzbereich formal etabliert, jedoch strukturell eng gefasst und institutionell auf die FMA beschränkt. Weder ein sektorübergreifender Zugang noch eine explizite Positionierung zu technologieübergreifenden Use Cases, etwa im Bereich künstlicher Intelligenz, sind bisher erfolgt.

Auch eine tiefergehende Evaluation der bisherigen Erfahrungen hinsichtlich Verfahrenstransparenz, Rechtsklarheit oder Lerngewinnen liegt nicht vor. Damit bleibt das österreichische Sandbox-Modell im Finanzbereich ein pionierhaftes Einzelinstrument mit begrenzter systemischer Reichweite.

Die **Datenschutzbehörde (DSB)** ist für sämtliche Fragen des Datenschutzes in Österreich zuständig und wird im Kontext von KI-Sandboxes insbesondere durch die Anforderungen der Datenschutz-Grundverordnung (DSGVO) und der europäischen KI-Verordnung eine zentrale Rolle einnehmen. Zwar hat die DSB bislang keine eigene Sandbox eingerichtet, sie hat sich jedoch im Jahr 2022 in einer öffentlichen Stellungnahme grundsätzlich offen gegenüber dem Konzept regulatorischer Testumgebungen geäußert, sofern diese im Einklang mit bestehenden datenschutzrechtlichen Vorgaben stehen.
Die DSB betont, dass der Spielraum für regulatorische Flexibilität im Datenschutzrecht durch die DSGVO begrenzt ist. Sie sieht dennoch Potenzial in begleitenden, kooperativ gestalteten Prüfformaten, die als rechtskonforme Alternativen zu experimentellen Ausnahmeregelungen dienen können. Diese könnten insbesondere in Form strukturierter Datenschutz-Folgeabschätzungen, Vorab-Konsultationen oder beratender Beteiligung bei KI-Pilotierungen umgesetzt werden.
Eine dezidierte Rolle der DSB bei der zukünftigen Gestaltung einer nationalen KI-Sandbox ergibt sich aus Artikel 57 (10) der europäischen KI-Verordnung[5]. Dieser sieht vor, dass Datenschutzbehörden in die nationale Umsetzung von KI-Testumgebungen eingebunden werden müssen, wenn KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu personenbezogenen Daten gewähren oder unterstützen. Im Lichte dieser neuen Verantwortung ist davon auszugehen, dass die DSB ihre institutionellen Kapazitäten mittelfristig ausbauen und enger mit anderen Behörden zusammenarbeiten wird.
Konkrete konzeptionelle Vorschläge, wie etwa eine datenschutzfokussierte Sandbox oder beratende Beteiligungsformate, liegen derzeit nicht vor. Eine Orientierung könnte das luxemburgische Modell „Sandkëscht“ bieten, das durch die lokale Datenschutzbehörde CNPD getragen wird. Es verbindet rechtskonforme Testverfahren mit beratender Aufsicht und könnte als Blaupause für eine österreichische Umsetzung dienen.

Die **Wirtschaftskammerorganisation (WKO)** ist als gesetzliche Vertretung aller Unternehmen und als einer der zentralen Sozialpartner in Österreich eine bedeutende Akteurin in der wirtschafts- und innovationspolitischen Standortgestaltung. Als Schnittstelle zwischen Wirtschaft, Verwaltung und Politik verfügt sie über umfassende Expertise in der Umsetzung praxistauglicher Rahmenbedingungen und Programme zur Unterstützung unternehmerischer Innovation.
Im Kontext regulatorischer Testumgebungen hat sich die WKO frühzeitig mit dem Konzept der Regulatory Sandbox auseinandergesetzt. In mehreren Stellungnahmen und Fachdialogen wurde betont, dass innovationsfördernde Rahmenbedingungen nicht durch pauschale

[5] Artikel 57 (10) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu personenbezogenen Daten gewähren oder unterstützen, sorgen die zuständigen nationalen Behörden dafür, dass die nationalen Datenschutzbehörden oder diese anderen nationalen oder zuständigen Behörden in den Betrieb des KI-Reallabors sowie in die Überwachung dieser Aspekte im vollen Umfang ihrer entsprechenden Aufgaben und Befugnisse einbezogen werden.

Deregulierung, sondern durch gezielte, rechtsklare Experimentierräume entstehen. In einem Positionspapier heißt es: „Innovative Projekte scheitern heute oft an Regelwerken, die weder technologische Entwicklungen noch neue Geschäftsmodelle reflektieren. Österreich braucht strukturierte Wege, um solche Innovationen kontrolliert zu erproben“ (WKO, 2021, S. 5).

Daher erscheint es zielführend, die WKO als institutionelle Vertreterin der Unternehmen systematisch in die Ausgestaltung, Steuerung und begleitende Bewertung zukünftiger Sandbox-Modelle einzubinden. Ihr Zugang zu unterschiedlichen Branchen, ihre Nähe zu unternehmerischen Bedarfen sowie ihre etablierte Struktur für Wissenstransfer und Rückkopplung machen sie zu einer strategisch relevanten Partnerin für die erfolgreiche Umsetzung anwendungsnaher und wirtschaftsgetragener KI-Sandboxes in Österreich.

Die **Arbeiterkammer (AK)** ist die gesetzlich verankerte Vertretung der Arbeitnehmer:innen. In technologiepolitischen Fragen setzt sich die AK für eine soziale und grundrechtskonforme Gestaltung des digitalen Wandels ein. Insbesondere mit Blick auf KI-Anwendungen betont sie regelmäßig die Bedeutung von Transparenz, Rechenschaftspflicht und dem Schutz vulnerabler Gruppen.
Zwar liegt bislang keine spezifische Stellungnahme der AK zu Regulatory Sandboxes im Bereich künstlicher Intelligenz vor, jedoch lassen sich aus bestehenden Positionen zur Digitalisierung, zur Plattformökonomie und zum Einsatz automatisierter Systeme wichtige Grundhaltungen ableiten. Aus Sicht der AK hat die KI-Verordnung eine Regelung zu Regulatory Sandboxes – diese ist unbedingt einzuhalten, insbesondere was die datenschutzrechtlichen Anforderungen betrifft. Darüber hinaus sollten Regulatory Sandboxes zu KI idealerweise durch Organisationen betrieben werden, die sich bereits seriös und menschenzentriert mit dem Thema auseinandersetzen (z. B. AI Factory, Statistik Austria), und sie müssen durch die zuständigen Behörden beaufsichtigt werden.

Die **Industriellenvereinigung (IV)** vertritt die österreichische Industrie sowie industrienahe Dienstleistungsunternehmen. In ihrem Branchenreport zur IT-Industrie hebt sie die Bedeutung digitaler Schlüsseltechnologien – insbesondere künstlicher Intelligenz – für die Wettbewerbsfähigkeit des Standorts hervor und fordert gezielte Maßnahmen zur Innovationsförderung.
Im Kapitel zu technologiepolitischen Rahmenbedingungen spricht sich die IV **ausdrücklich für die Entwicklung von Regulatory Sandboxes** aus. Diese sollen dazu dienen, neue Technologien unter realen Bedingungen und unter begleitender Aufsicht erproben zu können. Wörtlich heißt es:

> „*Für digitale Innovationen (wie z. B. den Einsatz von KI) sollten verstärkt regulatorische Sandboxes geschaffen werden, um Experimentierräume zu eröffnen, ohne sofort volle regulatorische Anforderungen auslösen zu müssen.“ (*IV, 2023, S. 15)

Darüber hinaus wird betont, dass solche Formate nicht nur Großunternehmen, sondern auch Start-ups und KMU offenstehen sollten. Die IV verweist auf den strategischen Mehrwert von Sandbox-Programmen für den Technologietransfer und für das Zusammenspiel zwischen Regulierung, Markt und Innovation. In Anlehnung an internationale Best Practices wird die Schaffung eines einheitlichen, rechtlich abgesicherten Rahmens für Reallabore empfohlen.

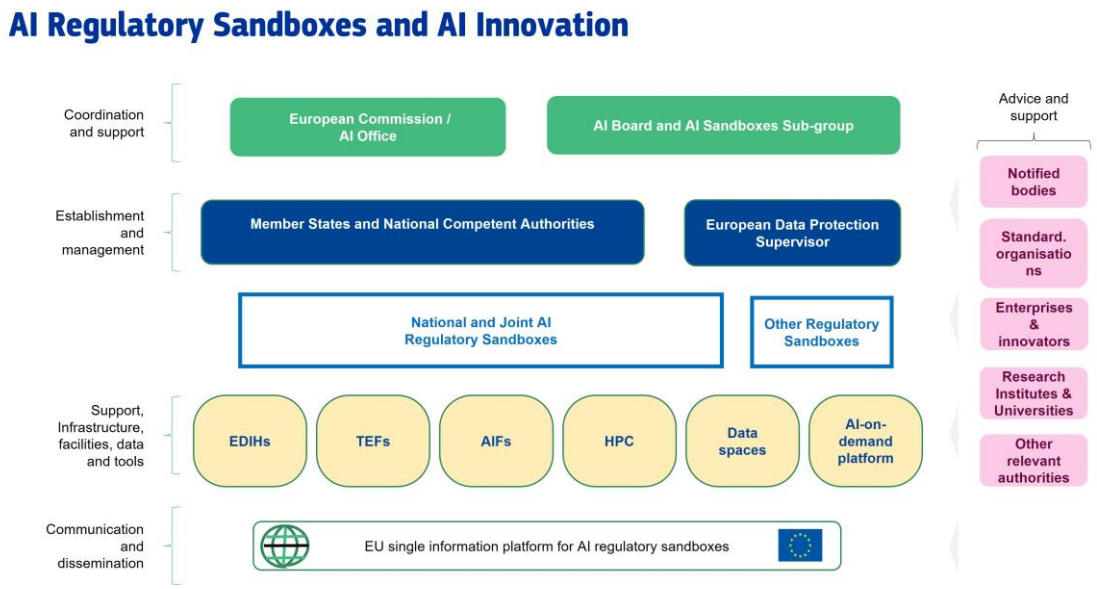
Die IV kann ein möglicher Akteur für die Weiterentwicklung wirtschaftsnaher Sandbox-Modelle sowohl auf nationaler Ebene als auch im Kontext europäischer Innovations- und Regulierungsstrategien sein. Ihre Einbindung könnte dazu beitragen, industriepolitische

Perspektiven frühzeitig in die Konzeption solcher Formate zu integrieren und deren Akzeptanz in der Unternehmenspraxis zu stärken.

Unterstützungs- und Umsetzungsinfrastrukturen

Regulatory Sandboxes benötigen nicht nur politische Steuerung und regulatorische Aufsicht, sondern auch eine leistungsfähige Infrastruktur für technologische Umsetzung, rechtliche Begleitung, Evaluierung und Zugang zu Testressourcen. In Österreich bestehen dafür bereits mehrere relevante Strukturen, insbesondere im Bereich digitaler Innovationsförderung und KI-Testzentren. Zentrale Akteure sind die **AI Factory** sowie die **DIHs** und **EDIHs**.

Abbildung 3: Europäische institutionelle Landschaft für KI Regulatory Sandboxes



Quelle: Europäische Kommission

Die **AI Factory Austria (AI:AT)** ist eine nationale Initiative zur Stärkung des KI-Ökosystems in Österreich. Sie dient als zentrale Werkstatt und Labor für KI-Innovationen, in der KI-Lösungen entwickelt, trainiert und getestet werden können – branchenübergreifend von Industrie und Unternehmen bis zur öffentlichen Verwaltung. Die AI Factory stellt modernste Supercomputing-Infrastruktur mit speziell für KI optimierten GPUs bereit und bietet umfassende Services wie Rechenleistung, Beratung, Schulungen und operative Unterstützung für Unternehmen und Forschungseinrichtungen. Ziel ist es, als Knotenpunkt das Netzwerk von Forschung, Wirtschaft und Verwaltung zu verbinden, Innovationen zu fördern und KI verantwortungsvoll und unter europäischen Datenschutz- und Ethikstandards voranzutreiben. Ein physischer AI Factory Hub fungiert zudem als One-Stop-Shop, Coworking-Space und Community-Zentrum mit rund 60 Mitarbeitenden, die Unterstützung bei Produktentwicklung, Projektbegleitung und Kapazitätsaufbau bieten. Damit stärkt die AI Factory die Wettbewerbsfähigkeit Österreichs als Technologiestandort und baut digitale Souveränität in Europa auf. Auch der Wissenstransfer über regulatorische Anforderungen spielt eine zunehmende Rolle, zum Beispiel durch vorbereitende Maßnahmen zur Konformitätsbewertung im Sinne der europäischen KI-Verordnung. Obwohl die AI Factory keine eigene Regulatory Sandbox im engeren Sinn betreibt, bietet sie strukturelle Anknüpfungspunkte für eine solche:

Ihre Nähe zu innovativen KMU, die Förderung anwendungsnaher Prototypen und der Aufbau interdisziplinärer Netzwerke können eine Brückenfunktion zur Entwicklung von Sandbox-Projekten erfüllen. Als bestehende Plattform mit erprobten Prozessen wäre sie sowohl für die Identifikation geeigneter Use Cases für Sandbox-Projekte als auch die Vorbereitung von Projekten auf regulatorische Anforderungen geeignet. Auch die Begleitung von KMU durch den Sandbox-Prozess, insbesondere durch Coaching, technische, wirtschaftliche und regulative Beratung, Zugang zu sicherer Infrastruktur und Partnernetzwerken, könnte geleistet werden.

Im Kontext der Umsetzung der europäischen KI-Verordnung und insbesondere der Artikel 57–59 zur Einrichtung nationaler KI-Sandboxes sollte geprüft werden, wie die AI Factory als Vorbereitungsplattform oder Implementierungspartnerin eingebunden werden kann. Gerade für KMU mit begrenzten Ressourcen kann diese Funktion entscheidend sein, um den Zugang zu sandboxbasierten Innovationspfaden zu sichern.

Die **DIHs** und **EDIHs** bilden ein zentrales Rückgrat der digitalen Innovationsinfrastruktur in Österreich. Insgesamt sechs national und vier europäisch co-finanzierte Hubs wurden eingerichtet, um insbesondere KMU bei der digitalen Transformation zu unterstützen. Thematische Schwerpunkte liegen unter anderem auf künstlicher Intelligenz, Cybersicherheit, Big Data, Blockchain und Industrie 4.0.
DIHs fungieren als regionale One-Stop-Shops, die Unternehmen den Zugang zu Testumgebungen, Know-how, Schulungsangeboten und Netzwerken erleichtern. Sie verbinden Unternehmen, Forschungseinrichtungen, Technologieanbieter und öffentliche Stellen und sind damit auch für Sandbox-Projekte mit sektoraler oder regionaler Ausrichtung potenziell hochrelevant. Im Kontext von KI Regulatory Sandboxes können DIHs/EDHIs insbesondere folgende Rollen übernehmen:

- Bereitstellung von technischen Testumgebungen für KI-Systeme,
- Unterstützung bei der Risikoanalyse und Konformitätsvorbereitung im Vorfeld einer Sandbox-Teilnahme,
- Sensibilisierung und Qualifizierung von Unternehmen zu rechtlichen, ethischen und technischen Anforderungen,
- Aufbau von regionalen Ankerpunkten für Sandbox-Pilotierungen mit lokaler Verankerung.

Auch auf europäischer Ebene wird die Rolle von EDIHs im Zusammenhang mit der Umsetzung der europäischen KI-Verordnung betont. In Erwägungsgrund 74 der europäischen KI-Verordnung wird festgehalten, dass EDIHs in ihrer jeweiligen Kompetenz technische und wissenschaftliche Unterstützung für Unternehmen sowie für Prüfstellen bereitstellen sollen. Dies betrifft auch vorbereitende Prozesse für Sandbox-Testungen.

Für eine zukunftsfähige Sandbox-Governance in Österreich wäre es sinnvoll, die vorhandenen DIH-/EDIH-Strukturen aktiv in den Aufbau operativer Sandbox-Prozesse einzubinden – etwa durch Pilotregionen, Partnerschaften mit Regulierungsbehörden oder sektorale Konsortien.

Wahrgenommene Erwartungshaltungen

Insgesamt lassen sich folgende **wahrgenommenen Erwartungshaltungen** gegenüber Regulatory Sandboxes identifizieren:

1. **Potenzial zur Förderung von Innovation**, insbesondere dort, wo bestehende Regeln technologische Entwicklung verzögern oder behindern.
2. **Wunsch nach regulatorischer Klarheit und Absicherung**, etwa durch Einbindung zuständiger Behörden, transparente Verfahren und definierte Schutzvorkehrungen.
3. **Bedarf nach klaren Zuständigkeiten und Governance-Strukturen**, um Konflikte zwischen unterschiedlichen Zielen – etwa Innovation und Schutzinteressen – frühzeitig zu adressieren.
4. **Sektorale und technologische Differenzierung**, um Sandbox-Formate an konkrete Anwendungsfelder, Risiken und gesellschaftliche Sensibilitäten anzupassen.

Diese Erwartungen zeigen, dass Regulatory Sandboxes als Konzept auf Resonanz stoßen – aber noch nicht einheitlich verstanden oder unterstützt werden. Die nächste Entwicklungsphase wird davon abhängen, ob es gelingt, ein gemeinsames Verständnis zwischen politischen, wirtschaftlichen, zivilgesellschaftlichen und behördlichen Akteuren zu schaffen – ohne dabei bereits bestehende Standards in Frage zu stellen.

Möglichkeiten zur Mitgestaltung und Pilotierung

Die institutionelle Bereitschaft zur Mitgestaltung und Pilotierung von Regulatory Sandboxes in Österreich zeigt sich bislang uneinheitlich. Während in einzelnen Sektoren konkrete Pilotformate geschaffen oder methodisch vorbereitet wurden, befinden sich viele Akteure noch im Stadium strategischer Orientierung oder politischer Positionsbildung. In der Gesamtschau überwiegt jedoch ein wachsendes Interesse am Format – insbesondere im Kontext digitaler, klimapolitischer und technologischer Transformationsprozesse.

Die institutionelle Landschaft in Österreich bietet grundsätzlich tragfähige Anknüpfungspunkte für den Aufbau von Regulatory Sandboxes. Mehrere zentrale Stellen – darunter Aufsichtsbehörden, Ministerien, Sozialpartner und Förderinstitutionen – erkennen das Potenzial regulierter Testumgebungen, um Innovation und Rechtssicherheit miteinander zu verbinden. Die Perspektiven fallen jedoch unterschiedlich aus: Sie reichen von klarer Befürwortung über sektorale Öffnung bis hin zu grundrechtlich motivierter Zurückhaltung.

Die Analyse zeigt: Regulatory Sandboxes sind in Österreich kein fremdes Konzept, sondern ein sich entwickelndes Instrument mit bereits sichtbaren institutionellen Bezugspunkten. Um ihr Potenzial vollständig zu entfalten, braucht es jedoch koordinierte Strukturen, klare Zuständigkeiten und sektorübergreifende Rahmenbedingungen. Die institutionelle Ausgangslage ist differenziert, aber prinzipiell anschlussfähig – und bildet damit eine belastbare Grundlage für weiterführende Pilotierung und strategische Verankerung.

7 KI Regulatory Sandboxes – Potenziale und Herausforderungen

7.1 EINLEITUNG

In diesem Kapitel werden die zentralen Herausforderungen und Potenziale von Regulatory Sandboxes im Bereich KI dargestellt. Die folgende Tabelle dient als Überblick:

Tabelle 5: Potenziale und Herausforderungen in der Übersicht

Herausforderungen	Potenziale
Datenschutzrechtliche Hürden: DSGVO lässt keine temporären Abweichungen zu	**Klärung regulatorischer Grauzonen** durch kontrolliertes Testen und rechtliche Begleitung
Blackbox-Problematik: Intransparenz vieler Modelle erschwert Kontrolle	**Vertrauensaufbau** durch öffentlich sichtbare, begleitete Testprozesse
Algorithmische Diskriminierung (Bias): Reproduktion sozialer Ungleichheiten	**Empirisch fundierte Regulierung** durch evidenzbasierte Evaluierung im Realbetrieb
Zurechnungsprobleme: Unklare Verantwortung bei KI-Entscheidungen	**Interdisziplinäre Governance** fördert frühzeitige Risikoerkennung und ethische Rahmung
Technische Dynamik: Lernfähigkeit erschwert statische Regulierung	**Adaptive Steuerung und Lernfähigkeit** von Behörden durch Sandbox-Erfahrung
Fehlende Standards: Unsicherheit bzgl. Testdesign, Evaluationskriterien etc.	**Standardentwicklung** in geschütztem Umfeld, z. B. für erklärbare KI oder ethische Leitplanken
Legitimitätsfragen bei öffentlichen KI-Projekten	**Demokratische Legitimationsgewinne** durch Partizipation und Transparenz in der Sandbox

Quelle: Eigene Zusammenstellung

7.2 REGULATORISCHE HERAUSFORDERUNGEN UND KONKRETER REGULIERUNGSBEDARF

Der Einsatz von Regulatory Sandboxes im Bereich von KI ist mit besonderen regulatorischen und ethischen Herausforderungen verbunden. Anders als in klassischen Innovationsfeldern, etwa Energie oder Mobilität, bringt KI ein hohes Maß an **technologischer Komplexität, normativer Unsicherheit und Grundrechtsnähe** mit sich.

Ein zentrales Problem besteht in der **Vereinbarkeit von experimentellem Testen mit datenschutzrechtlichen Vorgaben**. Viele KI-Anwendungen verarbeiten personenbezogene oder sensible Daten. Die DSGVO erlaubt jedoch keine temporäre Abweichung vom Schutzstandard – auch nicht zu Testzwecken (Gstrein, 2021). Besonders problematisch ist dies in Fällen automatisierter Entscheidungsfindung (Art. 22 DSGVO) oder beim Einsatz lernender Systeme, deren Outputs nicht vollständig vorhersagbar sind (Wachter et al., 2017).

Ein zweites zentrales Thema ist das **„Blackbox-Problem“**: Viele KI-Modelle sind inhärent intransparent, da ihre Funktionslogik nicht nachvollziehbar dokumentiert werden kann. In Sandbox-Projekten erschwert dies die Aufsicht, Evaluation und Verantwortungszuschreibung (Burrell, 2016). Insbesondere wenn öffentliche Stellen oder kritische Infrastrukturen beteiligt sind, stellt sich die Frage, wie regulatorische Rechenschaftspflichten erfüllt werden sollen.

Auch **ethische Fragen** stellen sich in Sandboxes verschärft: KI-Systeme können bestehende Vorurteile aus Trainingsdaten übernehmen (algorithmic bias), was zu diskriminierenden oder sozial ungerechten Ergebnissen führen kann (Binns, 2018). Eine sandboxbasierte Testung solcher Systeme erfordert daher klare Kriterien für Fairness, Nachvollziehbarkeit und gesellschaftliche Legitimität – Aspekte, die in klassischen Reallaboren meist weniger ausgeprägt sind.

Hinzu kommen **methodische Unsicherheiten**: Anders als bei technischen Innovationen (z. B. Bautechnik, Energienetze) lassen sich KI-Systeme oft nicht stabil „eingrenzen". Sie lernen, adaptieren und verändern sich dynamisch. Für Sandbox-Designs stellt dies hohe Anforderungen an Monitoring, Feedback-Schleifen und Governance-Architekturen (Smuha et al., 2021).

Schließlich gibt es **internationale regulatorische Divergenzen**. Während die EU mit der KI-Verordnung einen risikobasierten Ansatz verfolgt, setzen Länder wie das Vereinigte Königreich oder Singapur stärker auf „principles-based supervision"[6]. Sandbox-Projekte im Bereich KI müssen sich deshalb nicht nur an nationalen, sondern auch an globalen Standards und Interoperabilitätsfragen orientieren (OECD, 2023).

Bestehende Regelwerke (z. B. DSGVO, europäische KI-Verordnung)

Regulatory Sandboxes im Bereich KI operieren nicht im rechtsfreien Raum. Vielmehr müssen sie sich innerhalb eines bereits bestehenden europäischen und nationalen Regelungsrahmens bewegen, der zentrale Aspekte des KI-Einsatzes bereits adressiert. Folgende Regelungen sind dabei von besonderer Relevanz: die **Datenschutz-Grundverordnung (DSGVO),** die **europäische KI-Verordnung** und die **NIS-2-Richtlinie**. Je nach Anwendungsfall kommen weitere Rechtsvorschriften hinzu, z. B. für Medizinprodukte (MDR), FinTech (Payment Services Directive, PSD2), Telekommunikation, Verbraucherschutz und Produkthaftung. Diese flankierenden Regelwerke können zusätzliche Tests, Kennzeichnungspflichten, Marktüberwachungsmaßnahmen und Transparenzanforderungen einfordern.

Die DSGVO regelt bereits zentrale Dimensionen, die für KI-Sandboxprojekte unmittelbar relevant sind. Dies betrifft zum Beispiel die **Verarbeitung personenbezogener Daten**, die **Profilbildung**, die **automatisierte Entscheidungsfindung** sowie die Anforderungen an **Transparenz und Zweckbindung** (Gstrein, 2021). In Sandbox-Kontexten ist besonders relevant, dass die DSGVO **keine experimentellen Ausnahmen** kennt: Auch in einem Testumfeld gelten alle Schutzvorschriften uneingeschränkt, wodurch die Durchführung realitätsnaher Tests mit Nutzerdaten erheblich eingeschränkt ist (Wachter et al., 2017).

Mit der **KI-Verordnung** verfolgt die Europäische Union einen risikobasierten Regulierungsansatz für KI-Systeme. Der Entwurf unterscheidet vier Risikostufen – von „minimal risk" bis „unacceptable risk" – und sieht **strikte Anforderungen für sogenannte Hochrisikoanwendungen** vor (Veale & Zuiderveen Borgesius, 2021). Bereits im Entwurf war

[6] „Principle-based supervision" bei KI Regulatory Sandboxes bedeutet, dass die Aufsicht nicht strikt an festgelegte, detaillierte Regeln gebunden ist, sondern auf übergeordneten Prinzipien und Zielen basiert, wie etwa Innovationsschutz, Risikomanagement, Schutz von Grundrechten und rechtliche Sicherheit für Unternehmen. Die Aufsichtsbehörden üben dabei ihr Ermessen aus, um die spezifischen Anforderungen und Risiken jedes Projekts im Rahmen der Sandbox individuell zu bewerten und zu steuern.

vorgesehen, dass Mitgliedstaaten sogenannte **Regulatory Sandboxes als begleitende Instrumente** einrichten können, jedoch ausschließlich im Rahmen und unter den Bedingungen der europäischen KI-Verordnung (Smuha et al., 2021). Artikel 3 Abs. 55 der KI-VO definiert *KI Regulatory Sandboxes als einen kontrollierten Rahmen, der von einer zuständigen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für die Sandbox einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter Realbedingungen – zu testen.*

Besonders relevant ist, dass die europäische KI-Verordnung keine inhaltliche Ausnahme von ihren Anforderungen innerhalb der Sandbox zulässt, sondern Sandboxes **nur als Unterstützung bei der Umsetzung und Konformitätsprüfung** vorgesehen sind. Sie ermöglichen etwa eine **begleitete Testphase**, bieten aber **keinen Freiraum zur Abweichung** von materiellen Anforderungen. Damit sind sie formal eher als **unterstützendes Prüf- und Dialoginstrument** angelegt, nicht als normative Ausnahmeregelung im engeren Sinne (European Commission, 2023).

Die **NIS-2-Richtlinie** verstärkt die Anforderungen an Cybersicherheit, denen KI-Systeme in Regulatory Sandboxes genügen müssen, insbesondere wenn sie für kritische Infrastrukturen relevant sind. Sandboxes fungieren als kontrollierte Umgebungen, um diese NIS-2-Konformität vor der Markteinführung zu prüfen und zu fördern. Die Einbindung von NIS-2-konformen Sicherheitsmaßnahmen und Meldepflichten wird somit integraler Bestandteil der KI-Regulierung und -Innovation innerhalb dieser Sandboxes.

Darüber hinaus gelten auch sektorale Regelwerke wie die **Medizinprodukteverordnung (MDR)**, das **Produktsicherheitsgesetz** oder die **Antidiskriminierungsgesetzgebung** – etwa wenn KI-Systeme im Gesundheitssystem, im Bildungsbereich oder bei Sozialleistungen eingesetzt werden. Auch hier bestehen **keine temporären Ausnahmen oder Experimentierklauseln** für den Einsatz von KI im Sandbox-Rahmen.

Bestehende Regelwerke wie die DSGVO und die europäische KI-Verordnung legen bereits **einen klaren, restriktiven** Rahmen für KI-Systeme fest. Sie bieten **keine regulatorischen Ausnahmen für Testzwecke**[7], sondern eher formale Orientierungen für die sichere Umsetzung. Sandboxes können im Geltungsbereich dieser Regelungen nur dann operieren, wenn sie mit ihnen **kompatibel ausgestaltet** sind – was sie weniger zu Freiräumen als zu **begleiteten Anwendungsfeldern für risikominimierte Innovation** macht.

Grenzen für KI Regulatory Sandboxes

Trotz ihres Potenzials zur regulatorischen Innovation sind Regulatory Sandboxes im Bereich KI **nicht uneingeschränkt anwendbar**. Ihre Wirksamkeit und Legitimität hängen maßgeblich von der Art des getesteten Systems, dem betroffenen Rechtsbereich und der gesellschaftlichen Risikoakzeptanz ab. In bestimmten Konstellationen sind Sandboxes **weder rechtlich zulässig noch normativ vertretbar**.

[7] Ausgenommen sind hier die Bereiche Forschung und Verteidigungstechnologien.

Eine Grenze ergibt sich bei **verbotenen Anwendungen** im Sinne der europäischen KI-Verordnung. Diese schließt bestimmte KI-Systeme – etwa zu Social Scoring, zur manipulativen Verhaltensbeeinflussung oder biometrischen Massenüberwachung – explizit vom Einsatz aus (European Commission, 2023). Auch eine Erprobung in Sandbox-Form wäre in diesen Fällen **nicht mit Unionsrecht vereinbar**. Die Regelung sieht hier ein vollständiges Verbot vor und einen klaren „Red Line"-Bereich, in dem keine Testausnahmen zulässig sind.

Auch bestehende **Grundrechte**, insbesondere des Datenschutzes, der Nichtdiskriminierung und der informationellen Selbstbestimmung, setzen den Möglichkeiten einer KI Regulatory Sandbox Grenzen. Die DSGVO kennt keine experimentellen Abweichungen – insbesondere nicht bei sensiblen personenbezogenen Daten oder bei vollautomatisierten Entscheidungen ohne menschliche Interventionsmöglichkeit (Wachter et al., 2017).

7.3 PRAKTISCHE ANFORDERUNGEN AN KI-SANDBOXES

KI-Sandboxes stellen hohe Anforderungen an Planung, Umsetzung und Kontrolle. Damit sie wirksam und verantwortungsvoll funktionieren, müssen sie technisch, rechtlich und organisatorisch sauber konzipiert sein. Dieses Kapitel benennt die zentralen Anforderungen an das Design, die Aufsicht und die Beteiligung innerhalb solcher Testumgebungen.

Design und Durchführung

Das Design von KI-Sandboxes muss bereits zu Beginn klären, **welcher Anwendungsbereich, welches Ziel und welches Risikoprofil** getestet werden sollen.

Wichtig ist ein **strukturiertes Verfahren zur Auswahl und Zulassung von Projekten**. Dieses sollte auf nachvollziehbaren Kriterien beruhen, etwa Innovationshöhe, Gemeinwohlbezug, regulatorisches Testinteresse und Risikoangemessenheit (Baasch & Renda, 2021). Auf Basis der Risikoklassifizierung in der europäischen KI-Verordnung sind vor allem Projekte der Risikoklasse mit hohem Risiko relevant. Die Verfahren, Prozesse und administrativen Anforderungen für die Beantragung, Auswahl, Teilnahme und Beendigung der KI-Sandbox müssen einfach, leicht verständlich und klar kommunizierbar sein, um die Teilnahme von KMU, einschließlich Start-ups, mit begrenzten rechtlichen und administrativen Kapazitäten zu erleichtern.

Auch die **Dauer und Skalierung des Tests** müssen definiert werden. Typisch sind begrenzte Zeiträume (z. B. 6–12 Monate) mit klaren Ausstiegsszenarien oder Verlängerungsoptionen. Die Möglichkeit zur stufenweisen Erweiterung wie etwa vom isolierten Laborumfeld in reale Anwendungssituationen erhöht die Anschlussfähigkeit, erfordert aber zusätzliche Kontrollen (Willems & Van Dooren, 2021).

Neben der technischen Testarchitektur ist das **Anspruchsgruppenmanagement** entscheidend: Bereits in der Designphase sollten verschiedene relevante Akteure wie beispielsweise Regulierungsbehörden einbezogen werden. Nur so kann gewährleistet werden, dass die Sandbox nicht zu einem isolierten Technologietest wird, sondern als **regulatorisches Lernformat** wirkt (Yeung et al., 2019).

Rolle von Aufsicht, Ethik und Evaluierung

Damit KI-Sandboxes verantwortungsvoll und rechtskonform funktionieren, bedarf es klarer Mechanismen zur **Aufsicht, Reflexion und begleitenden Evaluation**. Diese Elemente sind nicht nachgelagert, sondern integraler Bestandteil der Sandbox-Architektur und entscheidend für ihre Legitimität.

Die **regulatorische Aufsicht** muss gewährleisten, dass alle bestehenden gesetzlichen Standards (z. B. DSGVO, KI-VO, sektorale Gesetze) auch im Testbetrieb eingehalten werden. Es muss verhindert werden, dass Sandboxes zu rechtsfreien Räumen verkommen oder als solche wahrgenommen werden. Das setzt **Zuständigkeiten, Ressourcen und Verfahren** in den beteiligten Aufsichtsbehörden voraus, die über die klassische Vollzugslogik hinausgehen (Gorwa et al., 2020).

Ein drittes Schlüsselelement ist die **Evaluation**: Jede KI-Sandbox sollte von Beginn an klare Evaluationsziele, Indikatoren und Methoden festlegen. Das soll nicht nur zur Messung technischer Leistungsfähigkeit dienen, sondern auch in Bezug auf Risiken, Nebenwirkungen und Governance-Erkenntnisse (Ansell & Gash, 2018). Dabei muss die Evaluation extern nachvollziehbar und öffentlich dokumentiert sein, um Vertrauen und Lerneffekt sicherzustellen.

Beteiligung von Betroffenen (z. B. Nutzer:innen, Zivilgesellschaft)

Die Einführung von Regulatory Sandboxes im Bereich KI erfordert nicht nur technische und rechtliche Sorgfalt, sondern auch **soziale Anschlussfähigkeit**. Gerade bei Anwendungen, die tief in Lebensrealitäten eingreifen wie im Bereich der Bildung, Arbeit, Gesundheit oder öffentlichen Verwaltung, ist die **aktive Einbindung von Betroffenen und zivilgesellschaftlichen Akteuren** ein zentrales Kriterium für Legitimität.

Transparenz ist dabei ein grundlegendes Prinzip: Zielsetzung, Verfahren, Testergebnisse und Learnings sollten unter Wahrung von Geschäftsgeheimnissen und Schutzrechten öffentlich einsehbar dokumentiert werden. Nur so lässt sich verhindern, dass KI-Sandboxes als „regulatorische Hinterzimmer“ wahrgenommen werden statt als **Teil demokratisch kontrollierter Technologiepolitik**.

7.4 INTERNATIONALE PRAXISBEISPIELE

Mehrere Staaten haben in den vergangenen Jahren Regulatory Sandboxes gezielt eingesetzt, um den Einsatz von KI-Systemen unter kontrollierten Bedingungen zu ermöglichen. Diese Sandboxes fokussieren sich dabei besonders auf hochregulierte Sektoren. Die Ansätze unterscheiden sich dabei hinsichtlich Rechtsrahmen, thematischer Fokussierung, institutioneller Steuerung und Partizipation. Die folgenden Beispiele zeigen unterschiedliche Strategien im Umgang mit KI-bezogenen Regulierungsfragen. Sie geben Hinweise, wie Sandboxes erfolgreich eingesetzt werden können und wo ihre Grenzen in der Praxis liegen. Im Anhang befinden sich weitere ausführliche Good-Practice-Darstellungen von ausgewählten, vielversprechenden Umsetzungsbeispielen.

Frankreich – Datenschutzorientierte KI-Sandbox der Commission Nationale de l'Informatique et des Libertés

Die französische Datenschutzbehörde **Commission Nationale de l'Informatique et des Libertés** (**CNIL)** betreibt seit 2021 eine eigene **Regulatory Sandbox** mit Fokus auf die Vereinbarkeit von KI-Systemen mit der DSGVO. Ziel ist es, im Rahmen der 6-monatigen Supportphase Organisationen dabei zu unterstützen, komplexe KI-Anwendungen unter realitätsnahen Bedingungen **rechtssicher zu entwickeln**, ohne Schutzprinzipien zu unterlaufen.

Der Schwerpunkt liegt auf Projekten mit hoher datenschutzrechtlicher Relevanz, etwa KI-Anwendungen für öffentliche Dienste in den Bereichen Beschäftigung, Versorgung und Transport oder Projekte zur Verbesserung der Gesundheitsversorgung, wie Daten-Sharing-Systeme für häusliche Pflege. Die CNIL bietet dabei keine Ausnahmen von geltendem Recht, sondern begleitet Projekte mit **praxisorientierter Beratung, Risikobewertung und Datenschutzfolgenabschätzungen** (CNIL, 2022). Typischerweise durchlaufen die Projekte ein mehrstufiges Verfahren mit Auswahl, Co-Kreation, Evaluierung und Ergebnisveröffentlichung.

Ein zentraler Erfolgsfaktor ist die **institutionelle Autorität der CNIL** sowie die Einbindung von **externen Anspruchsgruppen** aus Forschung, Ethik und Zivilgesellschaft. Diese breite Beteiligungsbasis wurde als Erfolgsfaktor festgehalten. Die Sandbox hat nicht nur praktische Datenschutzlösungen ermöglicht, sondern auch zur internen Kapazitätsentwicklung der Aufsichtsbehörde beigetragen (OECD, 2023).

Deutschland – Vorbereitung auf KI-Sandboxes im Rahmen der europäischen KI-Verordnung

Deutschland verfolgt bislang keinen expliziten KI-Sandbox-Ansatz, hat jedoch in mehreren Bereichen regulatorische Testformate. Im Rahmen der nationalen Reallabor-Strategie des **Bundesministeriums für Wirtschaft und Klimaschutz (BMWK)** wurden seit 2020 Rahmenbedingungen für regulatorisches Testen erarbeitet, die nun auf KI-Use-Cases übertragen werden sollen (BMWK, 2021). Im Zusammenhang mit der europäischen KI-Verordnung arbeitet Deutschland aktuell an der Einrichtung sektorspezifischer Sandbox-Infrastrukturen im Bereich Mobilität, Verwaltung und Gesundheit (siehe Fallvignette im Anhang). Diese sollen dazu dienen, Hochrisiko-KI-Anwendungen unter strenger Aufsicht und auf Basis EU-rechtlicher Konformitätsanforderungen zu testen.

Damit bereitet Deutschland regulatorisch und institutionell die Voraussetzungen für KI-bezogene Sandboxes vor, ohne sie bereits flächendeckend implementiert zu haben – ein Ansatz, der stark auf **Rechtsklarheit und föderale Koordination** setzt.

Großbritannien – Information Commissioner's Office (ICO) Sandbox

In Großbritannien betreibt das **ICO** seit 2019 eine **regulatorische Sandbox**, die sich auf datengetriebene Innovationen mit KI-Bezug konzentriert. Ziel ist es, Unternehmen und Organisationen bei der **datenschutzkonformen Entwicklung neuer Technologien** zu unterstützen, ohne Innovation zu behindern.

Ein Merkmal der ICO Sandbox ist, dass sie sich an Organisationen wendet, deren Projekte ein hohes gesellschaftliches Potenzial aufweisen. Anwendungsbeispiele reichen von Gesundheit und digitaler Bildung bis hin zum Bereich der Finanztechnologie. Erklärtes Ziel war es, **neuartige datenschutzrechtliche Fragestellungen** aufzuwerfen und entsprechende regulatorische Anpassungen vorzunehmen. Anders als viele andere Modelle erlaubt die ICO Sandbox **eine enge Kooperation zwischen Aufsicht und Projektteams**, bei der gemeinsam konkrete Lösungen für Datenschutzfragen entwickelt werden (ICO, 2021). Dieser Austausch wurde als wesentlicher Erfolg dargestellt.

Die Sandbox ist nicht als rechtsfreier Raum konzipiert, sondern als **strukturierte, betreute Testumgebung** mit klaren Anforderungen, z. B. zur Transparenz, zum Umgang mit sensiblen Daten und zur Rechenschaftspflicht. In vielen Fällen wurde das Modell genutzt, um **praktische Umsetzungshilfen für Art. 25 DSGVO (Privacy by Design)** zu erarbeiten oder Verfahren zur erklärbaren KI zu evaluieren[8] (Veale et al., 2021).

Besonders hervorzuheben ist, dass das ICO explizit auf **gesellschaftlichen Mehrwert, Anspruchsgruppenbeteiligung und evidenzbasierte Reflexion** setzt. Die Sandbox dient dabei nicht nur der einzelnen Projektförderung, sondern auch dem Aufbau von systemischem Regulierungswissen in einem dynamischen Technologiefeld und ermöglicht die Abstimmung relevanter Anspruchsgruppen.

Singapur – Agile KI-Governance mit Sandbox-Elementen

Auch außereuropäisch werden verschiedene Sandbox-Modelle im Bereich KI erprobt. Singapur verfolgt seit mehreren Jahren einen gezielt **agilen Ansatz in der Regulierung von KI-Technologien**. Bereits 2019 wurde im Rahmen der nationalen AI Strategy das Prinzip der **„soft law"-Regulierung** eingeführt. Dieses hat zum Ziel, durch freiwillige Rahmenwerke, kooperative Testphasen und flexible sandboxähnliche Formate Innovationsspielräume zu eröffnen, ohne regulatorische Schutzstandards zu vernachlässigen.

Im Zentrum steht das durch die Datenschutzbehörde Personal Data Protection Commission (**PDPC)** entwickelte **Model AI Governance Framework**, welches Unternehmen, KMU und Start-ups bei der ethischen und rechtssicheren Entwicklung von KI-Systemen unterstützt. Es enthält Leitlinien zu Fairness, Erklärbarkeit, Human Oversight und Data Governance und wurde mehrfach durch **regulatorische Pilotprojekte (Use Cases)** weiterentwickelt (PDPC, 2020).

Die singapurische Praxis unterscheidet sich von europäischen Ansätzen dadurch, dass **mehr mit regulatorischer Vorfeldberatung und kooperativer Compliance gearbeitet wird**, anstatt formal zugelassene Testumgebungen mit rechtlich definierten Ausnahmen zu schaffen. Die Pilotprojekte sind typischerweise **kurzfristig, sektorspezifisch und durch staatlich moderierte Co-Kreation geprägt** (Rajkomar & Tan, 2022). Dabei ist hervorzuheben, dass Singapur besonders auf die **Anschlussfähigkeit an internationale Standards** (z. B. OECD,

[8] Die Evaluierung von Verfahren für erklärbare KI (Explainable AI, XAI) erfolgt am besten durch ein systematisches Vorgehen, das Kriterien wie Verständlichkeit, Treue (Fidelity), Nützlichkeit und Vertrauenswürdigkeit in den Mittelpunkt stellt. Die Wahl und Gewichtung dieser Kriterien hängt stark vom Anwendungsfall, den Anforderungen der Nutzer und gegebenenfalls regulatorischen Vorgaben ab.

G20) achtet – etwa durch „Sandbox Interoperability Guidelines“, die eine Kompatibilität mit der europäischen KI-Verordnung und ähnlichen Regimen ermöglichen sollen (OECD, 2023).

Kanada – Sektorale Sandboxes mit Fokus auf Gesundheit und FinTech

Kanada setzt bei der Umsetzung von Regulatory Sandboxes auf einen starken sektoralen Zugang, insbesondere in Bereichen mit hoher Innovationsdynamik. Im Gesundheitswesen hat **Health Canada** beispielsweise eine experimentelle Zulassungsumgebung für neuartige Technologien wie KI-gestützte Diagnostik oder 3D-gedruckte Medizinprodukte geschaffen. Die Sandbox ermöglicht Unternehmen, in enger Zusammenarbeit mit der Behörde risikobasierte Zulassungswege zu entwickeln, ohne regulatorische Standards zu unterlaufen (Health Canada, 2021).

Im Finanzbereich betreiben die **Canadian Securities Administrators (CSA)** seit 2017 eine Sandbox, die FinTech-Unternehmen erlaubt, innovative Geschäftsmodelle unter behördlicher Aufsicht zu testen. Dabei steht die Verhältnismäßigkeit von Aufsichtspflichten und Innovationsgrad im Mittelpunkt. Projekte werden individuell begleitet, um potenzielle Rechtsunsicherheiten frühzeitig zu adressieren (CSA, 2017). Die kanadische Praxis zeigt, wie durch gezielte, behördennahe Experimentierräume sowohl regulatorische Klarheit als auch Innovationsförderung geschaffen werden können und das ohne strukturelle Ausnahme vom geltenden Recht.

Japan – sektorübergreifende Sandbox mit Fokus auf regulatorische Reform

Japan etablierte 2018 eine sektorübergreifende Regulatory Sandbox im Rahmen des Gesetzes zur Förderung der Produktivität in verschiedenen Bereichen. Unter der Koordination des Kabinettssekretariats ermöglicht die Sandbox auch internationalen Unternehmen, innovative Technologien wie KI, IoT oder Blockchain in realen Umgebungen zu testen, selbst wenn dem bestehende Vorschriften entgegenstehen. Während viele Länder Regulatory Sandboxes nutzen, um heimischen Unternehmen einen globalen Wettbewerbsvorteil bei Zukunftstechnologien zu ermöglichen, verfolgt Japan diesen Sonderweg der Öffnung, um für internationale Investments attraktiv zu sein. Diese Strategie könnte auch für kleine offene Ökonomien, wie jene Österreichs, erfolgversprechend sein. Die Projekte sind zeitlich begrenzt und unterliegen klaren Bedingungen, wobei die gewonnenen Daten zur Evaluierung und möglichen Anpassung von Regularien genutzt werden.

Ein herausragendes Beispiel ist die Erprobung von E-Scooter-Sharing-Diensten durch Unternehmen wie Luup. Die gesammelten Daten führten zur Anpassung des Straßenverkehrsgesetzes, wodurch E-Scooter unter bestimmten Bedingungen ohne Helm und Führerschein genutzt werden dürfen. Bis 2021 wurden über 30 Projekte genehmigt, die zu konkreten regulatorischen Reformen in Bereichen wie FinTech, Mobilität und Gesundheitstechnologie beitrugen.

Australien – Enhanced Regulatory Sandbox mit sektoraler Ausweitung

Australien implementierte 2020 die „Enhanced Regulatory Sandbox“ (ERS), die von der Australian Securities and Investments Commission (ASIC) verwaltet wird. Die ERS ermöglicht es Unternehmen, innovative Finanzdienstleistungen und Kreditaktivitäten für bis zu 24 Monate ohne vorherige Lizenzierung zu testen, sofern bestimmte Bedingungen erfüllt sind. Ziel ist es, Innovationen zu fördern, ohne den Verbraucherschutz zu vernachlässigen.

Zusätzlich hat die Australian Border Force (ABF) eine Sandbox für den Zollbereich eingeführt, um technologische Innovationen in der Handelsabwicklung zu testen. Diese kontrollierten Versuche dienen als Grundlage für zukünftige regulatorische und technologische Reformen im Zoll- und Grenzbereich. Damit zeigt Australien neue Anwendungsfälle auf, die in anderen Ländern weniger im Fokus stehen. Ein Ziel dieser Gegenüberstellung internationaler Beispiele ist aufzuzeigen, dass es eine Bandbreite von sektoralen Beispielen, Governance-Gestaltungen und allgemeinen Zugängen zu Sandboxes gibt. Australien verfolgt zudem einen risikobasierten Ansatz in der KI-Regulierung, der die Einführung von KI-spezifischen Sandboxes vorsieht. Diese sollen es ermöglichen, KI-Technologien in einem überwachten Umfeld zu testen und gleichzeitig regulatorische Standards zu wahren.

EU – EUSAiR (EU Regulatory Sandboxes for AI) Projekt

Das EUSAiR-Projekt ist ein von der Europäischen Union im Rahmen des Digital-Europe-Programms gefördertes zweijähriges Projekt, das darauf abzielt, die Umsetzung von KI Regulatory Sandboxes in den EU-Mitgliedstaaten zu unterstützen.

Die Universität Bologna leitet das Projekt, das darauf abzielt, standardisierte Rahmenwerke für KI-Sandboxes in der EU zu entwickeln. Italienische Partner, darunter das Italian Computing and Storage Consortium (ICSC), arbeiten daran, sektorübergreifende Pilotprojekte zu implementieren, die als Grundlage für die Umsetzung der europäischen KI-Verordnung dienen sollen. Das Ziel ist es, einheitliche Standards zu schaffen, die den Aufbau von KI-Sandboxes in den Mitgliedstaaten erleichtern. Es handelt sich bei EUSAiR um ein Vorzeigeprojekt und Vorgänger für grenzüberschreitende Kooperation.

Unter der Leitung des **CSC – IT Center for Science** führt **Finnland** einen der drei Pilotversuche durch, die darauf abzielen, die Effektivität von KI-Sandboxes zu testen und zu validieren. Ein besonderer Schwerpunkt liegt auf der Integration von KI-Sandboxes in bestehende Hochleistungsrechner-Infrastrukturen, wie dem LUMI-Supercomputer, um die Entwicklung und das Testen von KI-Systemen in großem Maßstab zu ermöglichen. Das Projekt zielt darauf ab, rechtliche Klarheit für Innovatoren zu schaffen und den Marktzugang für KMU zu erleichtern.

7.5 ANFORDERUNGEN UND ABGELEITETE ERKENNTNISSE FÜR DIE UMSETZUNG

Die Analyse internationaler Beispiele, rechtlicher Rahmenbedingungen und institutioneller Positionen zeigt: Regulatory Sandboxes können ein wirksames Instrument zur kontrollierten Erprobung und Regulierung von KI-Anwendungen sein – vorausgesetzt, sie sind rechtsstaatlich abgesichert, interdisziplinär gesteuert und mit klarer Lernorientierung verbunden.

Österreich verfügt bereits über erste sektorale Pilotansätze und strategische Bezugspunkte. Was bislang fehlt, ist eine kohärente, rechtskonforme und auf künstliche Intelligenz bezogene Umsetzung. Dieses Kapitel fasst zentrale Anforderungen zusammen, die sich aus den vorangegangenen Befunden ergeben – insbesondere hinsichtlich rechtlicher Grundlagen, institutioneller Voraussetzungen, Pilotfeldern, Governance und der europäischen Einbettung.

Es schafft damit die analytische Grundlage für die **konkreten Empfehlungen und Handlungsoptionen**, die in **Kapitel 8** systematisch weiterentwickelt werden.

Rechtliche und institutionelle Grundlagen sichern

Gemäß Art 75 Abs. 2 der europäischen KI-Verordnung müssen die Mitgliedstaaten sicherstellen, dass ihre zuständigen Behörden auf nationaler Ebene mindestens eine Sandbox für KI-Regulierung einrichten, die bis zum 2. August 2026 betriebsbereit sein muss. Hierfür sind die folgenden drei zentralen Anforderungen für die nationale Umsetzung in Österreich wichtig:

1. **Allfällige nationale Anpassungen zum EU-Durchführungsrechtsakt zu KI Regulatory Sandboxes vornehmen:** Um eine Fragmentierung in der Union zu vermeiden, erlässt die Kommission Durchführungsrechtsakte zur Festlegung der detaillierten Modalitäten für die Einrichtung, Entwicklung, Durchführung, den Betrieb und die Beaufsichtigung der KI Regulatory Sandboxes (EU KI-VO, Art. 58 Abs. 1). Es kann in der Praxis notwendig sein, nationale Rechtsvorschriften anzupassen, um detaillierte oder spezifische Regelungen zu konkretisieren oder nationale Verwaltungsverfahren entsprechend anzupassen. Dies erfolgt aber nicht durch eine eigentliche Umsetzung des Durchführungsrechtsakts selbst, sondern als begleitende Maßnahme zur Gewährleistung der einheitlichen Anwendung des EU-Rechts.
2. **Zuständigkeiten koordinieren:** Die Einführung von Sandboxes berührt mehrere politische und regulatorische Zuständigkeitsbereiche. Eine klare Aufgabenteilung zwischen Kanzleramt, Fachressorts, Datenschutzbehörde und anderen Anspruchsgruppen wie Förderinstitutionen ist Voraussetzung für eine funktionierende Umsetzung. Eine übergreifende Koordinierungsstelle kann helfen, Doppelstrukturen zu vermeiden und die Kohärenz sicherzustellen. Außerdem sollten die Marktüberwachungsbehörden[9] Tests unter realen Bedingungen beaufsichtigen (im Rahmen von Regulatory Sandboxes oder außerhalb; Art. 76 KI-VO) und technische Tests auf Anfrage der Behörden/öffentlichen Stellen für Grundrechte durchführen (Art. 77 Abs. 3 KI-VO).
3. **Notwendige Ressourcen und Kompetenzen sicherstellen:** Für den Betrieb von KI-Sandboxes braucht es eine institutionelle Einheit mit rechtlicher, technischer und administrativer Kompetenz. Diese muss in der Lage sein, Projekte aufzunehmen, zu begleiten, zu bewerten und die Ergebnisse systematisch zurückzuspielen. Bestehende

[9] Diese sind: Das Bundesamt für Sicherheit im Gesundheitswesen (BASG) in Kombination mit der Agentur für Gesundheit und Ernährungssicherheit (AGES) für Medizinprodukte und In-Vitro Diagnostika; das Bundesamt für Verbrauchergesundheit (BAVG) in Kombination mit der AGES für Spielzeug; die oberste Seilbahnbehörde für Seilbahnen; das Fernmeldebüro für Funkanlagen; das Bundesamt für Eich- und Vermessungswesen (BEV) für Maschinen, Sportboote, Geräte zur Verwendung in explosionsgefährdeten Bereichen, persönliche Schutzausrüstung, Geräte zur Gasverbrennung, Druckgeräte und Aufzüge; die Finanzmarktaufsicht (FMA) betreffend Punkt 5 b und c im von der FMA regulierten Bereich sowie die Datenschutzbehörde (DSB).

Einrichtungen wie die FFG, aws oder AI Factory können hierbei eine Rolle übernehmen, sofern ausreichende Kapazitäten und klare Zuständigkeiten vorhanden sind. Für den Betrieb sind die erforderlichen Ressourcen im öffentlichen Haushalt vorzusehen.

Zielgerichtete Pilotierung mit Fokus auf Hochrisikoanwendungen

Ein flächendeckender Start von KI-Sandboxes wäre politisch und organisatorisch schwer steuerbar. Deutlich sinnvoller erscheint ein gestuftes Vorgehen, das zunächst auf Pilotprojekte in besonders sensiblen Anwendungsfeldern setzt. Hochrisikoanwendungen bieten sich hierfür besonders an, da sie nicht nur technischen, sondern auch rechtlichen und gesellschaftlichen Prüfbedarf erzeugen.

Gerade in Bereichen wie Gesundheitsversorgung, Bildungswesen oder öffentlicher Verwaltung besteht ein hoher Bedarf, KI-Systeme in kontrollierten Umgebungen zu testen, bevor sie in den Regelbetrieb übergehen. So könnte beispielsweise die algorithmische Entscheidungsunterstützung in der medizinischen Diagnostik oder in der Sozialverwaltung auf ihre praktische Tauglichkeit, ihre Rechtskonformität und ihre gesellschaftliche Akzeptanz hin geprüft werden. Auch adaptive Lernsysteme in Schulen oder Hochschulen und datengetriebene Mobilitätslösungen zählen zu den Bereichen, in denen Pilotierungen wertvolle Erkenntnisse liefern können. Entscheidend ist, dass die Auswahl der Pilotfelder nachvollziehbar erfolgt – auf Basis gesellschaftlicher Relevanz, Innovationspotenzial, Grundrechtsnähe und Testbarkeit.

Solche Projekte sollten nicht isoliert durchgeführt werden, sondern eingebettet in ein strukturiertes Verfahren, das technische, rechtliche und ethische Aspekte gleichermaßen berücksichtigt. Eine systematische Begleitung, etwa durch Evaluationsgremien oder wissenschaftliche Einrichtungen, kann dabei helfen, Erfahrungen zu dokumentieren und praxisrelevante Rückschlüsse zu ermöglichen. Dabei sollte eine schrittweise Pilotierung vorgenommen werden, da sie mehrere Vorteile bietet. Sie ermöglicht es, erste praktische Erfahrungen mit Sandbox-Prozessen zu sammeln, institutionelle Abläufe zu erproben und potenzielle Risiken frühzeitig zu erkennen. Gleichzeitig kann sie helfen, das Vertrauen von Verwaltung, Wirtschaft und Öffentlichkeit in das neue Instrument zu stärken. Ein Fokus auf Hochrisikobereiche steht zudem in Einklang mit der Systematik der europäischen KI-Verordnung, die für besonders sensible Anwendungen spezifische Anforderungen an Testumgebungen formuliert. Damit wird auch die europäische Anschlussfähigkeit sichergestellt.

Governance: Partizipativ, interdisziplinär, evaluierbar

Die Steuerung von KI Regulatory Sandboxes stellt besondere Anforderungen. Aufgrund der technologischen Komplexität, der grundrechtlichen Sensibilität und der hohen gesellschaftlichen Relevanz vieler KI-Anwendungen reicht eine klassische verwaltungsinterne Organisation nicht aus. Stattdessen ist eine Governance-Struktur erforderlich, die verschiedene Wissensbereiche, Perspektiven, gesellschaftliche und wirtschaftliche Interessen systematisch einbezieht mit dem Ziel, eine kooperative Beziehung zwischen Regulierungsbehörden und den betroffenen Parteien zu unterstützen. Ein solches Format muss drei zentrale Merkmale aufweisen:

- **Partizipation:** Betroffene Gruppen, z. B. Unternehmen, Akteure aus der Zivilgesellschaft oder KI-Forschungszentren, sollten bereits in der Projektvorbereitung und im Testbetrieb eingebunden werden. Dies erhöht die Transparenz, die Legitimität und die Akzeptanz der Ergebnisse.
- **Interdisziplinarität:** Neben technischer und juristischer Expertise braucht es praktische, sozialwissenschaftliche und ethische Perspektiven. Nur so lassen sich die technische Umsetzung und Auswirkungen auf Grundrechte, Arbeitsverhältnisse oder gesellschaftliche Teilhabe angemessen beurteilen.
- **Evaluierbarkeit:** Sandbox-Projekte müssen systematisch begleitet und dokumentiert werden. Die Auswertung der Erfahrungen etwa zu Rechtsunsicherheiten, Interoperabilität oder Umsetzungshindernissen bildet die Grundlage für regulatorisches Lernen.

Internationale Vorbilder wie die britische Datenschutzaufsicht ICO oder die französische CNIL zeigen, wie Sandboxes als kooperativ gesteuerte Formate funktionieren können. Auch in Österreich bestehen bereits erste Gremien und Plattformen, an die angeknüpft werden kann, etwa der Fachbeirat Ethik der Künstlichen Intelligenz oder sektorale Evaluierungsstellen. Wichtig ist, diese Strukturen nicht isoliert zu nutzen, sondern in eine koordinierte Sandbox-Governance einzubinden.

Europäische Einbettung und Anschlussfähigkeit

Wichtige Gestaltungsprinzipien sind:

- inhaltliche Abstimmung mit der Risikologik der europäischen KI-Verordnung,
- Anschlussfähigkeit an bestehende europäische Test- und Förderarchitekturen,
- Einbeziehung von Unternehmen, insb. KMU, durch transparente Verfahren, technische Unterstützung und vertretbaren Ressourceneinsatz.

Europäische Kompatibilität ist nicht nur rechtlich notwendig, sondern auch strategisch vorteilhaft. Sie erleichtert die internationale Anerkennung von Testergebnissen, stärkt die Anschlussfähigkeit österreichischer Unternehmen und fördert eine einheitliche Innovations- und Regulierungslandschaft. Frühzeitige Abstimmungen auf EU-Ebene – etwa über Pilotprogramme oder bilaterale Kooperationen – können helfen, nationale Aktivitäten wirksam einzubetten und internationale Sichtbarkeit zu schaffen.

Regulatorisches Lernen im KI-Bereich ermöglichen

KI-Sandboxes bieten die Möglichkeit, technische Innovation und rechtliche Steuerung in einem kontrollierten Rahmen zusammenzuführen. Ihr eigentlicher Mehrwert liegt nicht allein in der Testbarkeit neuer Anwendungen, sondern in der Chance, systematisch –über rechtliche Graubereiche, unerwartete Nebenwirkungen, institutionelle Reibungsverluste und gesellschaftliche Anforderungen zu lernen.

Regulatorisches Lernen bedeutet, bestehende Normen an neuen Entwicklungen zu spiegeln und auf dieser Basis fundierte Anpassungen vorzunehmen. Damit dies gelingt, braucht es eine

Sandbox-Architektur, die nicht auf punktuelle Erprobung zielt, sondern auf Rückkopplung in den Rechtssetzungs- und Vollzugskontext (Kanton Zürich 2024).

Für KI-Sandboxes bedeutet das konkret, das zum einen Unsicherheiten bei der Anwendung der europäischen KI-Verordnung und anderer Normen dokumentiert und systematisch analysiert werden müssen. Zum anderen müssen die Auswirkungen von Hochrisiko-KI auf Grundrechte, Transparenz und Aufsichtspraxis sowie Hürden bei der technischen Umsetzung der Anforderungen nachvollziehbar erprobt und bewertet werden. Die Ergebnisse müssen in der Sandbox seitens der Aufsichtsbehörde erfasst werden und dann politischen, regulatorischen und unternehmerischen Stellen zur Verfügung stehen – in strukturierter, nachvollziehbarer Form.

Solches Lernen ist kein Nebeneffekt, sondern Kernaufgabe einer modernen Governance im KI-Bereich. Es erfordert verbindliche Evaluationsstandards, interdisziplinäre Begleitung und eine Infrastruktur, die den Wissenstransfer zwischen Verwaltung, Wissenschaft und Praxis sicherstellt. Nur so kann Österreich im Umgang mit KI nicht nur rechtlich reagieren, sondern strategisch gestalten.

7.6 SPANNUNGSFELDER UND UMSETZUNGSHÜRDEN FÜR KI-SANDBOX-MODELLE

Die Umsetzung von Regulatory Sandboxes im Bereich künstlicher Intelligenz wirft eine Vielzahl an Spannungsfeldern und praktischen Herausforderungen auf. Sie betreffen nicht nur technische oder administrative Aspekte, sondern spiegeln auch tieferliegende Zielkonflikte zwischen Innovationspolitik, Grundrechtsschutz, Marktlogik und gesellschaftlicher Verantwortung wider.

Vier strategische Spannungsachsen lassen sich besonders deutlich identifizieren:

- **Regulierungsbedarf und Innovationsfreiheit:** Der Wunsch nach beschleunigter KI-Erprobung trifft auf die Verpflichtung, bestehende Schutzstandards nicht zu unterlaufen.
- **Datennutzung und Datenschutz:** Die Nutzung datenbasierter Systeme – etwa in Medizin, Verwaltung oder Bildung – gerät rasch in Konflikt mit Anforderungen der DSGVO oder ePrivacy-Richtlinie.
- **Vertrauen und Governance:** Ohne nachvollziehbare Steuerung, transparente Verfahren und legitime Beteiligung drohen Vertrauensverluste – sowohl bei Nutzer:innen als auch in der Öffentlichkeit.
- **Nationale Spielräume und internationale Konvergenz:** Während die europäische KI-Verordnung gemeinsame Mindeststandards schafft, bleibt Raum für nationale Ausgestaltung – mit Spannungen zwischen Harmonisierung und eigenständiger Innovationspolitik.

Diese übergeordneten Spannungslinien prägen die konkrete Umsetzungspraxis. Im Folgenden werden zentrale Umsetzungshürden systematisch entfaltet – von rechtlichen Unklarheiten über sektorale Unterschiede bis hin zu Fragen der Steuerung und Zugänglichkeit. Die Analyse stützt sich auf internationale Erfahrungen, nationale Rahmenbedingungen und Rückmeldungen zentraler Anspruchsgruppen.

Regulierungsbedarf und Innovationsfreiheit

Das Spannungsfeld zwischen regulatorischer Sicherheit und innovationsfördernden Freiräumen ist ein zentrales Thema bei der Umsetzung von KI-Sandbox-Modellen. Während Befürworter:innen von Regulatory Sandboxes auf das Potenzial zur beschleunigten Erprobung neuer Technologien verweisen, betonen Kritiker:innen die Gefahr, dass Schutzstandards verwässert oder rechtliche Grauzonen ausgeweitet werden könnten.

Insbesondere bei Hochrisiko-KI-Anwendungen (z. B. in der Gesundheitsversorgung oder bei automatisierten Verwaltungsentscheidungen) stellt sich die Frage, wie viel Flexibilität in der Testphase rechtlich und ethisch vertretbar ist. Die europäische KI-Verordnung selbst sieht keine materiellen Ausnahmen von bestehenden Rechtsnormen vor, erlaubt jedoch in definierten Grenzen auch Tests unter realen Bedingungen, sofern diese überwacht, zeitlich befristet und risikominimierend ausgestaltet sind.

In der Praxis zeigt sich **ein Zielkonflikt**: Einerseits besteht der Anspruch, Innovationsprozesse nicht durch administrative Hürden oder regulatorische Unsicherheit zu verzögern. Andererseits müssen Normklarheit, Grundrechtsschutz und rechtsstaatliche Prinzipien gewahrt bleiben – gerade bei sensiblen Technologien.

Hinzu kommt eine **unterschiedliche Bewertung des Innovations- vs. Vorsorgeprinzips** zwischen Akteuren aus Verwaltung, Wirtschaft und Zivilgesellschaft. Während manche Institutionen den Fokus auf technologieoffene Ermöglichung legen, sehen andere in der vorauseilenden Regulierung eine Schutzvoraussetzung für gesellschaftliche Akzeptanz.

Die Herausforderung liegt weniger in einer binären Entscheidung, sondern in der Ausgestaltung intelligenter Regelungsmechanismen, die beides leisten: Innovation ermöglichen, ohne Regulierung auszusetzen, und Regulierung weiterentwickeln, ohne Innovation zu behindern.

Datenschutz und Datennutzung

Die Nutzung personenbezogener Daten ist ein zentrales Element vieler KI-Anwendungen – sei es in der medizinischen Diagnostik, in der öffentlichen Verwaltung oder im Bildungsbereich. Zugleich zählt der Datenschutz zu den sensibelsten und am strengsten regulierten Bereichen des europäischen Rechtsrahmens. Zwischen diesen beiden Polen – dem Bedürfnis nach umfangreicher Datennutzung für innovative KI-Systeme und dem Anspruch auf informationelle Selbstbestimmung – besteht ein dauerhaftes Spannungsfeld.

Die DSGVO setzt hier klare Grenzen, die auch in einer Regulatory Sandbox nicht aufgehoben werden dürfen. Anders als in klassischen Reallaboren gibt es im Datenschutz keine materiellen Ausnahmen für Testumgebungen. Dies begrenzt die Spielräume für die Entwicklung und Erprobung datenintensiver KI-Systeme, insbesondere dann, wenn Trainingsdaten aus sensiblen Bereichen wie Gesundheit, Soziales oder Bildung erforderlich sind.

Gleichzeitig zeigen viele Projekte, dass gerade im Umgang mit Daten zentrale Erkenntnisse über Risiken, Verzerrungen oder Diskriminierungspotenziale gewonnen werden können – Erkenntnisse, die außerhalb strukturierter Tests oft verborgen bleiben.

In der Praxis wird von Anspruchsgruppen eine **praxisnahe Auslegung und engmaschige Begleitung durch Datenschutzbehörden** gefordert. Begleitgremien, Datenschutz-Folgenabschätzungen, standardisierte Verfahren und transparente Rechenschaftspflichten können dazu beitragen, rechtliche Sicherheit zu schaffen, ohne das Innovationspotenzial datengetriebener KI-Systeme zu blockieren.

Vertrauen und Governance

Regulatory Sandboxes im Bereich KI sind nicht nur technische oder rechtliche Experimentierräume, sondern politische und gesellschaftliche Signale. Ihre Legitimität steht und fällt mit dem Vertrauen der beteiligten Akteure und der Öffentlichkeit in das Verfahren, die Ziele und die Steuerung solcher Testumgebungen.

Vertrauen entsteht nicht automatisch, sondern muss aktiv durch transparente, nachvollziehbare und inklusive Prozesse aufgebaut werden. **Zentrale Anforderungen für vertrauenswürdige Sandbox-Governance sind**:

- **Klar definierte Zuständigkeiten** für Auswahl, Steuerung, Begleitung und Beendigung von Projekten.
- **Einbindung unterschiedlicher Perspektiven** aus Wirtschaft, Zivilgesellschaft, Forschung und Aufsicht.
- **Verlässliche Rückkopplungsmechanismen**, durch die Erkenntnisse aus Sandbox-Prozessen systematisch in Regulierung, Aufsicht und Politik einfließen.

In mehreren Workshops innerhalb des vorliegenden Projekts wurde betont, dass **fehlende Transparenz und unklare Rollenverteilungen** zu Vertrauensverlust führen können sowohl auf Seiten der Unternehmen als auch bei Betroffenen oder der Öffentlichkeit. Dies gilt besonders für Entscheidungen über die Zulassung zu Sandboxes, die Bewertung von Risiken oder die Aufbereitung von Ergebnissen.

Erfolgreiche Sandbox-Governance erfordert daher ein **ausgewogenes Verhältnis zwischen Steuerung** (klare Regeln, Zuständigkeiten, Verfahren) und Offenheit (Teilhabe, Feedback, öffentliche Rechenschaft). Vertrauen ist dabei kein Selbstzweck, sondern eine **Bedingung für das Gelingen** regulatorischer Testformate im Bereich KI. Nur wenn Beteiligte darauf vertrauen können, dass Risiken ernst genommen, Ergebnisse reflektiert und Prozesse fair gestaltet sind, wird das Instrument langfristig akzeptiert und nutzbar.

Internationalisierung von Regeln vs. nationale Spielräume

Die Regulierung von KI findet zunehmend im europäischen und internationalen Rahmen statt. Mit der **europäischen KI-Verordnung** wird ein einheitlicher Rechtsrahmen geschaffen, der den sicheren, transparenten und ethisch vertretbaren Einsatz von künstlicher Intelligenz (KI) gewährleistet; und das einschließlich Regelungen für Regulatory Sandboxes. Gleichzeitig stehen nationale Akteure vor der Herausforderung, eigene Innovations- und Regulierungsstrategien innerhalb dieses Rahmens zu entwickeln.

Dieses Spannungsfeld zwischen europäischer Harmonisierung und nationaler Gestaltungsfreiheit prägt die Debatte um KI-Sandboxes in besonderem Maße.

Auf der einen Seite bieten gemeinsame Regeln **Rechtssicherheit, Marktintegration und Kompatibilität**. Sandbox-Projekte, die sich an EU-Vorgaben orientieren, können einfacher skaliert, validiert und international anerkannt werden. Das gilt auch für Konformitätsbewertungen, Dokumentationspflichten oder Kriterien für Hochrisiko-KI.

Auf der anderen Seite braucht es **nationale Spielräume**, um Regulatory Sandboxes gezielt an spezifische Gegebenheiten anzupassen – etwa an sektorale Regime, verwaltungstechnische Abläufe oder gesellschaftliche Präferenzen. Gerade im Bereich öffentlicher Daseinsvorsorge (z. B. Verwaltung, Bildung, Gesundheit), aber auch bei KI-Systemen in wirtschaftsrelevanten kritischen Bereichen, kann eine zu enge Auslegung europäischer Vorgaben lokale Innovationen behindern.

Daraus ergeben sich drei zentrale Herausforderungen:

- **Interpretationsspielräume nutzen**: Der Artikel 58 Abs. 2 der europäischen KI-Verordnung lässt gewisse nationale Gestaltungsräume zu[10] – diese sollten genutzt, aber nicht überstrapaziert werden.
- **Kompatibilität sichern**: Nationale Sandboxes müssen so konzipiert sein, dass ihre Ergebnisse anschlussfähig an europäische Prozesse und Standards bleiben.
- **Koordination stärken**: Es braucht Strukturen, um frühzeitig mit EU-Institutionen, anderen Mitgliedstaaten und Standardisierungsgremien in Austausch zu treten.

Eine zentrale Frage ist, wie Sandboxes **als Brücke** zwischen lokalen Bedarfen und europäischen Anforderungen gestaltet werden können und das nicht im Sinne nationaler Sonderwege, sondern als *testbasierte Beiträge* zur europäischen Innovations- und Regulierungspolitik.

[10] Vor allem Art. 58 Abs. 2 lit. c: „…dass die detaillierten Regelungen und Bedingungen für KI-Reallabore so gut wie möglich die Flexibilität der zuständigen nationalen Behörden bei der Einrichtung und dem Betrieb ihrer KI-Reallabore unterstützen."

8 Handlungsempfehlungen

Dieses Kapitel formuliert zentrale Handlungsempfehlungen für Entscheidungsträger:innen in Politik, Verwaltung und Förderinstitutionen. Die Vorschläge orientieren sich an den zuvor identifizierten Herausforderungen und leiten konkrete Schritte zur Umsetzung, Steuerung und Weiterentwicklung von KI-Sandbox-Modellen ab. Die Empfehlungen gliedern sich in sechs Bereiche, die unten dargestellt sind.

8.1 GESETZLICHE UND REGULATORISCHE VORAUSSETZUNGEN

Ein rechtlicher und regulatorischer Rahmen sollte (unter Berücksichtigung des aktuellen Entwurfs des EU-Durchführungsrechtsakts zu KI Regulatory Sandboxes) zumindest die folgenden Elemente beinhalten:

- **Klare Begriffsbestimmung** und **Anwendungsbereich**
- **Zulassungsvoraussetzungen** und Regelungen für die **Bewerbung bzw. Auswahl** von Bewerber:innen
- **Verfahrensregeln zur Umsetzung eines KI-Regulatory-Sandbox-Projektes**
- Beachtung bestehender **Schutzstandards**
- **Rückkopplung und Wissensintegration** auf der Verwaltungsseite

Eine gesetzlich abgesicherte Testinfrastruktur könnte Unternehmen dabei helfen, Innovationen in einem kontrollierten Umfeld zu entwickeln – ohne dabei rechtliche Grauzonen in Kauf nehmen zu müssen. Die europäische KI-Verordnung bietet hierfür mit seinen Vorgaben zu regulatorischen Testumgebungen einen geeigneten Bezugsrahmen, der nationale Lösungen sowohl ermöglicht als auch begrenzt. Mit der KI-VO und den damit verbundenen zukünftigen EU-Durchführungsrechtsakten besteht ein ausreichender gesetzlicher Rahmen für die Einrichtung einer nationalen KI-Sandbox.

8.2 INSTITUTIONELLE ZUSTÄNDIGKEIT UND GOVERNANCE

Regulatory Sandboxes benötigen nicht nur rechtliche, sondern auch funktionale institutionelle Voraussetzungen. Derzeit sind in Österreich Kompetenzen für Digitalisierung, Innovationsförderung, Datenschutz, Verbraucherschutz, Aufsicht und Sektorpolitik in unterschiedlichen Institutionen verortet. Diese Fragmentierung kann in der Umsetzung zu Reibungsverlusten, Unsicherheiten oder Zuständigkeitskonflikten führen.

Um dem entgegenzuwirken, wären **klare Governance-Prozesse** notwendig. Dabei müssen nicht zwingend neue Behörden, Gremien oder Instanzen geschaffen werden. Stattdessen könnten bestehende Einrichtungen koordiniert und die vorhandenen Zuständigkeiten pragmatisch gebündelt werden. Ein **effizienter Governance-Rahmen** könnte auf bereits vorhandene Formate zurückgreifen und diese intelligent verknüpfen.

Mögliche Schritte könnten sein:

- **Zuständigkeitsklärung durch Mandatsabstimmung:** Bestehende Anspruchsgruppen wie BMIMI, BMWET, BKA, BMF, BMSGPK, BMFWF, DSB, RTR, FFG, AK, WKO, IV und aws sollten ein gemeinsam abgestimmtes Verfahren zur Koordination und Fallverteilung vereinbaren.

- **Einrichtung eines operativen Steuerungsmechanismus innerhalb bestehender Strukturen:** Etwa durch eine ressortübergreifende Arbeitsgruppe oder eine befristete Koordinierungsstelle mit Projektauftrag.
- **Klare Ansprechstellen benennen:** Unternehmen und Antragsteller:innen müssen rasch wissen, wohin sie sich wenden können. Dazu würde es ausreichen, einen einheitlichen Zugangspunkt innerhalb bestehender Förder- oder Aufsichtsstrukturen zu definieren.

Die Aufgaben eines solchen Mechanismus umfassen:

- die Abstimmung und Vorauswahl geeigneter Projekte,
- den kostenfreien Zugang zur Sandbox für KMU und Start-ups,
- die Einbindung bestehender Aufsichts- und Ethikinstanzen,
- die Unterstützung bei rechtlichen und datenschutzrechtlichen Fragen, sowie
- die Sicherung der Rückkopplung in Rechtsetzung, Förderung und Aufsicht.

Langfristiges Ziel sollte nicht die Etablierung neuer Strukturen, sondern eine **leichte, transparente und nutzerorientierte Umsetzung** sein. Der Fokus läge auf der funktionalen Integration: Unternehmen sollte kein zusätzlicher Aufwand entstehen – im Gegenteil, sie sollten bei Antragstellung, Umsetzung und Auswertung entlastet werden.

Die Governance von Sandboxes sollte sich daher **an Prinzipien der Praktikabilität, Effizienz und Zugänglichkeit orientieren**. Nur so kann das Instrument selbst innovationsfreundlich wirken – nicht nur technisch, sondern auch institutionell.

8.3 PILOTIERUNG IN SCHLÜSSELBEREICHEN

Ein wirksamer Einstieg in KI Regulatory Sandboxes gelingt nicht über komplexe Gesamtkonzepte, sondern über konkrete Pilotprojekte mit klarem Nutzen und begrenztem Koordinationsaufwand. Der Fokus sollte auf ausgewählten Anwendungsfeldern liegen, in denen **hohe Sensibilität**, **gesellschaftliche Relevanz** und **erkennbarer Handlungsdruck** zusammentreffen – und in denen zugleich das Potenzial besteht, praxisnahe Erprobung mit bestehenden Förder- und Rechtsstrukturen zu verbinden.

Hierzu würden **niedrigschwellige Formate** benötigt, die Unternehmen, Verwaltung und Öffentlichkeit gleichermaßen zugänglich sind. Ziel sollte es sein, Erprobungsräume zu schaffen, die **Arbeitsaufwand reduzieren**, **regulatorische Klarheit schaffen** und den **Marktzugang erleichtern.**

Basierend auf der in Anhang III der europäischen KI-Verordnung angeführten Liste von KI-Systemen mit hohem Risiko, den sektoralen Analysen und Anspruchsgruppenrückmeldungen könnten folgende Sektoren als besonders geeignet vorgeschlagen werden (Tabelle 6):

Tabelle 6: Mögliche Sektoren für KI-Sandbox-Projekte

Sektor	Beispielhafte Anwendungen	Sensibilitäten
Gesundheitswesen und Medizintechnik	KI-gestützte Diagnosesysteme, klinische Entscheidungsunterstützung, medizinische Bildanalyse	Datenschutz (Gesundheitsdaten), ethische Abwägungen, Produktsicherheitsanforderungen
Öffentliche Verwaltung und Sozialwesen	Algorithmische Entscheidungsunterstützung im Sozial- oder Steuerwesen, Prozessautomatisierung in Förderverfahren	Diskriminierungsschutz, Transparenzanforderungen, Vertrauensdimensionen
Mobilität und Verkehrsinfrastruktur	Autonome Fahrzeuge, Verkehrssteuerungssysteme, intelligente Infrastrukturanalyse	Sicherheit, Haftungsfragen, Raum- und Umweltwirkung
Bildungsbereich	Adaptive Lernsysteme, automatisierte Förderentscheidungen, personalisierte Bildungsangebote	Fairness, Chancengleichheit, gesellschaftlicher Impact
Medien- und Kreativwirtschaft	Generative KI in Redaktion, Film, Musik, automatisierter Inhaltsklassifikation	Urheberrecht, Desinformation, Persönlichkeitsrechte
Industrie, Produktion und Energie	Predictive Maintenance, Qualitätssicherung, Energieeffizienzanalysen	Arbeitsplatzveränderungen, IT-Sicherheitsstandards, sektorale Aufsicht
Versicherungen und Bankwesen	KI-Systeme zur Bewertung der Kreditwürdigung natürlicher Personen, KI-Systeme zur Risikobewertung und Preisgestaltung in Bezug auf natürliche Personen im Falle von Lebens- und Krankenversicherungen	Diskriminierungsschutz, Transparenzanforderungen, Datenschutz (Gesundheitsdaten)

Quelle: Eigener Entwurf

8.4 METHODIK UND INFRASTRUKTUR FÜR SANDBOXES

Damit KI-Sandbox-Modelle in Österreich Wirkung entfalten können, bräuchte es nicht nur rechtliche und institutionelle Grundlagen, sondern auch eine handhabbare methodische und organisatorische Infrastruktur. Ziel sollte ein Verfahren sein, das Unternehmen und Verwaltung praktikabel unterstützt und nicht überfordert. **Standardisierte, nachvollziehbare Abläufe** könnten helfen, die Durchführung von Sandbox-Projekten zu vereinfachen und gleichzeitig die Qualität und Übertragbarkeit der Ergebnisse zu sichern. Damit entstünden keine neuen bürokratischen Hürden, sondern Werkzeuge, die Orientierung bieten – auch für kleinere Akteure ohne regulatorisches Spezialwissen.

Vorgeschlagen wird daher der Aufbau eines **Sandbox-Methodensets**, das folgende Komponenten umfassen könnte:

- **Antragsunterlagen, Sandbox-Plan und Testprotokolle:** einfache, vorstrukturierte Vorlagen für Projektbeschreibung, Risikoanalyse, Testdesign und Ablaufplanung,

- **Auswahlkriterien:** klare Orientierungspunkte wie Innovationshöhe, Risikoangemessenheit, Datenverarbeitung, gesellschaftlicher Nutzen oder Sektorbezug,
- **Evaluationsformate und -berichte:** anwendungsnahe Instrumente, die technische, rechtliche und soziale Lerneffekte systematisch erfassen; Vorlagen für die schriftliche Bestätigung und Exit-Reports,
- **Wissenstransfer:** transparente Dokumentation über ein öffentlich zugängliches Sandbox-Register oder eine Lernplattform, mit aufbereitbaren Ergebnissen für Praxis, Verwaltung und Politik.

Zur operativen Unterstützung könnten **niedrigschwellige Unterstützungsangebote** wie rechtliche und methodische **Beratungsstellen** für Antragsteller:innen, **technisch-ethische Prüfeinheiten** mit klarer Zuständigkeit für Fragen zu Datenschutz, Bias-Risiken oder Interoperabilität bzw. **Schnittstellen** zu bestehenden Policy Labs bereitgestellt werden.

Um erste Erfahrungswerte zu gewinnen, empfiehlt sich die Pilotierung einer **Modell-Sandbox-Plattform**, die sektorübergreifend funktioniert, digital gestützt ist und mit bestehenden europäischen Strukturen (z. B. EUSAiR, TEFs) kompatibel bleibt. Dabei sollte die Devise lauten: **so viel Struktur wie nötig – so wenig Hürden wie möglich**. Ziel sollte eine belastbare, aber praxistaugliche Infrastruktur sein, die Innovationen nicht aufhält, sondern in sichere Bahnen lenkt.

8.5 ANSPRUCHSGRUPPENBETEILIGUNG UND TRANSPARENZ

Damit KI-Sandboxes in Österreich wirksam, legitim und praxistauglich funktionieren, bräuchte es mehr als rechtliche Grundlagen und technische Standards. Entscheidend ist, **dass sie als transparente, anschlussfähige und niederschwellig zugängliche Formate wahrgenommen und genutzt werden können** – insbesondere von Unternehmen, die innovative Lösungen erproben möchten. **Beteiligung** darf **nicht zur Hürde werden**. Ziel sollte eine schlanke, effiziente Einbindung relevanter Akteure mit klaren Schnittstellen sein, ohne aufwendige Berichtspflichten oder komplexe Gremien. Es sollten daher zum einen **projektbegleitende Formate**, die frühzeitig Perspektiven aus Wirtschaft, Verwaltung, Aufsicht und ggf. Zivilgesellschaft einholen (etwa durch kompakte Online-Konsultationen, Fokusgruppen oder moderierte Feedbackrunden), seitens der zuständigen Behörde eingesetzt werden. Zum anderen sollte auf eine **klare Rollenverteilung** geachtet werden: Antragstellende sollen wissen, wer zuständig ist, wie Entscheidungen getroffen werden und wie Rückmeldungen einfließen. Weiters ist der Aufbau von **verbindlichen, aber einfachen Rückkopplungsmechanismen** sinnvoll, d. h. keine zusätzlichen Reportings, sondern nutzbare Formate wie Feedbackgespräche, Checklisten oder Lessons Learned aus abgeschlossenen Sandbox-Vorhaben.

Besonders wichtig wäre es, dass eine Beteiligung für Unternehmen **als Unterstützung** und **nicht als Kontrolle** erlebbar wird.

Transparenz sollte **pragmatisch gestaltet** werden, denn Transparenz ist sowohl eine Frage der Vollständigkeit als auch der Verständlichkeit. Unternehmen brauchen Klarheit über Verfahren, Kriterien und Anforderungen. Gleichzeitig erwartet die Öffentlichkeit Nachvollziehbarkeit bei sensiblen Technologien. Mögliche Maßnahmen wären daher auf der einen Seite **die Einrichtung eines öffentlichen Sandbox-Registers (d. h. Sandbox-Übersichtskarte)**, das aktuelle Vorhaben kurz und verständlich darstellt (d. h. wer testet was,

in welchem Rahmen, mit welchen Schutzvorkehrungen), und auf der anderen Seite die Bereitstellung von **einfachen Kommunikationsformaten** wie z. B. Erklärseiten, Praxisbeispiele, Videos oder Infografiken. Ergänzend dazu könnte auch die **Veröffentlichung aggregierter Ergebnisse** (keine sensiblen Betriebsgeheimnisse, sondern übertragbare Erkenntnisse für Politik, Verwaltung und andere Unternehmen) sinnvoll sein.

Wie Kapitel 7.3 zeigt, ist **Vertrauen** zentral für das Gelingen von KI-Sandboxes. Transparente Verfahren und nachvollziehbare Entscheidungen stärken nicht nur die Akzeptanz in der Öffentlichkeit, sondern auch das Vertrauen von Unternehmen in die Fairness und Berechenbarkeit des Formats. Besondere Bedeutung kommt dabei niedrigschwelligen Beteiligungs- und Feedbackformaten zu, die ohne zusätzlichen Ressourcenaufwand genutzt werden können – **gerade für KMU und Start-ups, die weder eigene Rechtsabteilungen** noch entsprechende **Stabsstellen haben**.

8.6 EUROPÄISCHE ANSCHLUSSFÄHIGKEIT GEWÄHRLEISTEN

Die Einführung von KI Regulatory Sandboxes in Österreich muss mit dem europäischen Rechtsrahmen – insbesondere der europäischen KI-Verordnung – kompatibel sein. Dieser sieht ausdrücklich vor, dass Mitgliedstaaten Testumgebungen einrichten können, jedoch nur **unter strengen Bedingungen**, etwa in Bezug auf **Transparenz, Aufsicht und Schutzstandards**. Sandbox-Modelle in Österreich sollten nicht als Sonderweg konzipiert werden, sondern als **konstruktive Ergänzung zu EU-Initiativen**. Ziel ist es, **Anschlussfähigkeit sicherzustellen**, ohne dabei unnötige Komplexität oder administrative Doppelstrukturen aufzubauen.

Insbesondere bei der Auswahl von Pilotprojekten (siehe 8.3) und der Definition von Kriterien (siehe 8.4) sollte eine **volle Ausrichtung auf die Risikologik der europäischen KI-Verordnung** erfolgen. **Nationale Anforderungen** sollten **nicht über die EU-Vorgaben hinausgehen**, wenn sie keinen erkennbaren Mehrwert bieten (Vermeidung von Gold Plating). Bezugnehmend auf die derzeit bestehenden Defizite des EK-Entwurfs hinsichtlich der Überführung/Nutzung der Sandbox-Ergebnisse für regulatorische Weiterentwicklung und Wachstum/Innovation könnte jedoch eine nationale Nachsteuerung/Schärfung zielführend sein. Zur Vermeidung von Inkohärenzen und zur Stärkung der Anerkennung von Sandbox-Ergebnissen sollte eine **frühzeitige Abstimmung mit EU-Gremien** (z. B. EU AI Office, Standardisierungsgremien) erfolgen, darüber hinaus wäre es sinnvoll, **europäische Infrastrukturen** zu **nutzen** und nicht zu duplizieren.

Bestehende europäische Programme wie die **eDIHs, TEFs** oder das **EUSAiR-Projekt** bieten bereits Strukturen, mit denen nationale Sandboxes verbunden werden können. Sinnvoll wäre daher zum einen die **Einbindung österreichischer Unternehmen und Einrichtungen in bestehende EU-Testinitiativen**, um Know-how, Standards und Sichtbarkeit zu stärken, zum anderen die Sicherstellung der **technischen und administrativen Kompatibilität** – z. B. bei Datenformaten, Evaluationsmethoden oder Förderlogiken. Gerade KMU würden von EU-weit anerkannten Testformaten profitieren – wenn sie **zugänglich und ressourcenschonend** ausgestaltet sind. Ergänzend dazu könnten KMU auch von der **Bündelung von Anträgen durch eine nationale Koordinationsstelle**, die EU-Pilotprojekte systematisch aufbereitet, kommuniziert und unterstützt, profitieren.

Sinnvoll könnte der Aufbau eines **Angebots von niedrigschwelligen Beratungen und Begleitungen** bei EU-Anträgen (z. B. durch FFG, aws oder DIHs) sein, als auch das **Aufsetzen von standardisierten Prozessen** in nationalen Sandboxes, die mit EU-Formaten kompatibel sind (etwa bei Anträgen, Dokumentation und Evaluierung). Komplementär würde sich die **Bereitstellung von gezielten Förderinstrumenten** für Unternehmen, die sich an EU-Pilotprojekten beteiligen wollen (etwa Reisekostenzuschüsse, Beratungspakete oder Matching-Formate), empfehlen.

9 Implementierungsszenarien für Österreich

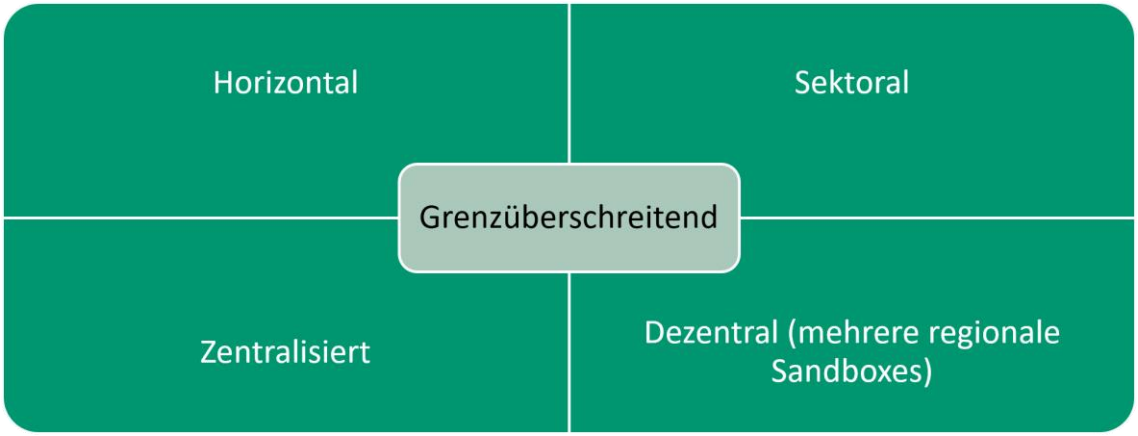
9.1 EINLEITUNG

Kapitel 9 verdichtet die Erkenntnisse der Kapitel 6 bis 8 in Implementierungsszenarien. So können mögliche Optionen in ihrer grundsätzlichen Machbarkeit und Sinnhaftigkeit diskutiert, realisierbare Umsetzungsszenarien im Detail betrachtet und mit ihren Chancen und Herausforderungen bewertet werden. Ausgehend von einem Überblick und einer Diskussion möglicher Sandbox-Optionen für Österreich erfolgt dann eine vertiefende Darstellung und Reflexion einer zentralisierten Sandbox-Lösung.

9.2 SZENARIOÜBERBLICK

Die KI-VO sieht in Artikel 57 Abs. 1 und 2 sowohl Möglichkeiten für die Einrichtung einer zentralisierten als auch einer (oder mehreren) dezentralen, d. h. regionalen oder lokalen, Sandbox vor. Zusätzlich können auch grenzüberschreitende Sandboxes mit anderen EU-Mitgliedsstaaten aufgebaut werden.

Abbildung 4: Grundlegende Optionen für die Gestaltung einer Regulatory Sandbox für KI in Österreich



Quelle: Eigener Entwurf

Eine Betrachtung der untersuchten Good-Practice-Beispiele (siehe Anhang 1) zeigt, dass die thematische Ausrichtung sowohl horizontal (also themenoffen) als auch sektoral gestaltet sein kann. Abbildung 3 bietet einen entsprechenden Überblick über die möglichen generischen Optionen. Betreffend der inhaltlichen Ausrichtung kann eine Sandbox entweder horizontal (wie z. B. die spanische KI-Sandbox), oder sektoral (z. B. Sandbox zu psychischer Gesundheit) gestaltet werden. Hinsichtlich der organisatorischen Umsetzung reichen die Optionen von einer zentralisierten Lösung über eine dezentrale Gestaltung bis hin zur Implementierung einer grenzüberschreitenden Sandbox in Zusammenarbeit mit EU-Nachbarländern und/oder Regionen. Im Folgenden werden verschiedene Umsetzungsszenarien für regulatorische KI-Sandboxes näher betrachtet. Sie zeigen, wie sich regulatorische Vorgaben in unterschiedlichen Modellen und Prozessen konkret ausgestalten lassen und welche Herausforderungen und Chancen bei der Institutionalisierung und dem Betrieb solcher Experimentierräume bestehen.

Dezentrale (regionale/lokale) Sandbox

Beschreibung

Ziel: Entwicklung, Test und Integration von spezialisierten, branchenspezifischen KI-Lösungen innerhalb regionaler wirtschaftlich-technologischer Stärkefelder in Österreich. Das Design einer dezentralen Sandbox würde dabei die räumliche Nähe zu relevanten Unternehmen bzw. regionalen Clustern schaffen. Die Sandbox könnte als ein organisatorisch vernetztes und räumlich verteiltes System gestaltet werden. Österreich könnte mehrere Sandboxes betreiben, wobei eine dezentrale Struktur die Flexibilität steigern und die Nutzung regionaler Ressourcen fördern würde. Beispielhafte Vorbilder für regionale Sandboxes finden sich in Deutschland[11], der Schweiz[12] und der Slowakei[13]. Sektorale Schwerpunkte der Sandboxes sollten auf Basis regionaler Stärkefelder gesetzt werden:

- Westösterreich: Life Sciences & Biotechnologie, Maschinenbau (I 4.0),
- Südösterreich: Mobilität, Automatisierung/Robotik, Medizintechnik,
- Ostösterreich: Maschinenbau (I 4.0), Life Sciences & Biotechnologie, Medizintechnik, Medientechnologien.

Organisation: Die dezentrale KI-Sandbox könnte aus mehreren regionalen Knotenpunkten bestehen, die eng miteinander vernetzt sind. Mögliche Ankerpunkte könnten hier beispielsweise die bestehenden DIHs für West-, Süd- und Ostösterreich sein. Jeder Knotenpunkt könnte Partner aus Wirtschaft, Forschung und Verwaltung in der jeweiligen Region einbinden. Dies stärkt regionale Innovationsökosysteme und ermöglicht eine bedarfsgerechte Unterstützung. Die Knotenpunkte könnten ihre Erkenntnisse untereinander austauschen, um Synergien zu nutzen und bewährte Verfahren gemeinsam zu entwickeln.

Inhaltlich würde die Sandbox neben der Bereitstellung von Testinfrastrukturen auch Zugang zu relevanten Datenquellen und regulatorischem Know-how bieten und stünde verschiedensten Akteuren offen: Start-ups, KMU, Großunternehmen und Forschungseinrichtungen. Die dezentrale Gestaltung würde es ermöglichen, lokale Besonderheiten zu integrieren, wie zum Beispiel branchenspezifische Herausforderungen oder regionale Schwerpunkte. Ein weiterer Vorteil entstünde durch die Möglichkeit, regionale Netzwerke zu stärken und den Know-how-Transfer zwischen Unternehmen, Wissenschaft und Verwaltung voranzutreiben. Praktisch könnten koordinierende Stellen die Zusammenarbeit der Knotenpunkte moderieren, gemeinsame Ressourcen bereitstellen und Standards für Datenschutz, Sicherheit und ethische Kriterien einhalten.

Für die **Governance** einer dezentralen regionalen KI-Sandbox in Österreich wäre ein umfassendes, koordiniertes und partizipatives Modell zentral, das sowohl nationale als auch regionale Besonderheiten und die Anforderungen der europäischen KI-Verordnung berücksichtigt. Die Steuerung der KI-Sandbox erfolgt typischerweise über eine spezialisierte Servicestelle auf Bundesebene. Die Servicestelle wirkt als zentrale Anlaufstelle für alle Beteiligten: Sie koordiniert die regulatorischen, technischen und ethischen Belange und sorgt

[11] https://www.digi-sandbox.nrw/
[12] https://www.innovationsandbox.ai/
[13] https://ickk.sk/en/ai/

für die Einhaltung der Vorgaben aus der EU-KI-Verordnung, wobei sie eng mit regionalen Behörden und Expert:innen vernetzt ist. Eine regionale Governance-Struktur müsste auf einer breiten Einbindung von Anspruchsgruppen aufbauen: Ministerien, Ländervertretungen, lokale Unternehmen, Sozialpartner, Wissenschaft und Zivilgesellschaft würden über Gremien wie den KI-Beirat und das AI Stakeholder Forum aktiv einbezogen.

Bewertung

Ein wesentlicher **Vorteil** einer regionalen KI-Sandbox ist die gezielte Berücksichtigung spezifischer Bedürfnisse und Herausforderungen der lokalen Wirtschaft. Die gewonnenen Erkenntnisse, etwa zu rechtlichen oder technischen Fragestellungen, kämen nicht nur den Beteiligten, sondern dem gesamten regionalen Innovationsökosystem zugute. Darüber hinaus könnte diese Bottom-up-Perspektive die Einführung innovativer KI-Lösungen in den Wirtschaftsalltag beschleunigen und die Wettbewerbsfähigkeit der ansässigen Unternehmen stärken.

Der größte **Nachteil** liegt demgegenüber in der sehr komplexen Governance. Alle für Testläufe in der Sandbox relevanten Gesetze und auch die für Sandboxes zuständige Behörde sind ausschließlich auf der Bundesebene verankert. Es wäre somit ein unpraktikables Design gegeben, in dem zwar ein regionaler/lokaler Betrieb der Sandbox erfolgen würde, die rechtliche Begleitung und Aufsicht der Testläufe aber auf Bundesebene erfolgen müsste. Eine Folge wären massive Transaktions- und Koordinationskosten im Sandbox-Betrieb.

Grenzüberschreitende Sandbox

Beschreibung

Ziel: Entwicklung, Testung und Integration von spezialisierten, branchenspezifischen KI-Lösungen innerhalb relevanter grenzüberschreitender Wertschöpfungsketten[14]. Eine (oder mehrere) grenzüberschreitende Sandbox(es) sollte(n) sektoriell ausgerichtet werden. Daher sollten die inhaltlichen Schwerpunkte insbesondere darauf ausgelegt werden, internationale Zusammenarbeit und regulatorische Harmonisierung zu fördern. Branchenschwerpunkte der Sandboxes sollten auf Basis von für den Standort Österreich relevanten Wertschöpfungsketten gesetzt werden; konkret könnten dabei die folgenden inhaltlichen Ausrichtungen angestrebt werden:

- Sachgüterproduktion: Fahrzeugbau, Maschinenbau (I 4.0), Elektrotechnik/Elektronik,
- Dienstleistungen: Logistik, Transport,
- Medientechnologien.

Die Sandbox sollte eine technische und **organisatorische** Plattform bieten, die den Zugang für Unternehmen, Forschungseinrichtungen und weitere Anspruchsgruppen aus allen beteiligten Regionen ermöglicht. Neben der Basisinfrastruktur sollte die Sandbox Anwendungen und Use Cases unterstützen, die für die beteiligten Regionen wirtschaftlich und

[14] Das EU-Recht erlaubt und fördert Sandboxes, die von mehreren Mitgliedstaaten gemeinsam betrieben werden (EUKI-VO Art. 57 Abs. 1 und 2).

gesellschaftlich relevant sind. Durch den grenzüberschreitenden Charakter können Synergien genutzt und Erfahrungen im gemeinsamen Wirtschafts- und Kulturraum (DACH) geteilt werden. Eine länderübergreifende, aber auch bundeslandspezifische Steuerung ist wichtig. Für die Sandbox wäre ein Gremium denkbar, das Interessen aus allen Regionen vertritt und die Einhaltung ethischer Standards sowie regulatorischer Anforderungen sicherstellt. Für den Aufbau und Betrieb einer grenzüberschreitenden Sandbox sind ausreichende finanzielle Mittel nötig, die von EU-Förderprogrammen, nationalen und regionalen Förderungen sowie privaten Investoren getragen werden könnten.

Auf Basis der angestrebten **inhaltlichen Ausrichtung** bzw. der relevanten Wertschöpfungsketten könnte die geographische Abdeckung zum einen Österreich sowie zum anderen deutsche Bundesländer (bspw. Bayern, Baden-Württemberg, Nordrhein-Westfalen) umfassen. Der österreichische Knoten der grenzüberschreitenden Sandbox würde an einem zentralen Ort mit ausreichenden infrastrukturellen Angeboten – d. h. Bundesländerhauptstädte oder die Bundeshauptstadt Wien – angesiedelt. Eine grenzüberschreitende KI-Sandbox könnte als ein kooperatives Innovations- und Testumfeld gestaltet werden, das die Forschungs- und Entwicklungsaktivitäten aus beiden Ländern und den beteiligten Bundesländern bündelt.

Eine grenzüberschreitende KI-Sandbox, die Österreich, Bayern, Baden-Württemberg und Nordrhein-Westfalen umfasst, erfordert ein **abgestimmtes und mehrstufiges Governance-Modell,** um die gemeinsame Entwicklung, Erprobung und Regulierung von KI-Systemen effektiv zu ermöglichen. Dabei sollten mehrere zentrale Aspekte berücksichtigt werden: Operativ ist ein gemeinsames Steuerungsgremium sinnvoll, das Vertreter aus Österreich, Bayern, BW und NRW zusammenbringt. Dieses Gremium organisiert Zulassungsverfahren, definiert Testkriterien, überwacht die Einhaltung der Vorschriften und sorgt für den Wissensaustausch. Zur **Steuerung der Zusammenarbeit** empfiehlt sich ein **kooperatives Modell**, das bestehende nationale Behörden und KI-Initiativen integriert. Auf nationaler und regionaler Ebene müssen zentrale Anlaufstellen geschaffen werden, die als Koordinatoren der Sandbox fungieren. Außerdem muss die Zusammenarbeit zwischen den beteiligten Ländern und Regionen auf gegenseitiger Abstimmung der regulatorischen Anforderungen basieren, um Rechtssicherheit für Anbieter zu gewährleisten.

Bewertung

Vorteile: Eine grenzüberschreitende KI-Sandbox würde Synergien nutzen, Doppelarbeit vermeiden und Unternehmen den Zugang zu einer größeren, integrierten KI-Testumgebung eröffnen. Allerdings müssten nationale Besonderheiten (z. B. Sprache, spezifische Compliance-Anforderungen) berücksichtigt werden. Konkrete Beispiele wie internationale Sandbox-Gipfel, ein europaweiter Austausch zu Sandbox-Projekten oder die Entwicklung gemeinsamer Dateninfrastrukturen zeigen, wie grenzüberschreitende KI-Sandboxes

Innovationszyklen verkürzen, den Wissenstransfer beschleunigen und Unternehmen helfen, ihre Wettbewerbsfähigkeit nachhaltig zu stärken[15].

Nachteile: Auch wenn die Einrichtung grenzüberschreitender Sandboxes in der europäischen KI-Verordnung (Art. 57 Abs. 1) als mögliche Option vorgesehen ist und wie oben umrissen Vorteile bringen kann, sind die Einrichtung und der Betrieb sehr aufwändig. Darüber hinaus bieten die seitens der EU geplanten kommunikativen und koordinativen Strukturen einen ausreichenden Rahmen für den wechselseitigen Austausch zu Ergebnissen aus den nationalen Regulatory Sandboxes.

9.3 GESTALTUNGSSZENARIEN FÜR EINE ZENTRALISIERTE KI-SANDBOX

Eine zentralisierte KI Regulatory Sandbox bringt mehrere Vorteile gegenüber einer dezentralen Lösung mit sich. Erstens ermöglicht sie eine einheitliche Kontrolle und Governance durch eine zentrale Autorität, was eine konsistente und effiziente Umsetzung der regulatorischen Anforderungen sicherstellt. Zweitens fördert die Zentralisierung die Ressourceneffizienz durch die Bündelung von technischem Fachwissen und Infrastruktur an einem Standort. Darüber hinaus lässt sich die Rechtssicherheit verbessern, da klare und einheitliche Regeln innerhalb eines zentralen Rahmens gelten. Viertens wird der Austausch bewährter Praktiken und das regulatorische Lernen erleichtert, was Innovationen in einem reglementierten Umfeld fördert. Weiters erleichtert eine zentrale Sandbox vor allem Klein- und Mittelunternehmen (KMU) sowie Start-ups den Marktzugang durch gezielte Unterstützung, Schulungen und technische Expertise. In Ergänzung dazu kann eine zentralisierte Umgebung schneller auf neue Herausforderungen und technologische Entwicklungen reagieren, da Anpassungen zentral koordiniert werden. Auch bieten zentrale Sandboxes eine bessere Übersicht und Kontrolle für die Aufsichtsbehörden, was das Risikomanagement und den Verbraucherschutz verbessern kann. Schließlich ermöglicht eine zentrale KI Regulatory Sandbox eine effizientere Dokumentation und Nachweisführung der Compliance gegenüber regulatorischen Anforderungen, was den Übergang in den regulären Markt erleichtert.

Eine zentralisierte KI-Sandbox kann dabei zwei komplementäre Ausrichtungen haben: 1. horizontal (d. h. themenoffen) oder 2. sektoral (d. h. auf spezifische Branchen und/oder Anwendungsfelder fokussiert). Die Darstellung des Implementierungsszenarios erfolgt, wo notwendig, aufgeteilt auf beide Ausrichtungsvarianten.

Verortung, Zielsetzung und inhaltliche Ausrichtung

Die Sandbox wird an einem zentralen Ort mit ausreichenden infrastrukturellen Angeboten – d. h. Bundesländerhauptstädte oder Bundeshauptstadt Wien – angesiedelt. Die Sandbox ist für Bewerbungen aus allen Bundesländern Österreichs offen.

Zielsetzung der **horizontalen Bundes-Sandbox** ist die Entwicklung, Testung und Evaluation von KI-Lösungen, die branchenübergreifend und vielseitig einsetzbar sind. Das Design einer

[15] https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/wirtschaft-arbeit/wirtschaftsstandort/dokumente/sandbox_de.pdf

zentralisierten Sandbox würde dabei die Konzentration von ausreichend Expert:innen sowie einen einfachen Zugang zu zentral verfügbaren Infrastrukturen ermöglichen.

Dementsprechend sollte die Sandbox themenoffen konzipiert werden. Der Fokus der horizontalen Sandbox würde daher auf der Vielseitigkeit liegen: Technologien und Use Cases werden nicht für einen einzigen Sektor optimiert, sondern für möglichst viele Anwendungskontexte für KI-Systeme mit hohem Risiko (EU KI-VO, Art. 6 Abs. 2) zugänglich gemacht. Dadurch können Unternehmen Hochrisikoanwendungen in KI-Projekten testen, die beispielsweise für Verwaltung, Mobilität, Gesundheit, Bildung oder die Industrie relevant sind.

Ein spezifisches Merkmal der horizontalen Ausrichtung ist, dass keine hochgradige Spezialisierung auf einzelne Branchen erfolgt. Die Lösungskompetenz bleibt breit, das heißt, die eingesetzten KI-Systeme und Tools sollen schnell und unkompliziert in verschiedenen Kontexten adaptiert werden können. Dies erhöht die Innovationsgeschwindigkeit, birgt jedoch die Herausforderung, dass nicht alle branchenspezifischen Anforderungen im Detail abgedeckt werden.

Die zentralisierte Sandbox mit sektoraler Ausrichtung hat die Entwicklung, Testung und Integration von spezialisierten, branchenspezifischen KI-Lösungen zum Ziel. Das Design einer zentralisierten Sandbox ermöglicht dabei die Konzentration von kritischen Massen an Expert:innen sowie einen einfachen Zugang zu zentral verfügbaren Infrastrukturen.

Die Sandbox sollte folglich themenspezifisch konzipiert werden. Der Fokus der sektoralen Sandbox(es) liegt auf Spezialisierung: Technologien und Use Cases werden jeweils für einen einzigen Sektor optimiert, so kann spezifisches Domänenwissen gebündelt bereitgestellt werden.

Sektorielle Schwerpunkte sollten auf Basis nationaler Stärkefelder gesetzt werden; konkret könnten dabei die folgenden inhaltlichen Ausrichtungen vorgenommen werden:

- Life Sciences & Biotechnologie / Gesundheit
- Industrie 4.0 (Maschinenbau & Automatisierung)
- Energieerzeugung und -versorgung
- Verkehr und Logistik
- Finanz- und Versicherungsdienstleistungen
- Medien und Kreativwirtschaft

Gestaltung & Architektur

Eine **zentralisierte KI-Sandbox** mit **horizontaler Ausrichtung** in Österreich bietet eine Plattform, in der Projekte mit regulatorischer Begleitung und Unterstützung realitätsnah entwickelt, getestet und evaluiert werden können. Solch eine Sandbox wird von der national zuständigen Behörde eingerichtet, unterstützt durch klare regulatorische Rahmenbedingungen gemäß der europäischen KI-Verordnung, die bis August 2026 betriebsbereit sein muss. Organisatorisch wäre eine zentrale Verwaltung sinnvoll, die alle relevanten Anspruchsgruppen von Unternehmen, Forschungseinrichtungen und der öffentlichen Verwaltung bis hin zum Mediensektor einbindet. Die Sandbox sollte eine Infrastruktur bieten, die den Zugang zu Datensätzen, KI-Modellen, Testumgebungen und regulatorischem Expertenwissen ermöglicht. Ein wichtiger Punkt ist sowohl die enge Zusammenarbeit mit rechtlichen Expert:innen, um die

Einhaltung von Datenschutz, Urheberrecht und KI-spezifischen Gesetzen wie der europäischen KI-Verordnung sicherzustellen, als auch die direkte und multidisziplinäre Einbindung von Domänenexpert:innen, um technisches und soziotechnisches Wissen einzubringen. Die zentralisierte horizontale Sandbox sollte über die folgenden konkreten Gestaltungselemente verfügen:

- **One-Stop-Shop für Unternehmen beim Onboarding und im Testbetrieb:** Der gesamte Prozess eines Sandbox-Use-Cases wird über eine enge laufende Zusammenarbeit mit dem Unternehmen abgewickelt. So können die Kommunikation und die inhaltliche Interaktion für das Unternehmen möglichst einfach und transaktionskostenschonend gestaltet werden.
- **Offene, sektorunabhängige Infrastruktur** mit flexiblen technischen und rechtlichen Rahmenbedingungen, die viele Anwendungsfälle unterstützen. Dabei sollte ein Angebot mit standardisierte Zugangsmöglichkeiten für vielfältige Organisationen bereitgestellt werden. Die Bereitstellung von organisatorischen und infrastrukturellen Ressourcen sollte entweder durch (Technische) Universitäten und/oder Forschungs- und Technologieorganisationen erfolgen.
- **Grundlegende Dienstleistungen:** Zentrale Anlaufstelle, die Beratungen und eine Risikobewertung von KI-Systemen gemäß der Klassifizierung und den regulatorischen Leitlinien der EU KI-VO durchführt.
- **Erweiterte Dienstleistungen:** Angebot von Testumgebungen und maßgeschneiderten individuellen Unterstützungswegen für Unternehmen, unter Nutzung bestehender Innovationsinfrastrukturen, beispielsweise die der AI Factory.
- **Dateninfrastruktur:** Sichere Integration und Verwaltung von Datenquellen durch „Data Owners“ (z. B. öffentliche Stellen, Unternehmen), inklusive Maßnahmen zum Datenschutz und Privacy-by-Design. Die Sandbox ermöglicht Zugriff auf relevante Daten, die für KI-Tests benötigt werden, und gewährleistet dabei Compliance mit gesetzlichen Vorgaben.
- **Flexibles Projektmanagement- und Governance-Modul:** Koordination der Projektvorschläge und deren iterative Spezifizierung in Zusammenarbeit mit teilnehmenden Organisationen. Die Governance gewährleistet Einhaltung von regulatorischen, ethischen und Datenschutzanforderungen und unterstützt interdisziplinäre Zusammenarbeit zwischen Unternehmen, Forschung und Behörden.
- **Partnernetzwerk und technische Kooperation:** Integration externer Partner wie etwa Drohnenanbieter für Datenerhebung oder KI-Entwickler. Die Architektur erlaubt modulare Anpassungen durch verschiedene Partner, die spezifische Hardware oder Software beisteuern.

Governance

Die **Governance** einer **zentralisierten horizontalen KI-Sandbox** in Österreich basiert auf einem rechtlichen und organisatorischen Rahmen, der es ermöglicht, KI-Systeme in einer kontrollierten Umgebung zu testen, zu entwickeln und zu validieren. Dabei wird die Governance so gestaltet, dass sie die Entwicklung von KI fördert und gleichzeitig Risiken

minimiert. Die zentrale Steuerung und Koordination erfolgen durch nationale Behörden, die auch für die Einhaltung der europäischen KI-Verordnung zuständig sind.

In Österreich gibt es eine koordinierte Struktur im Bereich künstliche Intelligenz, unter anderem durch das AI Policy Forum (als interministerielle Arbeitsgruppe), den KI-Beirat (als beratendes Gremium), die KI-Servicestelle (als nationale Anlaufstelle für KI-Regulierung) sowie das AI Stakeholder Forum, welches den breiten Austausch zwischen Regierung, Wirtschaft, Forschung, Sozialpartnern und Zivilgesellschaft fördert. Die Governance der KI-Sandbox könnte an diese Struktur angelehnt werden, indem das Thema Sandbox in die internen Strukturen und Agenden der bereits existierenden Gremien integriert wird (etwa durch Task Forces). Die Governance umfasst dabei verschiedene Akteure, darunter Ministerien, Expert:innen, Unternehmen, zivilgesellschaftliche Organisationen und Sozialpartner, was eine breite und vernetzte Steuerung ermöglicht.

Die Governance einer zentralisierten horizontalen KI-Sandbox ist gekennzeichnet durch klare Verantwortlichkeiten und Rechenschaftspflichten, wobei Prozesse für Planung, Entwicklung, Überwachung und Stilllegung von KI-Anwendungen definiert sind. Dabei wird auch die Einhaltung ethischer, rechtlicher und betrieblicher Anforderungen berücksichtigt. So werden beispielsweise auch Datenschutzaspekte und Compliance geprüft und sichergestellt, dass KI-Systeme verantwortungsvoll, transparent und nachvollziehbar eingesetzt werden.

Die nationale Behörde stellt Ressourcen bereit und sorgt für eine ausreichende finanzielle Ausstattung der Sandbox (bspw. wurden für die spanische KI-Sandbox zur operativen Vorbereitung der EU KI-VO pro Jahr rd. 1,1 Mio. EUR budgetiert), damit diese wirkungsvoll betrieben werden kann. Sie bietet zudem Anleitung und Aufsicht und unterstützt die Teilnehmer:innen, wobei kleine und mittlere Unternehmen sowie Start-ups das Angebot der Sandbox kostenlos nützen können.

Ein weiterer Aspekt der Governance ist die Förderung des Austauschs zwischen den verschiedenen Anspruchsgruppen sowie die Koordination der Aktivitäten auf nationaler und europäischer Ebene, um Erfahrungen zu sammeln und bewährte Praktiken zu verbreiten. Die Behörden berichten regelmäßig über die Aktivitäten und Ergebnisse der Sandbox, um die Entwicklung kontinuierlich zu überwachen und regulatorisch zu lernen.

Beim Aufbau der Governance-Struktur sollte auf die Prinzipien von Accountability (Rechenschaftspflicht), Responsibility (Verantwortlichkeit) und Transparency (Transparenz), geachtet werden.

Eine **zentralisierte sektorale KI-Sandbox** in Österreich könnte in ihrer Governance so gestaltet werden, dass sie auf die speziellen Anforderungen und rechtlichen Rahmenbedingungen eines bestimmten Wirtschafts- oder Anwendungssektors zugeschnitten ist. Dabei bleibt der rechtliche und ethische Rahmen, wie er durch die nationale KI-Strategie und die europäische KI-Verordnung sowie den zugehörigen Durchführungsrechtskaten der EU vorgegeben wird, erhalten, wird aber sektorspezifisch operationalisiert.

In einer sektoralen Sandbox erfolgt die Governance durch eine enge Zusammenarbeit von Fachministerien, regulatorischen Behörden und branchenspezifischen Anspruchsgruppen wie unter anderem Unternehmen, Forschungseinrichtungen und Sozialpartnern aus dem jeweiligen Sektor. So kann sichergestellt werden, dass die Sandbox den branchentypischen

Herausforderungen gerecht wird und etwaige Risiken für Verbraucher:innen, Umwelt oder die Gesellschaft passgenau adressiert werden.

Die Steuerung einer sektoralen KI-Sandbox erfolgt dezentral, das heißt innerhalb der Zuständigkeit der jeweiligen Fachressorts (z. B. Gesundheit, Energie, Verkehr) in Zusammenarbeit mit den relevanten sektoralen Regulierungsbehörden (z. B. FMA, Bundesamt für Sicherheit im Gesundheitswesen etc.). Die Koordination könnte über eine nationale Koordinationsstelle wie die KI-Servicestelle beim Rundfunk und die Telekom Regulierungs-GmbH (RTR) erfolgen. Diese Servicestelle bietet rechtliche Orientierung und unterstützt die Umsetzung der europäischen KI-Verordnung, wovon auch sektorale Sandboxes profitieren.

Organisatorisch sind sektorale Sandboxes durch klare Governance-Elemente wie definierte Verantwortlichkeiten, Rechenschaftspflichten und Kontrollmechanismen gekennzeichnet. Dabei erfolgt ein enges Monitoring der laufenden Projekte in der Sandbox, um die Einhaltung von Datenschutz, ethischen Standards und regulatorischen Vorgaben sicherzustellen. Zudem gibt es häufig ein beratendes Gremium, bestehend aus sektoralen Expert:innen, um bei komplexen Fragen fachlich zu unterstützen.

Sektorale KI-Sandboxes fördern zudem den Austausch und die Zusammenarbeit zwischen regulatorischen Einrichtungen, Unternehmen und Forschung innerhalb des Sektors. Sie dienen so auch als Innovationsplattformen, in denen neuartige KI-Anwendungen unter realen Bedingungen getestet und validiert werden können, bevor eine breitere Zulassung oder Markteinführung erfolgt. Die Finanzierung und Ressourcenbereitstellung erfolgen durch das zuständige Ministerium oder in Kooperation mit EU-Fördertöpfen.

Prozesse und Ablauf

Der idealtypische Prozess innerhalb der KI-Sandbox sollte sich durch seine Niederschwelligkeit, klare Struktur und intensive Begleitung auszeichnen. Es sollte dabei auf die oft begrenzten Ressourcen insbesondere von KMU und Start-ups Rücksicht genommen werden (für diese sollte die Teilnahme an der Sandbox keine allfälligen Gebühren erforderlich machen). Die Sandbox sollte offen für alle Unternehmen sein, wobei von einem besonderen Bedarf bei KMU und Start-ups ausgegangen werden kann. Dementsprechend werden bürokratische Hürden reduziert, vereinfachte Antrags- und Dokumentationsverfahren angeboten und spezifische Beratungs-, Informations- und Schulungsangebote bereitgestellt. Der Prozess ist von Transparenz geprägt: Alle Schritte – von der Antragstellung über die Durchführung von Audits und Dokumentation bis zur Evaluierung des Projekterfolgs – werden verständlich vermittelt und können mit Hilfe von Mustervorlagen sowie digitalen Plattformen flexibel und ressourcenschonend absolviert werden. Der Prozess umfasst folgende aufeinander abgestimmte Elemente, die speziell auf die Bedürfnisse von KMU und Start-ups zugeschnitten sind:

Onboarding

- **Beratungen, Bedarfsanalyse und Zieldefinition:** Zu Beginn wird gemeinsam mit Expert:innen über Beratungsgespräche der konkrete Bedarf des Unternehmens ermittelt.

Sollte dieser ein Sandbox-Projekt notwendig machen, so werden in Folge die Ziele des Sandbox-Projekts definiert. Dabei werden die individuellen Herausforderungen sowie die Möglichkeiten für den praktischen KI-Einsatz besprochen.

- **Niederschwelliger Zugang und vereinfachte Formalitäten:** Bürokratische Hürden werden reduziert. Antrags- und Dokumentationsverfahren werden so einfach wie möglich gestaltet, beispielsweise durch die Option einer Anerkennung des Sandbox-Zugangs in bestehenden Programmen ähnlich der Verzahnung mit ERC Grants/EU-Programmen, um mehrfache Antragsverfahren und somit eine zusätzliche Belastung für Unternehmen zu vermeiden. Hilfestellungen wie Checklisten oder digitale Dokumentenverwaltung helfen, den Einstieg zu erleichtern, und beschleunigen den Prozess.
- **Bereitstellung technischer Ressourcen und Infrastruktur:** Das Unternehmen erhält unkompliziert Zugang zu den benötigten Tools, technischen Plattformen und relevanten Daten, die durch die die Sandbox-Infrastruktur betreibende Organisation angeboten werden. Die Einrichtung erfolgt mit personalisierten Zugangsdaten, und technische Unterstützung steht bereit, um den Einstieg zu erleichtern.
- **Einführung und Schulung:** Durch speziell für KMU konzipierte Informationsmaterialien, Workshops und digitale Lernformate werden die rechtlichen, technischen und organisatorischen Rahmenbedingungen verständlich und praxisnah vermittelt. Individuelle Lernpfade und personalisierte Schulungen berücksichtigen die Vorkenntnisse und das Lerntempo der Teilnehmer:innen.
- **Begleitung und laufender Support:** Unabhängige Expert:innen stehen für Rückfragen bereit, erleichtern die Orientierung und bieten fortlaufende Unterstützung. So können Fragen schnell beantwortet und Hindernisse frühzeitig adressiert werden.
- **Maximale Dauer des Onboardings:** Auf Basis bestehender Erfahrungswerte mit bestehenden Sandboxes kann ein Zeitraum von einigen Wochen bis zu sechs Monaten für das Onboarding vorgeschlagen werden, bevor die Testphase startet.

Testbetrieb

- **Entwicklung des Sandbox-Plans** mit Informationen über den Antragsteller und das in dem ausgewählten Antrag angegebene KI-System; dem voraussichtlichen Zeitplan für das Sandbox-Projekt, einschließlich eines Enddatums; der Ziele der Teilnahme und des Umfangs der Aktivitäten, die in der KI-Regulierungs-Sandbox durchgeführt werden sollen; einer Beschreibung der Anforderungen und Verpflichtungen gemäß der Verordnung (EU) 2024/1689 und gegebenenfalls anderer Rechtsvorschriften der Union, die in den Anwendungsbereich der Teilnahme an der Sandbox fallen; einer Angabe, ob das in dem ausgewählten Antrag angegebene KI-System die Verarbeitung personenbezogener Daten und die Notwendigkeit der Einbeziehung der zuständigen Datenschutzbehörde, Risikomanagement-Sicherheitsvorkehrungen und ein Verfahren zur Überwachung, Bewältigung und Meldung schwerwiegender Vorfälle, die während der Teilnahme an der KI-Regulierungs-Sandbox auftreten könnten, erfordert, wenn dies angesichts der voraussichtlich auftretenden Risiken als notwendig und angemessen erachtet wird; und gegebenenfalls einem Plan für Tests unter realen Bedingungen, die im Rahmen der Sandbox überwacht werden.

- **Iterative Projektbegleitung:** Kontinuierliche, kooperative Weiterentwicklung der Projekte in enger Abstimmung mit Behörden in den beteiligten Regionen und Sandbox-Administratoren.
- **Maximale Laufzeit für den Testbetrieb:** Die Dauer der Teilnahme an der Sandbox muss in einem angemessenen Verhältnis zur Einrichtung und zum Betrieb der Sandbox stehen, wobei zum einen die verfügbaren Kapazitäten, Ressourcen und Prioritäten, die von der zuständigen Behörde festgelegt wurden, zu berücksichtigen sind und zum anderen die Frage, ob das Sandbox-Projekt mehrere oder alle Aspekte der Konformitätsbewertung gemäß Artikel 43 der KI-VO oder andere in dieser Verordnung festgelegte Verpflichtungen abdeckt, relevant ist. Weiters haben die Komplexität, der Umfang und die spezifischen Anforderungen des ausgewählten Sandbox-Projekts direkten Einfluss auf die Laufzeit. Auf Basis bestehender Erfahrungswerte mit bestehenden Sandboxes werden mindestens 6 Monate für die Pilotphase und optional weitere 6 Monate für den vertiefenden Testbetrieb eingeplant.
- **Option auf Verlängerung des Testbetriebs:** Bis 30 Kalendertage vor dem geplanten Ende der Teilnahme können die zuständige Behörde und der Anbieter oder potenzielle Anbieter beschließen, die Dauer des Sandbox-Projekts zu verlängern, wenn beide damit einverstanden sind und eine solche Verlängerung gerechtfertigt ist.
- **Abbruch des Testbetriebs:** Die zuständigen Behörden können den Testprozess oder die Teilnahme an einer Sandbox vorübergehend oder dauerhaft aussetzen, wenn keine Maßnahmen zur Risikominderung möglich sind. Die zuständigen Behörden können davon ausgehen, dass keine Risikominderung möglich ist, wenn eine oder mehrere der folgenden Bedingungen zutreffen: wenn die im Sandbox-Plan festgelegten Teilnahmebedingungen und Parameter verletzt wurden; wenn die Bedingungen für eine vorübergehende oder dauerhafte Aussetzung des Testverfahrens oder der Teilnahme an der KI Regulatory Sandbox gemäß Artikel 57 Absatz 11 der KI-VO erfüllt sind, weil bei der Entwicklung und Erprobung von KI-Systemen erhebliche Risiken für die Gesundheit, Sicherheit und Grundrechte festgestellt wurden, die nicht wirksam gemindert werden können; sowie auf begründeten Antrag des Teilnehmers an einem Sandbox-Projekt.

Übergang in Normalbetrieb

- **Bewertung und Abschluss:** Dokumentation der Ergebnisse und gewonnenen Erkenntnisse durch die zuständige Behörde. Erfolgreich bewertete Systeme erhalten einen schriftlichen Nachweis, der mindestens folgende Elemente enthält: Arten von Aktivitäten, die in der Sandbox in Bezug auf Entwicklung, Schulung, Validierung und Testen des KI-Systems, soweit zutreffend, erfolgreich durchgeführt wurden, unter Angabe des Sektors oder der Sektoren, in denen die Sandbox betrieben wurde; die im Zusammenhang mit der Sandbox bewerteten rechtlichen Anforderungen und Verpflichtungen; ein Nachweis darüber, ob das zugelassene Sandbox-Projekt abgeschlossen wurde.
- **Exit Report:** Der gemäß Artikel 57 Absatz 7 der KI-VO vorgesehene Abschlussbericht dient Regulierungszwecken und enthält zusätzlich zu den oben genannten Elementen folgende Punkte: Beschreibung der wichtigsten regulatorischen Fragen, die in der KI Regulatory Sandbox untersucht wurden; wie diese Fragen gelöst wurden, einschließlich

spezifischer Empfehlungen, bewährter Verfahren, Instrumente, Benchmarks oder getesteter Maßnahmen, die wiederholt werden könnten; gegebenenfalls eine Aufzeichnung schwerwiegender Vorfälle innerhalb der KI Regulatory Sandbox; bewährte Verfahren und gewonnene Erkenntnisse, die in ähnlichen Fällen ausgeweitet werden können.

- **Feedback und kontinuierliche Verbesserung:** Während des gesamten Prozesses kann das Unternehmen regelmäßig Feedback geben und erhält selbst Rückmeldungen zu Fortschritt und Optimierungspotenzial. So wird die Sandbox individuell angepasst und kontinuierlich verbessert.
- **Sicherstellung von Datenschutz und Compliance:** Besonders wichtig sind die transparenten Informationen zu Datenschutz und sicheren Datenverarbeitungsprozessen. Rollenbasierte Zugriffskontrollen und Compliance-Checks werden von Anfang an eingerichtet.

Die zuständigen Behörden können freiwillige Folgeaktivitäten für Anbieter oder potenzielle Anbieter durchführen, die zuvor an der KI Regulatory Sandbox teilgenommen haben, sofern diese darauf abzielen, (i) die Wirksamkeit ihrer Teilnahme an der KI Regulatory Sandbox zu bewerten, (ii) relevante Informationen zu gewinnen, um KI-Innovationen und deren Einführung nach dem Verlassen der KI Regulatory Sandbox zu fördern, und (iii) diese Ergebnisse für die Erstellung des nationalen Jahresberichts zu nutzen. Der Wissenstransfer wird durch Workshops, gemeinsame Lernformate und eine offene Feedbackkultur gefördert. Die ausgelagerten technischen und administrativen Aufgaben nehmen den KMU einen Großteil des Aufwands ab, sodass sie sich auf die Weiterentwicklung ihrer Produkte und Innovationen konzentrieren können. Nach Abschluss eines Sandbox-Projekts können die Ergebnisse optional nicht nur für das Unternehmen selbst, sondern auch als Best Practice für die Community öffentlich geteilt werden, wodurch andere KMU von den Erfahrungen profitieren können.

Auf Anfrage der Marktüberwachungsbehörden im Rahmen von nachträglichen Marktüberwachungsmaßnahmen müssen die zuständigen Behörden, die das KI-System überwacht haben, zusätzlich zu den bereits vorgelegten Unterlagen Informationen über das in der Sandbox entwickelte oder getestete KI-System bereitstellen. Sensible Betriebsdaten im Zusammenhang mit den Tätigkeiten von Strafverfolgungs-, Grenzkontroll-, Einwanderungs- oder Asylbehörden dürfen dabei nicht offengelegt werden.

Resümierende Bewertung

Tabelle 7 präsentiert die spezifischen Chancen und Herausforderungen für eine zentralisierte KI Regulatory Sandbox in der Zusammenschau.

Tabelle 7: Gegenüberstellung von Chancen und Herausforderungen der beiden Ausprägungen einer zentralisierten KI-Sandbox

Ausrichtung	Chancen	Herausforderungen
Horizontal	• **Vielseitigkeit und Skalierbarkeit:** Horizontale Sandboxes bieten Unternehmen aus verschiedenen Branchen einen niederschwelligen Zugang zur Testung und Entwicklung von KI-Anwendungen, was Innovation fördert und eine schnelle Übertragung von Lösungen in unterschiedliche Anwendungsfelder ermöglicht. • **Synergieeffekte und Wissenstransfer:** Über sektorale Grenzen hinweg profitieren die Teilnehmer:innen vom Austausch vielseitiger Erfahrungen und Herangehensweisen, wodurch neue Anwendungsfälle identifiziert und Innovationen beschleunigt werden. • **Einheitliche regulatorische Orientierung:** Ein horizontaler Ansatz erleichtert die Umsetzung übergreifender Vorgaben, wie sie etwa die EU KI-VO vorsieht, und unterstützt Anbieter dabei, mit einer Lösung mehrere Compliance-Anforderungen zu adressieren.	• **Heterogene Anforderungen:** Die Vielfalt der beteiligten Branchen erschwert die Entwicklung einheitlicher Prozesse und technischer Standards, da unterschiedliche Domänen verschiedene Bedürfnisse und Risikoaspekte aufweisen. • **Verwässerung von Spezialisierung und Effizienz:** Allgemeine, branchenübergreifende Testansätze sind oft weniger tiefgehend als branchenspezifische, was die Identifikation und Kontrolle branchentypischer Risiken erschweren kann. • **Abstimmung von Daten- und Rechtsschutz:** Personenbezogene und branchenspezifische Daten unterliegen oft speziellen Schutzniveaus, deren Integration in eine horizontale Sandbox sorgfältig gesteuert werden muss.
Sektoral	• **Branchenspezifische Optimierung:** Sie können gezielt auf die besonderen Anforderungen, Risiken und Regularien einer Branche eingehen, wie z. B. im Gesundheitswesen, Finanzsektor, Medien oder Verkehr. So werden spezifische Compliance- und Ethikfragen besser adressiert. • **Förderung tieferer Innovation:** Durch die Fokussierung auf einen Sektor lassen sich speziellere Use Cases entwickeln, testen und validieren, was die Entwicklung hoch spezialisierter KI-Lösungen ermöglicht. • **Regulatorische Klarheit:** Verbesserte Zusammenarbeit mit branchenspezifischen Aufsichtsbehörden vereinfacht die Einhaltung von Vorschriften und passt Evaluationen an die besonderen Risiken des Sektors an.	• **Begrenzte Skalierbarkeit und Übertragbarkeit:** Innovationen und Erfahrungen aus einer branchenspezifischen Sandbox sind oft nicht ohne Anpassungen auf andere Branchen übertragbar, was die Verbreitung beschleunigter Innovation einschränken kann. • **Fragmentierung:** Es besteht die Gefahr, dass mehrere Sektor-Sandboxes nebeneinander entstehen, die nicht harmonisiert sind, sodass doppelte Anstrengungen, Intransparenz und Medienbrüche entstehen. • **Hoher Spezialisierungsaufwand:** Für den Aufbau und Betrieb muss tiefes Branchenwissen vorhanden sein, was Ressourcen und Expertenkapazitäten bindet. • **Komplexität im Datenschutz und in der Regulierung:** Je nach Branche bestehen sehr unterschiedliche und oft anspruchsvolle rechtliche

Ausrichtung	Chancen	Herausforderungen
	• **Strategische Partnerschaften:** Branchenspezifische Sandboxes ermöglichen es Unternehmen, Forschungseinrichtungen und Behörden, enger zusammenzuarbeiten und besondere Kenntnisse des Sektors zu bündeln.	Anforderungen (z. B. Gesundheitsdaten im Medizinsektor), die eine Sandbox technisch und organisatorisch stark belasten können. • **Zugangsbarrieren:** Branchenspezifische Sandboxes können kleinere oder branchenfremde Akteure ausschließen oder den Zugang erschweren, was Innovationen von außen behindert.

Quelle: Eigene Zusammenstellung

Sektorale Sandboxes können vor allem zur Entwicklung neuer branchen- oder technologiefeldspezifischer Standards und Leitlinien beitragen, indem praxisbezogene Erkenntnisse systematisch dokumentiert und in die Fachwelt zurückgespielt werden. Diese branchenspezifische regulatorische Klarheit ermöglicht es, KI-Lösungen schnell, sicher und rechtskonform im jeweiligen Sektor einzuführen und die Wettbewerbsfähigkeit der Unternehmen nachhaltig zu stärken. Eine horizontale KI Regulatory Sandbox kann demgegenüber die Koordination zwischen verschiedenen Sektoren verbessern und so eine einheitliche, adaptive Regulierung fördern, was insbesondere für Technologien gilt, die mehrere Branchen beeinflussen. Dies begünstigt eine flexible, lernfähige Regulierung, die sich an die schnelle Entwicklung im Bereich KI anpasst und die Wettbewerbsfähigkeit Europas stärkt.

10 Bibliographie

Allen, H. J. (2019). Regulatory sandboxes. *George Washington Law Review, 87*(3), 579–645. https://www.gwlr.org/wp-content/uploads/2019/06/87-Geo.-Wash.-L.-Rev.-579.pdf

Ansell, C., & Gash, A. (2018). Collaborative platforms as a governance strategy. *Journal of Public Administration Research and Theory, 28*(1), 16–32. https://doi.org/10.1093/jopart/mux030

Ansell, C., Sørensen, E., & Torfing, J. (2014). *Public innovation through collaboration and design*. Routledge. https://doi.org/10.4324/9780203795958

Asia-Pacific Economic Cooperation. (2021). *FinTech regulatory sandboxes: Capacity building – Summary report*. Asia-Pacific Economic Cooperation. https://www.apec.org/docs/default-source/publications/2021/3/FinTech-regulatory-sandboxes-capacity-building-summary-report/221_ec_FinTech-regulatory-sandboxes-capacity-building-summary-report.pdf

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business 37*(3), 371-414 https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1817&context=njilb

Australian Border Force (2025). *Regulatory sandbox for customs and border processes*. https://www.abf.gov.au/about-us/what-we-do/regulatory-sandbox, Zugriffsdatum: 5.5.2025

Australian Securities and Investments Commission. (2020). *INFO 248: Enhanced regulatory sandbox*. https://asic.gov.au/for-business-and-companies/innovation-hub/enhanced-regulatory-sandbox-ers/info-248-enhanced-regulatory-sandbox/

Auer, R., & Claessens, S. (2018). Regulating cryptocurrencies: Assessing market reactions to regulatory news. *BIS Quarterly Review* (September), 51–65. https://www.bis.org/publ/qtrpdf/r_qt1809f.htm

Baker McKenzie. (2020). *A guide to regulatory FinTech sandboxes internationally*. Baker McKenzie. https://www.bakermckenzie.com/-/media/files/insight/publications/2020/05/a_guide_to_regulatory_fintech_sandboxes_internationally_8734.pdf

Bason, C., & Austin, R. D. (2019, March–April). The right way to lead design thinking. *Harvard Business Review*, 82–91. https://hbr.org/2019/03/the-right-way-to-lead-design-thinking

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. In *Proceedings of the 2018 Conference on Fairness, Accountability and Transparency* (S. 149–159). PMLR 81. https://proceedings.mlr.press/v81/binns18a.html

Black, J., & Murray, A. D. (2019). Regulating AI and machine learning: Setting the regulatory agenda. *European Journal of Law and Technology, 10*(3). https://www.ejlt.org/index.php/ejlt/article/view/722

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. https://academic.oup.com/book/36491

Bundesministerium für Finanzen (BMF). (2023). *Regulatory Sandbox Beirat – Aufgaben und Zusammensetzung*. https://www.bmf.gv.at/themen/finanzmarkt/sandbox-beirat.html, Zugriffsdatum: 7.5.2025

Bundesministerium für Wirtschaft und Klimaschutz. (2019). *Freiräume für Innovationen – Das Handbuch für Reallabore*. https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/freiraeume-fuer-innovationen-1650878

Bundesministerium für Wirtschaft und Klimaschutz. (2024, 15. Oktober). *Reallabore-Gesetz: Referentenentwurf*. https://www.bmwk.de/Redaktion/DE/Downloads/Gesetz/20241015-referententwurf-reallaboreg-luv-download.pdf

Bundesministerium für Wirtschaft und Klimaschutz. (2024). *Reallabore-Gesetz Überblicksseite*. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2025/07/04-reallabore-innovationsportal.html, Zugriffsdatum: 27.06.2025

Bundesministerium für Arbeit und Wirtschaft. (2021). *Artificial Intelligence Mission Austria 2030 (AIM AT 2030)*. https://www.digitalaustria.gv.at/dam/jcr:44ad1b93-6358-42b8-9f65-1e74c9a39e7f/KI%20Strategie_AIM_AT_2030_UAbf.pdf

Bundeskanzleramt. (2020). *FTI-Strategie 2030 – Strategie der Bundesregierung für Forschung, Technologie und Innovation*. https://www.bundeskanzleramt.gv.at/dam/jcr:1683d201-f973-4405-8b40-39dded2c8be3/FTI_strategie.pdf

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie. (2024). *100 % Erneuerbare-Energie-Reallabore – Die Initiative*. https://www.reallabore.at, Zugriffsdatum: 7.5.2025

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie. (2025). *Energie.Frei.Raum – Programm & Evaluierung*. https://www.bmimi.gv.at/themen/innovation/publikationen/evaluierungen/energie-frei-raum.html, Zugriffsdatum: 7.5.2025

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie. (2024). *Green SandboxBuilder – Abschlussbericht* (Schriftenreihe 13/2024). https://nachhaltigwirtschaften.at/resources/sdz_pdf/schriftenreihe-2024-13-GreenSandboxBuilder.pdf

Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Cabinet Secretariat (Government of Japan). (2025, February 25). *Regulatory sandbox* (overview, English). https://www.cas.go.jp/jp/seisaku/s-portal/pdf/underlyinglaw/Japans_Regulatory_Sandbox_e.pdf

Cambridge Centre for Alternative Finance. (2019). *Early lessons on regulatory innovations to enable inclusive FinTech: Innovation offices, regulatory sandboxes and RegTech* (with UNSGSA). https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf

Canadian Securities Administrators. (2017, February 23). *The Canadian Securities Administrators launches a regulatory sandbox initiative* [News release]. https://www.securities-administrators.ca/news/the-canadian-securities-administrators-launches-a-regulatory-sandbox-initiative/, Zugriffsdatum: 8.5.2025

Commission nationale de l'informatique et des libertés (CNIL). (2023, July). *Bilan – Bac à sable « santé numérique » : Les recommandations de la CNIL aux lauréats*. https://www.cnil.fr/sites/cnil/files/2023-07/bilan_bac_a_sable_sante_numerique.pdf

Commission nationale de l'informatique et des libertés (CNIL). (2023, July). *Bilan – Bac à sable « EdTech » : Les recommandations de la CNIL aux lauréats*. https://www.cnil.fr/sites/cnil/files/2023-07/bilan_bac_a_sable_edtech.pdf

Commission nationale de l'informatique et des libertés (CNIL). (2025, April 11). *Intelligence artificielle et services publics : la CNIL publie le bilan de son « bac à sable »*. https://www.cnil.fr/fr/bilan-bac-a-sable-IA-services-publics, Zugriffsdatum: 8.5.2025

Commission nationale de l'informatique et des libertés (CNIL). (2025, April). *Bac à sable « IA et services publics » : Les recommandations de la CNIL aux lauréats*. https://www.cnil.fr/sites/cnil/files/2025-04/bac_a_sable_recommandations.pdf

CSC – IT Center for Science. (2025, February 17). *EUSAiR project – toward AI regulatory sandboxes* [News]. https://csc.fi/en/news/eusair-project-toward-ai-regulatory-sandboxes/, Zugriffsdatum: 8.5.2025

Digital Austria. (n.d.). *Digital Austria Act 2.0 – Schwerpunkte digitaler Innovation* [Portal]. https://www.digitalaustria.gv.at/, Zugriffsdatum: 7.5.2025

Digital Austria. (n.d.). *Digital Roadmap / Programme overview*. https://www.digitalaustria.gv.at/s/digitalroadmap, Zugriffsdatum: 7.5.2025

Economic Commission for Latin America and the Caribbean (ECLAC). (2024). *Regulatory sandboxes in developing economies: An innovative governance approach*. ECLAC. https://hdl.handle.net/11362/80496

European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0).* https://edpb.europa.eu/system/files/2020-10/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

Energieinstitut an der Johannes Kepler Universität Linz. (2024). *Factsheet: Regulatory Sandboxes im Energiebereich in Österreich.* https://energieinstitut-linz.at/wp-content/uploads/2024/11/RE-FRESCH-Factsheet-Regulatory-Sandboxes.pdf

European Commission. (2020). *An SME Strategy for a sustainable and digital Europe (COM(2020) 103 final).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0103

European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (COM(2021) 206 final).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Commission. (2022, June 27). *Spanish regulatory sandbox for AI pilot project launched*. https://digital-strategy.ec.europa.eu/en/news/spanish-regulatory-sandbox-artificial-intelligence

European Commission. (2023, February 14). *Launch of the European Blockchain Regulatory Sandbox*. https://digital-strategy.ec.europa.eu/en/policies/eu-blockchain-sandbox

European Commission. (2023). *Better Regulation Toolbox.* https://commission.europa.eu/system/files/2023-09/BR%20toolbox%20-%20Jul%202023%20-%20FINAL.pdf

European Union. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu/eli/reg/2024/1689/oj

ETIP SNET. (2023). Regulatory Sandboxes – Policy Report drafted by WG5's Regulatory Sandboxes Task Force. Publications Office of the European Union. https://data.europa.eu/doi/10.2833/008080

Financial Conduct Authority. (2015). *Regulatory sandbox (November 2015).* https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf

Financial Conduct Authority. (2015). *Regulatory sandbox.* https://www.fca.org.uk/publications/documents/regulatory-sandbox, Zugriffsdatum: 8.5.2025

FFG – Österreichische Forschungsförderungsgesellschaft. (2024). *Green SandboxBuilder – Projektbeschreibung (Projekt-ID 4425010).* https://www.ffg.at/projekt/4425010, Zugriffsdatum: 5.5.2025

Fraunhofer ISI & Trinomics. (2023). Study on Regulatory Sandboxes in the Energy Sector. Energy Transition Expertise Centre (EnTEC). https://data.europa.eu/doi/10.2833/848065

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

FMA – Finanzmarktaufsicht Österreich. (n.d.). *FMA Sandbox (Überblicksseite).* https://www.fma.gv.at/en/fintech-point-of-contact-sandbox/fma-sandbox/, Zugriffsdatum: 9.5.2025

FMA – Finanzmarktaufsicht Österreich. (2023, September 27). *Granting of authorisation as a crowdfunding service provider in the Regulatory Sandbox – CONDA Capital GmbH.* https://www.fma.gv.at/en/announcement-granting-of-authorisation-as-a-crowdfunding-service-provider-in-the-regulatory-sandbox-conda-capital-gmbh/, Zugriffsdatum: 9.5.2025

Financial Stability Board. (2020). *Regulatory and supervisory issues relating to outsourcing and third-party relationships (Discussion paper).* https://www.fsb.org/2020/11/regulatory-

and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships/, Zugriffsdatum: 7.5.2025

Financial Stability Board. (2021). *Regulatory and supervisory issues relating to outsourcing and third-party relationships: Overview of responses to the public consultation.* https://www.fsb.org/uploads/P140621.pdf

future.lab TU Wien. (2024). *Innovationswerkstatt – Workshop for Social Innovation and Sustainable Transformation in Urban Development.* https://futurelab.tuwien.ac.at/en/research-center/innovationswerkstatt, Zugriffsdatum: 8.5.2025

Gamper, A. M., & Koch, B. A. (2014). Federalism and legal unification in Austria. In D. Halberstam & M. Reimann (Eds.), *Federalism and legal unification: A comparative empirical investigation of twenty systems* (S. 103–119). Springer. https://link.springer.com/book/10.1007/978-94-007-7398-1

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society, 7*(1). https://doi.org/10.1177/2053951719897945

Gobierno de España. (2022). *Resumen ejecutivo: Piloto Sandbox de Inteligencia Artificial*. Ministerio de Asuntos Económicos y Transformación Digital. https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/20220627-Resumen-Piloto-Sandbox_IA-Final-ES.pdf

GRÜNSTATTGRAU. (2024). GRÜNSTATTGRAU – Die Plattform für Bauwerksbegrünung. https://gruenstattgrau.at/, Zugriffsdatum: 8.5.2025

Health Canada. (2025). Enabling advanced therapeutic products (ATPs). https://www.canada.ca/en/health-canada/corporate/about-health-canada/activities-responsibilities/strategies-initiatives/health-products-food-regulatory-modernization/advanced-therapeutic-products.html, Zugriffsdatum: 9.5.2025

Hoffmann-Riem, W. (2008). *Innovationsfreundliches Recht: Grundlagen, Technikfolgen, Governance*. Mohr Siebeck. https://www.mohrsiebeck.com/buch/innovationsfreundliches-recht-9783161493482

Hofmann, S., Schünemann, W. J., & Tami, A. (2020). Experimentation and evaluation in public sector innovation. *Public Administration, 98*(4), 837–852. https://doi.org/10.1111/padm.12627

ICO – Information Commissioner's Office. (2024). Regulatory Sandbox: Insights and final reports. https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/ (siehe z. B. Insights Report: https://ico.org.uk/media2/migrated/4030434/regulatory-sandbox-insights-report.pdf)

Industriellenvereinigung (IV). (2023). *IT-Industrie – Struktur, Trends und Standort-Anforderungen in Österreich*. Wien.

Innovationsstiftung für Bildung. (2021). Innovationslabore für Bildung. https://innovationsstiftung-bildung.at/, Zugriffsdatum: 8.5.2025

Jasanoff, S. (2011). Constitutional moments in governing science and technology. *Science and Engineering Ethics, 17*(4), 621–638. https://doi.org/10.1007/s11948-011-9305-5

Jenik, I., & Lauer, K. (2017). *Regulatory sandboxes: Potential for financial inclusion?* CGAP. https://www.cgap.org/research/publication/regulatory-sandboxes-potential-financial-inclusion

Kattel, R., Cepilovs, A., Drechsler, W., Kalvet, T., Lember, V., & Tõnurist, P. (2022). Innovation bureaucracy: A comparative analysis of innovation functions in public organizations. *Governance, 35*(2), 379–397. https://doi.org/10.1111/gove.12661

Kuhlmann, S., Stegmaier, P., & Konrad, K. (2019). Innovation governance: Towards a new approach to cope with societal challenges and tipping points. *Review of Policy Research, 36*(3), 421–438. https://doi.org/10.1111/ropr.12342

Leimüller, G., Rohrhofer, J., Gerger, A., Schranz, C., Aichholzer, M., Schachenhofer, M., Benes, C., & Ozclon, F. (2024). *Green SandboxBuilder: Regulatory Sandboxes im Bereich des nachhaltigen Bauens und Sanierens*. Schriftenreihe des BMK – Energie- und Umweltforschung, 13/2024. https://repositum.tuwien.at/entities/publication/33f26ee9-5b4b-4ffe-8e0d-1c9f8f2d10d5/full

Mantelero, A. (2022). AI and data protection by design: Shaping a risk-based approach to regulatory experimentation. *Computer Law & Security Review, 45*, 105692. https://doi.org/10.1016/j.clsr.2022.105692

OECD. (2021). *Regulatory sandboxes: Design and implementation considerations*. OECD Publishing. https://www.oecd.org/gov/regulatory-policy/regulatory-sandboxes-design-and-implementation-considerations.pdf

OECD. (2023). *Regulatory sandboxes in artificial intelligence*. *OECD Digital Economy Papers, No. 356.* https://doi.org/10.1787/3c8f3cdb-en

Parlament Österreich. (2022). *Foresightbericht: Datenschutz und algorithmische Systeme.* Parlamentsdirektion – Fachbereich Zukunftsthemen.

Parlament Österreich. (2022b). *Foresightbericht: Regulatorische Experimentierräume und adaptive Governance.* Parlamentsdirektion – Fachbereich Zukunftsthemen.

Personal Data Protection Commission (PDPC) Singapore. (2020). *Model AI Governance Framework (2nd ed.).* https://www.pdpc.gov.sg/Help-and-Resources/AI

Potacs, M., & Kircher, S. (2021). Regulatory Sandbox in der Finanzmarktaufsicht. *Recht der Wirtschaft (RdW), 2021*(14), 520–524.

Rajkomar, M., & Tan, S. C. (2022). Regulatory innovation and trust-building in emerging AI systems: Lessons from Singapore. *Asian Journal of Comparative Law, 17*(1), 45–68.

Rat der Europäischen Union. (2020). *Council conclusions on regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework (ST 13026/20).* https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/en/pdf

Sabel, C. F., & Simon, W. H. (2017). The management side of due process in the service-based welfare state. In N. R. Parrillo (Ed.), *Administrative Law from the Inside Out* (S.

63–86). Cambridge University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075353

Sabel, C. F., & Zeitlin, J. (2012). Experimentalist governance. In D. Levi-Faur (Ed.), *The Oxford Handbook of Governance* (S. 169–183). Oxford University Press. https://charlessabel.com/papers/Sabel%20and%20Zeitlin%20handbook%20chapter%20final%20(with%20abstract).pdf

Sitra. (2023). *Data economy tools in health sector ecosystems*. https://www.sitra.fi/en/projects/data-economy-tools-in-health-sector-ecosystems/, Zugriffsdatum: 8.5.2025

Smuha, N. A., Ahmed-Rengers, E., Hine, E., Li, W., MacLaren, J., Piselli, R., & Yeung, K. (2021). How the EU can achieve legally trustworthy AI: A response to the European Commission's proposal for an Artificial Intelligence Act. *SSRN Working Paper*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991

Stirling, A. (2008). "Opening up" and "closing down": Power, participation, and pluralism in the social appraisal of technology. *Science, Technology, & Human Values, 33*(2), 262–294. https://doi.org/10.1177/0162243907311265

TU Wien. (2024). *Green SandboxBuilder – Regulatory sandboxes in the field of sustainable construction and refurbishment*. https://www.tuwien.at/en/cee/ibb/zdb/research/ongoing-research-projects/greensandboxbuilder, Zugriffsdatum: 7.5.2025

UNSGSA (Office of the UN Secretary-General's Special Advocate). (2020). *Briefing on regulatory sandboxes*. https://www.unsgsa.org/sites/default/files/resources-files/2020-09/2020_UNSGSA_Briefing_Regulatory%20Sandboxes.pdf

van den Broek, J., Bos, L., & Kotterink, B. (2021). Responsible experimentation in the public sector: Balancing innovation and public values. *Technology in Society, 66*, 101628. https://doi.org/10.1016/j.techsoc.2021.101628

van Twist, M., & Scherpenisse, J. (2011). *An experiment with government*. NSOB. https://www.nsob.nl/publicaties (Startseite der Publikationsreihe)

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97–112. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law, 8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI. *Science Robotics, 2*(6), eaan6080. https://www.science.org/doi/10.1126/scirobotics.aan6080

Wagner, B., Eiden, L., & Müller, L. (2021). *Regulatory sandboxes and experimental governance: An ethical perspective* (HIIG Working Paper). https://www.hiig.de/en/publication/regulatory-sandboxes-and-experimental-governance/

Willems, T., & Van Dooren, W. (2021). Organizing for impact: How public agencies can structurally scale pilot projects. *Public Management Review, 23*(4), 509–527. https://doi.org/10.1080/14719037.2019.1668468

WKO – Wirtschaftskammer Österreich. (2021). *Positionspapier zur Innovationsfreundlichkeit im Bauverfahren*. https://www.wko.at

World Bank. (2020). *How to build a regulatory sandbox: A practical guide for policy makers*. https://digitalfinance.worldbank.org/sites/default/files/2022-11/How-to-Build-a-Regulatory-Sandbox-A-Practical-Guide-for-Policy-Makers.pdf

World Bank. (2020). *Global experiences from regulatory sandboxes (FinTech Note No. 8).* https://www.worldbank.org/en/topic/financialsector/publication/global-experiences-from-regulatory-sandboxes

Yeung, K., Howes, A., & Pogrebna, G. (2019). AI governance by human rights–centred design, deliberation and oversight: An end to ethics washing. In *The Oxford Handbook of AI Ethics*. Oxford University Press. https://academic.oup.com/edited-volume/34287/chapter/290657408

Zetzsche, D. A., Arner, D. W., Buckley, R. P., & Weber, R. H. (2020). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law, 25*(1), 31–103. https://ir.lawnet.fordham.edu/jcfl/vol25/iss1/2

11 Abbildungsverzeichnis

12 Tabellenverzeichnis

13 Abkürzungsverzeichnis

Abkürzung	Erläuterung
ABF	Australian Border Force
AI	Artificial Intelligence (künstliche Intelligenz)
AIT	Austrian Institute of Technology
AK	Arbeiterkammer
APEC	Asia-Pacific Economic Cooperation
ASAI	Österreichische Gesellschaft für Künstliche Intelligenz
ASIC	Australian Securities and Investments Commission
AT	Austria (Österreich)
AVG	Allgemeines Verwaltungsverfahrensgesetz
AWS	Austria Wirtschaftsservice Gesellschaft mbH
BE	Belgien
BGBL	Bundesgesetzblatt
BMBWF	Bundesministerium für Bildung, Wissenschaft und Forschung
BMF	Bundesfinanzministerium
BMK	Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
BMSGKP	Bundesministeriums für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
BMFWF	Bundesministerium für Frauen, Wissenschaft und Forschung
BMIMI	Bundesministerium für Innovation, Mobilität und Infrastruktur
BMWET	Bundesministerium für Wirtschaft, Energie und Tourismus
B-VG	Bundesverfassungsgesetz
CCAF	Cambridge Centre for Alternative Finance
CNIL	Commission Nationale de l'Informatique et des Libertés
CSA	Canadian Securities Administrators

DACH	Deutschland-Österreich-Schweiz
DIH	Digital Innovation Hub
DK	Dänemark
DSB	Datenschutzbehörde
DSGVO	Datenschutz-Grundverordnung
EDIH	European Digital Innovation Hub
EIWOG	Elektrizitätswirtschafts- und -organisationsgesetz
ES	Spanien
ETIP SNET	European Technology & Innovation Platform Smart Networks for Energy Transition
EU	Europäische Union
FCA	Financial Conduct Authority
FFG	Forschungsförderungsgesellschaft
FH	Fachhochschule
FI	Finnland
FMA	Finanzmarktaufsichtsbehörde
FMABG	Finanzmarktaufsichtsbehördengesetz
FOG	Forschungsorganisationsgesetz
FR	Frankreich
FTI	Forschung, Technologie und Innovation
GwG	Gaswirtschaftsgesetz
ICO	Information Commissioner's Office
idgF	in der geltenden Fassung
IKEM	Institut für Klimaschutz, Energie und Mobilität
IoT	Internet of Things
IV	Industriellenvereinigung
KI	Künstliche Intelligenz
KMU	Klein- und Mittelunternehmen

MDR	Medizinprodukteverordnung
MoU	Memorandum of Understanding
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
ÖGUT	Österreichische Gesellschaft für Umwelt und Technik
PDPC	Personal Data Protection Commission
PL	Polen
RTR	Rundfunk und Telekom Regulierungs-GmbH
SITRA	Finnish Innovation Fund
SWD	Staff Working Document der Europäischen Kommission
TEF	Testing and Experimentation Facility
TKG	Telekommunikationsgesetz
TRL	Technology Readiness Level
TU	Technische Universität
UNSGSA	Office of the UN Secretary-General's Special Advocate
WKO	Wirtschaftskammer Österreich
ZSI	Zentrum für soziale Innovation

14 Anhang 1: INTERNATIONALE GOOD-PRACTICE-BEISPIELE

Für die Entwicklung einer nationalen KI-Sandbox in Österreich ist es entscheidend, auf erprobte Modelle aus dem In- und Ausland zurückzugreifen. Good-Practice-Beispiele bieten die Möglichkeit, unterschiedliche Ansätze im Umgang mit Innovationsförderung, Regulierung und Governance vergleichend zu betrachten. Sie zeigen, wie regulatorische Testumgebungen konkret ausgestaltet werden können, welche Akteure eingebunden sind und welche Herausforderungen in der Umsetzung auftreten.

Die folgenden vier Beispiele decken unterschiedliche geografische und institutionelle Kontexte ab. Sie wurden ausgewählt, weil sie für die österreichische Diskussion unmittelbar anschlussfähig sind – sei es durch ihre sektorale Ausrichtung, ihren Governance-Ansatz oder ihre Einbindung in europäische Regulierungsprozesse:

- ein staatlich koordinierter Pilot zur Umsetzung der EU KI-VO in **Spanien** (siehe Kapitel 10.2.1),
- ein regionales Innovationsformat im Metropolitanraum **Zürich** (siehe Kapitel 10.2.2),
- ein thematisch fokussiertes Reallabor zur digitalen Gesundheitsförderung in **Baden-Württemberg** (siehe Kapitel 10.2.3),
- eine datenschutzzentrierte Sandbox unter Aufsicht der **luxemburgischen** CNPD (siehe Kapitel 10.2.4).

Alle Good-Practice-Beispiele sind entlang eines einheitlichen Schemas aufgebaut. Dieses umfasst Ausgangssituation, rechtlichen Rahmen, beteiligte Akteure, Gegenstand der Erprobung, Ablauf, Finanzierung, Governance, Evaluationsstrategie und Lessons Learned. Durch die vergleichbare Struktur lassen sich übertragbare Elemente und konkrete Handlungsoptionen für eine österreichische Umsetzung systematisch ableiten.

14.1 SPANISCHE KI-SANDBOX ZUR OPERATIVEN VORBEREITUNG DER EU KI-VO

Land / Region:

Spanien (nationaler Pilot mit EU-Kooperation)

Sektor / Branche

Die spanische KI-Sandbox ist sektorübergreifend konzipiert und adressiert vor allem sogenannte Hochrisiko-KI-Systeme gemäß der geplanten EU KI-VO. Zielbranchen sind unter anderem:

- **Gesundheitswesen** (z. B. medizinische Diagnose- und Entscheidungssysteme)
- **Industrie & Produktion** (z. B. KI in Qualitätskontrolle oder Robotik)
- **Mobilität** (z. B. autonome Systeme, Verkehrsmanagement)
- **Energie** (z. B. intelligente Netze, Verbrauchsprognosen)
- **Finanzsektor** (z. B. KI in Kreditvergabe, Betrugserkennung)

Durch die offene Ausschreibung und das modulare Design konnten sich KMU, Start-ups und größere Unternehmen aus verschiedenen Sektoren beteiligen, sofern ihre Anwendungen dem Hochrisiko-Regime der KI-VO unterliegen oder dies perspektivisch zu erwarten ist.

Ausgangssituation

Mit dem Vorschlag für die europäische KI-Verordnung (COM/2021/206) verfolgt die Europäische Kommission das Ziel, Hochrisiko-KI-Systeme durch ein verbindliches Regelwerk zu regulieren. Gleichzeitig besteht in vielen Mitgliedstaaten – insbesondere bei Start-ups und KMU – eine erhebliche Unsicherheit darüber, wie die Anforderungen (z. B. Risikomanagement, Transparenz, Konformitätsbewertung) praktisch umzusetzen sind.

Spanien entschied sich 2022 dazu, in enger Kooperation mit der Europäischen Kommission eine nationale **Regulatory Sandbox für KI** einzurichten, um:

- die praktische Operationalisierung der Anforderungen der KI-VO zu testen,
- Unternehmen frühzeitig auf die Umsetzung vorzubereiten,
- Aufsichtsbehörden und Standardisierungsstellen in die Auslegung und Umsetzung einzubinden,
- und durch Erfahrungswissen zur EU-weiten Harmonisierung beizutragen.

Die Initiative war eingebettet in Spaniens **Nationale Strategie für Künstliche Intelligenz (ENIA)** sowie in das nationale Aufbau- und Resilienzprogramm (Komponente 16), das mit Mitteln aus dem **EU Recovery and Resilience Fund** finanziert wird.

Rechtlicher Rahmen

Die spanische KI-Sandbox wurde als **pilotiertes Experimentierumfeld** auf Grundlage des nationalen **Recovery and Resilience Plan (PERTE Digitalización)** initiiert, ohne dass eine spezielle gesetzliche Experimentierklausel erforderlich war. Rechtsgrundlage war vielmehr eine Kombination aus:

- dem nationalen Rechtsrahmen für staatlich geförderte Pilotprojekte,
- dem politischen Mandat durch die **Estrategia Nacional de Inteligencia Artificial (ENIA)**,
- sowie der flankierenden Unterstützung durch die Europäische Kommission im Rahmen der Vorbereitung der KI-VO.

Im Sinne eines **Soft-Law-Ansatzes** wurden keine formellen gesetzlichen Vorschriften ausgesetzt. Stattdessen wurde die Sandbox als „kontrollierte Umgebung“ konzipiert, in der regulatorische Anforderungen der zukünftigen KI-VO **simuliert** und **gemeinsam interpretiert** werden konnten. Dabei war insbesondere die **praktische Anwendung von Pflichten aus Art. 9–15 KI-VO** (z. B. Daten-Governance, Risikomanagement, Transparenz, Konformitätsbewertung) Gegenstand der Tests.

Ein wichtiger rechtlicher Nebeneffekt war die Stärkung der Behördenkompetenz zur späteren **Anerkennung von Konformitätsverfahren** und zur Vorbereitung einer **nationalen Aufsichtsstruktur** für KI.

Beteiligte Akteure

1. **Öffentliche Stellen**
   - **Ministerio de Asuntos Económicos y Transformación Digital / SEDIA (Spanisches Wirtschaftsministerium / Staatssekretariat für Digitalisierung und KI)**
     → *Gesamtkoordination des Projekts*, Durchführung der Ausschreibung, Auswahl der Teilnehmer, Definition der Arbeitsstruktur (FG1/FG2), Ansprechpartner für die EU-Kommission.
   - **Europäische Kommission (GD CONNECT, JRC)**
     → *Politisch-strategische Begleitung*, Sicherstellung der Kohärenz mit der KI-VO, Abstimmung über Harmonisierungspotenziale, Bewertung der Übertragbarkeit auf andere Mitgliedstaaten.
   - **Agencia Española de Protección de Datos (AEPD)**
     → *Fachaufsicht für datenschutzrechtliche Implikationen* der getesteten KI-Systeme, Beratung der Teilnehmer:innen in Fragen der DSGVO-Konformität, Input zur Gestaltung datenschutzfreundlicher KI-Anwendungen.
   - **Instituto Nacional de Ciberseguridad (INCIBE)**
     → *Unterstützung bei Sicherheits- und Resilienzfragen*, z. B. Anforderungen an IT-Sicherheitsarchitektur, Risikomanagement und Bedrohungsanalysen.
   - **Normierungs- und Standardisierungsstellen (UNE, ENAC)**
     → *Einbindung bestehender bzw. Entwicklung neuer Normen*, insbesondere zur Konformitätsbewertung, zu technischen Dokumentationen und zur Qualitätssicherung.
2. **Unternehmen / Start-ups (Teilnehmer der Sandbox)**
   - Entwicklung und Vorstellung eines *Hochrisiko-KI-Systems* mit Relevanz für die KI-VO
   - Teilnahme an einem kooperativen Testverfahren im Rahmen von **Focus Group 1 (FG1)**
   - Gemeinsame Ausarbeitung, Erprobung und Bewertung von **Konformitätsstrategien**, z. B. für Risikomanagement, Erklärbarkeit, technische Dokumentation
   - *Feedbackgeber* zu Umsetzbarkeit, Aufwand und Klarheit der geplanten EU-Vorgaben
3. **Forschungsinstitutionen / Standardisierungsnetzwerke**
   - Universitäten, Technologiezentren, u. a. Barcelona Supercomputing Center
     → *Unterstützung bei der technischen Bewertung*, Methodenanalyse, ethischen Fragen, teilweise Co-Design der Evaluationskriterien
   - Beteiligung an **Focus Group 2 (FG2)** zur Ableitung von *Guidelines, Standards und Tools*
4. **Weitere Anspruchsgruppen**

- **Zivilgesellschaftliche Gruppen (Ethik, Grundrechte, Verbraucherorganisationen)**
  → *Beratende Mitwirkung bei FG2*, z. B. bei Fragen zu Transparenzpflichten, Nichtdiskriminierung, sozialer Akzeptanz
- **Digital Innovation Hubs / TEFs**
  → *Technische Infrastruktur*, unterstützende Testumgebung für reale Szenarien

Gegenstand der Erprobung

Im Zentrum der spanischen KI-Sandbox stand die praktische Erprobung der Anforderungen der zukünftigen europäischen KI-Verordnung (insb. Kapitel 2 und 3) für sogenannte Hochrisiko-KI-Systeme. Ziel war es, regulatorische Pflichten des geplanten Rechtsrahmens in realen Anwendungsszenarien gemeinsam mit Unternehmen und Aufsichtsbehörden umzusetzen und dabei Umsetzbarkeit, Herausforderungen und Unterstützungsbedarfe systematisch zu erfassen.

Konkret wurden folgende Elemente erprobt:

- **Risikomanagementsysteme gemäß Art. 9 KI-VO**

  → Aufbau, Pflege und Dokumentation systematischer Verfahren zur Risikoidentifikation, -bewertung und -minderung bei KI-Anwendungen.

- **Daten- und Daten-Governance-Anforderungen (Art. 10 KI-VO)**

  → Prüfung der Qualität, Repräsentativität, Relevanz und Bias-Kontrolle der Trainingsdaten.

- **Technische Dokumentation und Transparenz (Art. 11–13 KI-VO)**

  → Erstellung strukturierter technischer Dokumentation zur Nachvollziehbarkeit der Systemlogik und Nachweis der Erfüllung regulatorischer Anforderungen.

- **Human Oversight – menschliche Aufsicht (Art. 14 KI-VO)**

  → Implementierung von Kontrollmechanismen, Warnsystemen und menschlichen Eingriffsmöglichkeiten.

- **Konformitätsbewertungsverfahren und freiwillige Vorabkontrolle**

  → Simulation von Konformitätsprozessen in Zusammenarbeit mit Standardisierungsstellen und Vorbereitung auf spätere CE-Kennzeichnung.

- **Post-Market-Monitoring und Feedback-Schleifen (Art. 61 KI-VO)**

  → Erprobung von Überwachungspflichten nach Inverkehrbringen, inklusive interner Audits, Fehlerberichterstattung und Updates.

Die Erprobung erfolgte in **kooperativen Testszenarien zwischen Behörden und Unternehmen** in **Focus Group 1 (FG1)**. Parallel arbeitete **Focus Group 2 (FG2)** an der Auswertung und Ableitung von Good Practice Guidelines, Evaluationsmetriken und Empfehlungen für ein zukünftiges europäisches Sandbox-Modell.

In der ersten Kohorte der Sandbox wurden **16 Unternehmen** aus verschiedenen Sektoren über ein Open-Call-Verfahren ausgewählt. Die teilnehmenden Firmen stammten aus folgenden Anwendungsfeldern:

- **Gesundheitswesen / Medizintechnik** (z. B. KI-gestützte Diagnostik)
- **Human Resources** (z. B. Sprachanalyse in Bewerbungsprozessen)
- **Finanz- und Versicherungswesen** (z. B. Risikobewertungsmodelle)
- **Verkehr / Mobilität** (z. B. prädiktive Verkehrssteuerung)
- **Energie / Smart Grids** (z. B. Steuerung und Optimierung von Stromnetzen)
- **Öffentliche Verwaltung** (z. B. Dokumentenanalyse im E-Government)

Der Schwerpunkt lag auf **Klein- und Mittelunternehmen (KMU)**, die ihre Systeme häufig erstmalig regulatorisch strukturierten. Die Sandbox ermöglichte ihnen den Zugang zu Aufsichtskompetenz und technischem Feedback sowie die gemeinsame Entwicklung konformer Verfahren unter realen Bedingungen.

Dauer & Ablauf

Die spanische KI-Sandbox ist als mehrjähriger Pilot im Zeitraum **2022–2025** konzipiert und wird im Rahmen des **spanischen Aufbau- und Resilienzplans (PERTE Digitalización)** mit **rund 4,3 Mio. EUR** finanziert. Der operative Ablauf gliederte sich in drei zentrale Phasen:

Phase 1: Konzeption & Ausschreibung (Q2–Q4 2022)

- Gemeinsame Ausarbeitung der Methodik durch das spanische Wirtschaftsministerium (SEDIA), die Europäische Kommission und weitere beteiligte Institutionen
- Veröffentlichung eines **Open Calls zur Teilnahme an FG1** (Unternehmen mit Hochrisiko-KI-Systemen)
- Parallel: Aufbau von **Focus Group 2 (FG2)** mit Expert:innen aus Behörden, Normung, Wissenschaft und Ethik

Phase 2: Testbetrieb in Sandbox (Q1–Q4 2023)

- Durchführung der Tests in **FG1** mit etwa **3 Monaten Testzeitraum pro Unternehmen**
- Begleitung durch zuständige Behörden (Datenschutz, Standardisierung, Cybersicherheit)
- Iterative Feedbackschleifen zwischen Unternehmen und Regulierungspartnern
- **FG2** analysierte parallel die Prozesse, sammelte Erfahrungswissen und erarbeitete Entwürfe für Umsetzungshilfen und Leitlinien

Phase 3: Auswertung & Dissemination (ab Q4 2023)

- Erstellung von **Leitlinien, Toolkits und Standards** auf Basis der Testergebnisse
- Veröffentlichung der Ergebnisse im Rahmen der **spanischen EU-Ratspräsidentschaft (2023)**

- Geplante Öffnung der Ergebnisse für andere EU-Mitgliedstaaten mit Ziel eines **paneuropäischen Sandbox-Modells**
- Fortsetzung und Skalierung des Programms bis 2025 mit erweiterten Anwendungsfällen und institutioneller Verstetigung

Finanzierung und Ressourcen

Die spanische KI-Sandbox wurde vollständig durch öffentliche Mittel finanziert und in den **nationalen Aufbau- und Resilienzplan (Plan de Recuperación, Transformación y Resiliencia)** eingebettet. Die Finanzierung erfolgte im Rahmen von **Komponente 16 („Reforma institucional y fortalecimiento de las capacidades del sistema nacional de ciencia, tecnología e innovación“) der spanischen ENIA** (Estrategia Nacional de Inteligencia Artificial). Als Finanzierungsquelle diente primär der **EU-Aufbaufonds „NextGenerationEU“**, aus dem Spanien im Rahmen des Instruments für Aufbau und Resilienz (RRF) Mittel bezog.

Für das Pilotprojekt der KI-Sandbox wurden **rund 4,3 Mio. EUR** budgetiert, mit einem geplanten Umsetzungszeitraum von **2022 bis 2025**. Die Mittel wurden vom **Ministerio de Asuntos Económicos y Transformación Digital** verwaltet und zweckgebunden für folgende Einsatzbereiche verwendet:

- Aufbau und Koordination der Governance-Struktur (FG1, FG2)
- Durchführung und Supervision der Tests mit Unternehmen
- Erstellung von Leitlinien, Dokumentationsstandards und Tools
- Begleitforschung, Evaluierung und Dissemination

Personelle Ressourcen:

Das Projekt stützte sich auf ein multidisziplinäres Team aus Beamt:innen, technischen Fachleuten und externen Expert:innen aus Behörden (z. B. Datenschutz, Cybersicherheit), Forschungseinrichtungen und Standardisierungsorganisationen. Die operative Koordination erfolgte durch eine zentrale Projektgruppe im Ministerium (SEDIA), ergänzt durch projektbezogene Ausschreibungen für fachliche Beratung und technische Begleitung.

Infrastrukturelle Ressourcen:

Die Tests wurden in virtuellen und teilrealen Umgebungen durchgeführt. Dabei wurde teilweise auf vorhandene digitale Infrastruktur von Forschungseinrichtungen, Digital Innovation Hubs und Testeinrichtungen aus dem EU-Programm *Digital Europe* (z. B. TEFs) zurückgegriffen. Die technische Umsetzung der Testprozesse erfolgte in enger Zusammenarbeit mit Unternehmen, wobei keine physisch-institutionalisierte Sandbox errichtet wurde, sondern ein **„prozessuales Sandbox-Modell“** verfolgt wurde.

Governance-Modell

Das Governance-Modell der spanischen KI-Sandbox folgt einem **zweistufigen Strukturprinzip**, das zwischen operativer Durchführung und strategischer Auswertung

unterscheidet. Es wurde entwickelt, um sowohl regulatorisches Lernen als auch Praxiserprobung zu ermöglichen – unter enger Einbindung nationaler und europäischer Stellen.

Zweistufige Steuerungsstruktur

Focus Group 1 (FG1): Operative Testeinheit

- Zuständig für die Durchführung konkreter Testszenarien mit Unternehmen.
- Moderiert durch das *Ministerio de Asuntos Económicos y Transformación Digital* (SEDIA).
- Beteiligung zuständiger Behörden, darunter:
    - **Agencia Española de Protección de Datos (AEPD)** – Datenschutz,
    - **Instituto Nacional de Ciberseguridad (INCIBE)** – Cybersicherheit,
    - Nationale Normungsstellen (UNE, ENAC) – Standardisierung und Konformitätsfragen.
- Unternehmen entwickelten gemeinsam mit Behörden und Expert:innen konkrete Lösungsstrategien zur praktischen Umsetzung der Anforderungen der KI-VO (z. B. Risikomanagement, Datenqualität, Konformitätsprozesse).
- Die Tests wurden in **zeitlich begrenzten Kohorten** durchgeführt (ca. 3 Monate), mit enger Supervision durch öffentliche Stellen.

Focus Group 2 (FG2): Strategisch-reflexive Begleitstruktur

- Aufgabe: *Ableitung von Leitlinien, Standardvorschlägen und Lessons Learned* zur operativen Umsetzung der KI-VO.
- Zusammensetzung:
    - Vertreter:innen der **Europäischen Kommission**,
    - **Standardisierungsinstitutionen** (CEN/CENELEC, ETSI),
    - **Hochschulen und Forschungszentren**,
    - **Ethikexpert:innen und zivilgesellschaftliche Organisationen**.
- Arbeiteten entlang der in FG1 erhobenen Anwendungsfälle, analysierte deren Umsetzbarkeit und entwickelten **praxisnahe Empfehlungen** für eine mögliche EU-weite Harmonisierung.

Weitere Governance-Elemente

Transparente Auswahlprozesse für Unternehmen via Ausschreibung mit öffentlich einsehbaren Kriterien

- Die Beteiligung an FG1 erfolgte über einen **offenen nationalen Call for Applications**, veröffentlicht im Oktober 2022.
- Der Ausschreibungsprozess wurde vom Ministerium (SEDIA) gesteuert und zielte insbesondere auf **Start-ups und KMU** mit Hochrisiko-KI-Anwendungen ab.

- Die Unternehmen mussten ein **konzeptionelles Dossier** einreichen (max. 10 Seiten), das folgende Inhalte umfasste:
    - Beschreibung des KI-Systems und seine potenzielle Relevanz unter der KI-VO,
    - Innovationsgrad, gesellschaftlicher Nutzen und Reifegrad (TRL),
    - Identifizierte regulatorische Unklarheiten oder Umsetzungsbarrieren.
- Die Einreichungen wurden durch ein **interdisziplinäres Expertengremium** (aus Verwaltung, Forschung, Standardisierung) nach einem Kriterienkatalog bewertet.
- Der Aufwand für Unternehmen lag laut Ministerium bei **5–10 Arbeitstagen**.
- Insgesamt wurden **16 Unternehmen** aus Bereichen wie Gesundheit, Mobilität, HR, Energie, Verwaltung und Finanzen ausgewählt.
- Die Teilnahme war **kostenfrei** und wurde organisatorisch von der öffentlichen Hand getragen.

Dokumentation und Berichterstattung

- Alle Teilprojekte unterlagen **systematischen Dokumentationspflichten** gegenüber FG1 und wurden durch strukturierte Feedback- und Reviewprozesse in FG2 eingespeist.
- Die Ergebnisse flossen in nationale und europäische **Leitliniendokumente** ein.

Ethikleitlinien

- Die Sandbox orientierte sich am **spanischen Ethikrahmen für KI** sowie an den **OECD AI Principles**.
- Ethikfragen wurden systematisch in FG2 adressiert und in alle Leitfäden integriert.

Einbindung europäischer Akteure

- Die Europäische Kommission war durch die Generaldirektion CONNECT und das Joint Research Centre aktiv eingebunden.
- Ziel war die Entwicklung eines **paneuropäischen Referenzmodells**, das auf andere Mitgliedstaaten übertragbar ist.
- Eine spätere Koordination über das **AI Board** ist ausdrücklich vorgesehen.

Ausrichtung auf institutionelle Verstetigung

- Das Projekt diente der **Vorbereitung einer dauerhaften nationalen KI-Aufsicht**, wie sie in Art. 59 und 60 KI-VO vorgesehen ist.
- Die Erfahrungen sollen langfristig in die operative Gestaltung von Konformitätsbewertung und Marktüberwachung einfließen.

Evaluations- und Skalierungsstrategie

Die spanische KI-Sandbox war von Beginn an als **lernorientierter Pilot** mit politischem Folgeanspruch konzipiert. Entsprechend wurde ein strukturierter Evaluationsrahmen integriert, dessen Ergebnisse sowohl national als auch europäisch weiterverwendet werden sollten.

Erfolgsmessung:

- Die Evaluation erfolgte entlang **konkreter Umsetzungserfahrungen** der teilnehmenden Unternehmen in Bezug auf zentrale Pflichten der KI-VO (z. B. Risikomanagement, Transparenz, technische Dokumentation).
- Die **Focus Group 2 (FG2)** sammelte während der Testphase systematisch Daten zur Umsetzbarkeit, Rechtsklarheit, Belastbarkeit und Effizienz der Prozesse.
- Ergänzt wurde dies durch **qualitative Rückmeldungen** der teilnehmenden Unternehmen, Expert:innen und Behörden (z. B. zu Aufwand, Rechtssicherheit, Standardisierungspotenzial).
- Die Ergebnisse wurden im **„Resumen ejecutivo“** dokumentiert und im Kontext der spanischen EU-Ratspräsidentschaft veröffentlicht, u. a. zur Einspeisung in die Arbeit des **AI Board**.

Skalierungs- und Verstetigungspläne:

- Die spanische Regierung verfolgt das Ziel, auf Basis der Pilotphase eine **dauerhafte nationale KI-Aufsichtsstruktur** zu etablieren. Die Sandbox diente der Vorbereitung dieser Struktur – insbesondere hinsichtlich Kompetenzen, Schnittstellen und Prüfverfahren.
- Es besteht eine klare politische Zielsetzung, dass die erarbeiteten **Leitlinien und Tools** mittelfristig EU-weit anwendbar gemacht werden (z. B. durch Harmonisierung über das AI Board).
- Die Öffnung des Modells für **andere Mitgliedstaaten** wurde von Beginn an angestrebt. Die Europäische Kommission war nicht nur Beobachterin, sondern explizit Partnerin mit der Option zur Nachnutzung.
- Perspektivisch ist die Integration in das entstehende EU-Ökosystem für vertrauenswürdige KI geplant – inklusive Verknüpfung mit TEFs, Digital Innovation Hubs und nationalen Aufsichtsbehörden.

Ergebnisse / Lessons Learned

Die spanische KI-Sandbox hat wertvolle praktische Erkenntnisse für die Umsetzung der europäischen KI-Verordnung hervorgebracht. Die Ergebnisse stammen vor allem aus dem offiziellen Abschlussbericht der Pilotphase (Gobierno de España, 2023), dem Staff Working Document der Europäischen Kommission zur regulatorischen Lernpraxis (SWD (2023) 277 final) sowie begleitenden politischen Mitteilungen und Analysepapieren.

Technische und regulatorische Erkenntnisse:

- Unternehmen konnten zentrale Anforderungen der KI-VO, insbesondere zu Risikomanagement (Art. 9), Datenqualität (Art. 10), Transparenz (Art. 13) und

menschlicher Aufsicht (Art. 14), in kontrollierten Szenarien umsetzen und dabei Umsetzungsbarrieren identifizieren (Gobierno de España, 2023, S. 3–4).

- Die Sandbox zeigte, dass gerade KMU erheblichen Unterstützungsbedarf bei der Auslegung und Umsetzung der technischen Dokumentationspflichten haben. Es wurden einheitliche, standardisierte Strukturierungshilfen für Konformitätsprozesse entwickelt (SWD (2023) 277 final, S. 27).
- Die Zusammenarbeit mit Behörden (z. B. Datenschutzaufsicht, Cybersicherheitsagentur) ermöglichte frühzeitige Klärungen bei der Anwendung horizontaler Vorschriften (z. B. DSGVO, Produktsicherheitsrecht).

Entwicklung von Umsetzungshilfen:

- Die Arbeit der Focus Group 2 (FG2) resultierte in einer Reihe von Good Practice Guidelines zur Umsetzung der AI-Act-Anforderungen, die in Form von Empfehlungen, Tools und Checklisten formuliert wurden. Diese sollen als Grundlage für eine EU-weit anwendbare Implementierungshilfe dienen (Gobierno de España, 2023).
- Die Ergebnisse wurden der Europäischen Kommission übermittelt und während der spanischen EU-Ratspräsidentschaft 2023 öffentlich vorgestellt (European Commission, 2022).

Auswirkungen auf bestehende Regelungen:

- Die Sandbox zeigte, wo nationale Rechtsvorschriften (z. B. zu Aufsicht, Haftung, Interoperabilität) künftig angepasst werden müssen, um effektiv mit der KI-VO koordiniert zu werden (SWD (2023) 277 final, S. 38).
- Darüber hinaus förderte das Projekt ein stärkeres Verständnis der Anforderungen in Behörden, was als Vorbedingung für den künftigen Aufbau einer nationalen Aufsichtsstruktur betrachtet wird.

Übertragbarkeit auf andere Kontexte:

- Die zweigleisige Struktur (FG1: operative Tests; FG2: strategisch-methodische Auswertung) wird im Bericht der Kommission als besonders geeignetes Modell für andere Mitgliedstaaten hervorgehoben (SWD (2023) 277 final, Box 7).
- Spanien wird aufgrund der Erfahrungen als Referenzfall für die Entwicklung eines EU-weiten Ansatzes zu regulatorischen Sandboxes im Rahmen der KI-VO angesehen (European Commission, 2023a).

Relevanz für Österreich

Die spanische KI-Sandbox liefert zentrale Erkenntnisse und Referenzstrukturen, die für den Aufbau einer regulatorischen Sandbox für künstliche Intelligenz in Österreich unmittelbar nutzbar sind – sowohl in rechtlicher, institutioneller als auch in praktischer Hinsicht.

Übertragbare Elemente:

- **Modulare Struktur mit operativer Testeinheit (FG1) und strategischer Reflexionseinheit (FG2):** Dieses Modell erlaubt die gleichzeitige Durchführung

konkreter Praxistests mit Unternehmen und die evidenzbasierte Entwicklung regulatorischer Leitlinien. Es könnte in Österreich z. B. durch eine Kooperation von FFG, BMIMI, Datenschutzbehörde und Forschungseinrichtungen umgesetzt werden.

- **Frühe Einbindung zuständiger Behörden (z. B. Datenschutz, Standardisierung, Marktaufsicht):** Das spanische Modell zeigt, wie Kooperationsstrukturen aufgebaut werden können, bevor ein gesetzlicher Rahmen wie die KI-VO vollständig in Kraft tritt.
- **Sektorübergreifender Ansatz:** Durch die Offenheit für Use Cases aus Gesundheit, Mobilität, Industrie, Verwaltung etc. lassen sich unterschiedliche regulatorische Konstellationen in einem einzigen Format abbilden. Diese Breite wäre auch für Österreich – etwa im Rahmen eines Bundesreallabors für KI – sinnvoll.
- **Förderung regulatorischen Lernens innerhalb der Verwaltung:** Österreichische Behörden könnten über eine Sandbox gezielt interne Kompetenzen im Umgang mit KI-Anwendungen aufbauen, insbesondere im Hinblick auf die zukünftige Marktaufsicht gemäß KI-VO.

Herausforderungen für Österreich:

- **Fehlende rechtliche Experimentierklausel:** Im Gegensatz zu Spanien existiert derzeit in Österreich keine klar definierte rechtliche Grundlage für regulatorische Erprobung außerhalb bestehender Gesetze. Hier wäre etwa ein sektorbezogener Rechtsrahmen (z. B. in der DSGVO oder dem E-Government-Gesetz) zu prüfen.
- **Fragmentierung der Zuständigkeiten:** Während Spanien auf eine zentrale Koordination durch das Wirtschaftsministerium setzt, ist in Österreich die Zuständigkeit für KI-Politik auf mehrere Ministerien verteilt. Eine erfolgreiche Umsetzung erfordert daher abgestimmte Governance.
- **Ressourcenausstattung und Dauer:** Der spanische Pilot war mit rund 4,3 Mio. EUR über drei Jahre finanziert. Für ein tragfähiges österreichisches Modell wäre eine vergleichbare mittelfristige Förderlogik erforderlich.

Potenziale:

- Österreich könnte mit einem nationalen KI-Reallabor ein starkes Signal für innovationsfreundliche und grundrechtskonforme Regulierung setzen – etwa im Bereich *Public Interest AI*, nachhaltiger Technologieentwicklung oder vertrauenswürdiger Gesundheitsanwendungen.
- Die Einbindung europäischer Akteure (z. B. über das AI Board oder gemeinsame Pilotprojekte) würde es ermöglichen, eine österreichische Lösung mit der europäischen Harmonisierung zu verzahnen.

Referenzen

European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM(2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Commission. (2022, June 27). First regulatory sandbox on artificial intelligence presented. https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented

European Commission. (2023). AI regulatory sandbox approaches in EU Member States – Overview. https://artificialintelligenceact.eu/de/ai-regulatory-sandbox-approaches-eu-member-state-overview/

European Commission. (2023). Regulatory learning in the EU: Guidance on regulatory sandboxes, testbeds, and living labs. Commission Staff Working Document SWD (2023) 277 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2023:277:FIN

Gobierno de España. (2023). Resumen ejecutivo: Piloto Sandbox de Inteligencia Artificial. Ministerio de Asuntos Económicos y Transformación Digital.

Ministerio de Ciencia, Innovación y Universidades. (2024). Guía para entornos controlados de pruebas (sandbox). TECHFRIENDLY S.L. Secretaría General de Innovación

14.2 INNOVATION-SANDBOX FÜR KÜNSTLICHE INTELLIGENZ IN DER SCHWEIZ

Land / Region:

Schweiz – Kanton Zürich (Metropolitanraum Zürich)

Sektor / Branche

Die Innovation-Sandbox Zürich ist sektorübergreifend angelegt und fokussiert auf KI-Anwendungen mit erhöhtem Klärungsbedarf im regulatorischen Umfeld. In der ersten Pilotphase (2022–2024) wurden insbesondere folgende Bereiche adressiert:

- Mobilität & Smart City (z. B. KI-basierte Erkennung freier Parkplätze, Verkehrsflusssteuerung)
- Infrastruktur & Bauwesen (z. B. automatisierte Inspektion und Wartung mittels Drohnen und Computer Vision)
- Öffentliche Verwaltung & E-Government (z. B. maschinelle Übersetzung von Verwaltungsdokumenten, KI-Assistenz bei Standardvorgängen)
- Bildung (z. B. KI-gestützte Korrektur von Aufgaben im Schulbereich, datenschutzkonforme Lernsysteme)
- Industrie & Robotik (z. B. Normierungsfragen für autonome Systeme, Vorbereitung auf EU-Regulierung)

Im Rahmen von offenen Ausschreibungen konnten sich Unternehmen, Forschungseinrichtungen und öffentliche Stellen bewerben, sofern die Vorhaben praxisrelevant waren und offene Rechtsfragen im Kontext von KI betrafen – etwa in Bezug auf Datenschutz, Transparenz oder Interoperabilität. Die Auswahl der Use Cases zielte bewusst auf sektorale Diversität, um sektorübergreifende Erkenntnisse für eine künftige KI-Regulierung zu gewinnen.

Ausgangssituation

Die Schweiz verfügt bislang über keinen spezifischen Rechtsrahmen für künstliche Intelligenz, was zu **Unsicherheiten bei der Entwicklung und Anwendung von KI-Systemen** führt – insbesondere im Hinblick auf Datenschutz, Transparenzanforderungen und Haftungsfragen (vgl. BAKOM 2025: 26). Bestehende Regelungen wie das Datenschutzgesetz (DSG) oder das Informations- und Datenschutzgesetz (IDG) der Kantone sind auf klassische Datenverarbeitung ausgelegt, greifen aber bei komplexen KI-Systemen oft zu kurz (vgl. Kanton Zürich 2024: 7)

Zugleich beherbergt die Schweiz global führende KI-Forschungsstandorte wie in Zürich das ETH AI Center oder die Digital Society Initiative der Universität Zürich. Dieses Potenzial konnte bislang jedoch nur begrenzt wirtschaftlich genutzt werden. Um diese Lücke zu schließen und Innovation gezielter mit regulatorischer Orientierung zu verbinden, initiierte der Kanton Zürich im Jahr 2021 **die Innovation-Sandbox für KI** (vgl. Kanton Zürich 2024: 4).

Ziel war es, einen praxisnahen Rahmen zu schaffen, in dem KI-Anwendungen unter realen Bedingungen, aber unter Einhaltung geltenden Rechts, erprobt werden können – ohne regulatorische Grauzonen oder rechtliche Sonderregelungen. Die Sandbox sollte es Unternehmen, Behörden und Forschungseinrichtungen ermöglichen, **verantwortungsvoll mit neuen KI-Technologien zu experimentieren, gleichzeitig aber regulatorisches Wissen aufzubauen** (vgl. Kanton Zürich 2024: 6 f.).

Das Projekt wurde auch als strategische Antwort auf europäische Entwicklungen verstanden: Mit der europäischen KI-Verordnung entsteht ein verbindlicher Rechtsrahmen für risikobasierte KI-Regulierung in Europa. Auch wenn die Schweiz nicht direkt an die KI-VO gebunden ist, sollten Zürcher Akteure durch die Sandbox frühzeitig an deren Anforderungen herangeführt und die internationale Anschlussfähigkeit der Region gestärkt werden (vgl. Greater Zurich Area 2024).

Rechtlicher Rahmen

Die Innovation-Sandbox Zürich wurde **ohne eine speziell dafür geschaffene gesetzliche Grundlage** (d. h. Reallaborgesetz) eingerichtet. Es existiert in der Schweiz aktuell weder auf Bundesebene noch im Kanton Zürich ein *Reallaborgesetz* oder eine *generelle Experimentierklausel* für KI-Anwendungen. Daher muss die Sandbox vollständig innerhalb des geltenden Rechtsrahmens operieren (vgl. SECO 2022: 16 f.; Volz 2022: 52).

Das heißt: **Rechtliche Ausnahmen oder temporäre Deregulierungen sind nicht möglich**. Stattdessen basiert die Sandbox auf einer *pragmatischen Verwaltungspraxis*, bei der die geltenden Bestimmungen – insbesondere Datenschutzrecht (Bundesgesetz über den Datenschutz, DSG) und fachspezifische Normen – aktiv angewendet und im Rahmen konkreter Projekte interpretiert werden (vgl. BAKOM 2025: 33; Volz 2022: 53).

Zentral dabei ist die enge Einbindung der kantonalen Datenschutzaufsicht und die Anwendung von „Privacy by Design"-Prinzipien, etwa im Smart-City-Projekt zur Parkplatzbewirtschaftung oder bei Übersetzungsdiensten für Behörden (vgl. BAKOM 2025: 34). Für Projekte mit Bundesrechtsbezug (z. B. Luftfahrtrecht beim Drohneneinsatz) sind zusätzliche Klärungen mit den zuständigen Stellen auf Bundesebene erforderlich, formale Ausnahmeregelungen werden jedoch nicht erteilt (vgl. Volz 2022: 54).

Die Sandbox ist somit als realitätsnaher Testrahmen ausgestaltet, der regulatorische Herausforderungen nicht ausgeklammert, sondern innerhalb des bestehenden Rechtsrahmens produktiv bearbeitet. Dies entspricht dem sogenannten *„legal sandboxing within existing law"*, wie es in der Schweiz derzeit möglich ist (vgl. SECO 2022: 22). Gleichzeitig hat diese Ausgestaltung bereits vor Augen geführt, dass der Handlungsspielraum begrenzt ist – insbesondere bei personenbezogenen Daten oder bei sektorübergreifenden KI-Systemen. In der Auslegeordnung des Bundes wird daher diskutiert, ob künftig rechtliche Grundlagen für Sandbox-Formate geschaffen werden sollten (vgl. BAKOM 2025: 33 f.).

Beteiligte Akteure

Die Innovation-Sandbox Zürich wurde als **kooperatives Vorhaben** zwischen öffentlicher Hand, Wissenschaft, Wirtschaft und Zivilgesellschaft konzipiert. Ziel ist es, rechtliche,

technische und gesellschaftliche Perspektiven von Anfang an systematisch zu integrieren (vgl. Kanton Zürich 2024: 6; von Thiessen 2024).

Öffentliche Stellen:

Die Federführung lag bei der **Volkswirtschaftsdirektion des Kantons Zürich**, insbesondere dem *Amt für Wirtschaft und Arbeit*. Dieses koordiniert die Gesamtinitiative und stellt die organisatorische Infrastruktur bereit. Unterstützt wird es von weiteren kantonalen Stellen wie dem **Statistischen Amt**, der **Stabsstelle Digitale Verwaltung** sowie dem **Amt für Wirtschaft des Kantons Schwyz**. Zudem ist die **Metropolitankonferenz Zürich** als regionaler Zusammenschluss von acht Kantonen und Städten maßgeblich beteiligt – sie stellt Mittel und Vernetzungsressourcen zur Verfügung (vgl. BAKOM 2025: 32; Kanton Zürich 2024: 5).

Forschungseinrichtungen:
Die wissenschaftliche Expertise kommt insbesondere vom **ETH AI Center**, der **Digital Society Initiative (DSI)** und dem **Center for Information Technology, Society, and Law (ITSL)** der Universität Zürich. Diese begleiten die Projekte mit rechtlicher, ethischer und technischer Expertise. Auch Fachhochschulen wie die **ZHAW School of Management and Law** und die **Hochschule Luzern** wirken mit (vgl. SECO 2022: 23; Volz 2022: 59).

Unternehmen & Start-ups:

Bisherige Pilotprojekte wurden gemeinsam mit verschiedenen Unternehmen realisiert, u. a.

- **Parquery AG** (Smart City / Computer Vision)
- **Pixmap AG** und **IBM Research Zürich** (Infrastrukturinspektion via Drohne)
- **ANYbotics AG** (Robotik / autonome Systeme)
- **nüüt AG** (Übersetzungstechnologie)

Zudem nahmen mehrere Verwaltungseinheiten als Praxispartner teil, etwa das **Handelsregisteramt Schwyz**, die **Fachstelle Integration** des Kantons Zürich sowie ein Zürcher Schulträger.

Zivilgesellschaft & Multiplikatoren:

Im Sinne eines offenen Innovationsverständnisses werden auch zivilgesellschaftliche Akteure und thematisch relevante Fachpersonen einbezogen – z. B. Datenschutzexpert:innen, Verwaltungspraktiker:innen und Branchenverbände wie **swissICT**. Die Sandbox versteht sich explizit als Lernplattform für alle beteiligten Akteursgruppen.

Gegenstand der Erprobung

In der ersten Phase der Sandbox (2022–2024) wurden fünf konkrete KI-Anwendungsfälle unter realen Bedingungen erprobt, um rechtliche Unsicherheiten sichtbar zu machen und sektorspezifische Handlungsempfehlungen zu entwickeln (vgl. Kanton Zürich 2024: 9 ff.):

- **Smart Parking in Frauenfeld**: Kamerabasiertes KI-System von **Parquery AG** zur anonymen Erkennung freier Parkplätze. **Themen:** Datenschutz, Bildverarbeitung im öffentlichen Raum, kommunale Mobilitätssteuerung.

- **Infrastrukturinspektion via Drohne**: Projekt mit **Pixmap AG** und **IBM Research** zur automatisierten Wartung von Start- und Landebahnen. **Themen:** Luftfahrtrecht, Datenhoheit, Predictive Maintenance.
- **Maschinelle Übersetzung in Behörden**: Gemeinsamer Test durch das **Handelsregisteramt Schwyz** und die **Fachstelle Integration Zürich**. **Themen:** Übersetzungsqualität, Datenschutz, lokales Hosting, Bias-Risiken.
- **KI in der Schule**: Automatisierte Korrektur handschriftlicher Schüleraufgaben im Matheunterricht. **Themen:** Schulrecht, Datenschutz bei Minderjährigen, algorithmische Transparenz.
- **Leitfaden für autonome Systeme**: Mit **ANYbotics AG** und Partnern: Erstellung regulatorischer Orientierungshilfen zu KI-Robotik. **Themen:** Normierung, Schnittstellen zum EU-Recht (KI-VO, Maschinenverordnung).

Diese Use Cases dienten als Grundlage für rechtliche Best Practices und praxisnahe Leitfäden (z. B. zu Datenschutz-Checks oder ethischen Implikationen). Alle Projekte wurden dokumentiert und in Fachveranstaltungen öffentlich reflektiert.

Phase II (2024–2026): thematische Erweiterung und Vertiefung

Auf Basis der positiven Resonanz wurde die Sandbox 2024 in eine zweite Phase überführt. Nach einem öffentlichen Call mit 24 Einreichungen wurden sechs neue Pilotprojekte ausgewählt (vgl. Kanton Zürich 2024: 18; GZA 2024):

- **KI-Assistenzsysteme im Gesundheitswesen**: Fokus auf Diagnoseunterstützung und interaktive Patienteninformation. **Themen:** Gesundheitsdatenschutz, Verantwortungsteilung Mensch-Maschine, Medizintechnikrecht.
- **Automatisierte Prüfung von Baugesuchen**: Einsatz von KI zur Vorabkontrolle von Einreichungen im Bauverfahren. **Themen:** Verwaltungsverfahrensrecht, Transparenzpflichten, Interoperabilität.
- **Deepfake-Erkennung für Behörden und Medienhäuser**: Entwicklung von Tools zur Authentizitätsprüfung digitaler Inhalte. **Themen:** Beweissicherung, Informationsintegrität, Meinungsfreiheit.
- **Ethik-Self-Check für KI-Projekte im öffentlichen Sektor**: Entwicklung eines Online-Tools zur ethischen Selbstevaluation. **Themen:** Fairness, Diskriminierungsrisiken, ethisches Impact Assessment.
- **Assistenzsysteme für Menschen mit Behinderung**: KI-gestützte Kommunikationstechnologien für mehr Barrierefreiheit. **Themen:** Inklusion, technische Standardisierung, soziales Vergaberecht.
- **Automatisierte Textanalyse in der Justiz**: Pilotierung von Natural Language Processing zur Erschließung von Gerichtsurteilen. **Themen:** Justiztransparenz, Rechtsstaatlichkeit, algorithmische Nachvollziehbarkeit.

Diese Projekte befinden sich seit Mitte 2024 in Umsetzung. Sie sollen vertiefte Erkenntnisse zur sektoralen Skalierbarkeit und zur Übertragbarkeit in föderale Verwaltungsstrukturen liefern. Gleichzeitig werden Schnittstellen zur zukünftigen nationalen KI-Governance vorbereitet.

Dauer & Ablauf

Die Sandbox wurde im Jahr **2021** durch einen Beschluss der Volkswirtschaftsdirektion des Kantons Zürich initiiert. Bereits im **März 2022** startete die erste Umsetzungsphase. Der gesamte Ablauf war **modular** angelegt und gliederte sich in zwei aufeinanderfolgende Phasen:

Phase I (2022–2024): Pilotierung & Grundlagenentwicklung

- **Frühjahr 2022:** Projektstart mit Aufbau des Koordinationsteams und der interdisziplinären Steuerungsgruppe.
- **Mai–Juni 2022:** Öffentliche Ausschreibung („Call for Projects“) für erste Pilotvorhaben.
- **Sommer 2022:** Auswahl von fünf Projekten anhand definierter Kriterien (z. B. Reifegrad, Regulierungsrelevanz, gesellschaftlicher Nutzen).
- **Herbst 2022 bis Frühjahr 2024:** Umsetzung der Pilotprojekte durch teilnehmende Organisationen in enger Abstimmung mit dem Sandbox-Team und den Rechtsexpert:innen.
- **Frühjahr 2024:** Veröffentlichung des Abschlussberichts der Phase I (*Play & Learn*, März 2024), inklusive Lessons Learned, Handlungsempfehlungen und Entscheidungsgrundlagen für eine Fortsetzung (vgl. Kanton Zürich 2024: 5–8).

Phase II (2024–2026): Skalierung & Vertiefung

- **April 2024:** Zweiter öffentlicher Projekt-Call, über 20 Bewerbungen.
- **Mai 2024:** Auswahl von sechs neuen Projekten durch das Steuerungsgremium.
- **Sommer 2024 bis Ende 2026:** Umsetzung der Projekte mit verstärkter sektoraler Fokussierung (u. a. Gesundheit, Justiz, Inklusion) und begleitender Dokumentation.
- Ergänzend wurden begleitende **Workshops, Diskussionsrunden und Vernetzungsformate** eingeführt, um Wissenstransfer, sektorübergreifende Reflexion und Vorbereitung auf nationale Regulierungsdiskussionen zu fördern (vgl. Greater Zurich Area 2024; BAKOM 2025: 34).

Bis **Ende 2026** sollen alle Projekte aus Phase II abgeschlossen und evaluiert sein. Auf dieser Basis wird entschieden, ob die Sandbox **dauerhaft institutionalisiert** oder auf Bundesebene weiterentwickelt wird – z. B. als schweizweites Reallabor für KI-Anwendungen.

Finanzierung und Ressourcen

Die Innovation-Sandbox Zürich wird **ausschließlich öffentlich finanziert**, primär durch Mittel der kantonalen Standortförderung sowie Beiträge des regionalen Verbunds der **Metropolitankonferenz Zürich**. Es werden keine konkreten Zahlen zu den Gesamtkosten der Sandbox genannt. Eine direkte Projektförderung für teilnehmende Unternehmen war nicht vorgesehen – die Sandbox stellte stattdessen **Infrastruktur, rechtliche Beratung und Maßnahmen zur Steigerung der Sichtbarkeit** bereit (vgl. Kanton Zürich 2024: 6; GZA 2024).

Finanzielle Trägerschaft:

- Hauptverantwortlich für das Budget ist das **Amt für Wirtschaft des Kantons Zürich**.

- Zusätzliche Mittel kommen vom Metropolitanraum Zürich, der als regionalpolitische Initiative eine Förderung innovationsbezogener Kooperationen verfolgt.
- Die Finanzierung erfolgt **aus dem ordentlichen Standortentwicklungsbudget**, nicht über ein Innovations- oder Forschungsprogramm. Eine Beteiligung des Bundes erfolgte in Phase I nicht (vgl. Kanton Zürich 2024: 7).

Leistungen für Teilnehmer:

- Die Sandbox stellt **juristische Expertise, Vernetzungsangebote und Workshops** zur Verfügung, jedoch **keine monetäre Projektförderung**.
- Die Teilnahme ist **kostenfrei**, aber an die Verpflichtung zur aktiven Kooperation und Ergebnisdokumentation geknüpft.
- Alle Partner müssen ihre eigenen Sachkosten (z. B. Personal, Technologieeinsatz) selbst tragen.

Personelle Ressourcen:

- Ein kleines **Kernteam** (Projektleitung, juristische Beratung, Kommunikation) ist in der Volkswirtschaftsdirektion des Kantons angesiedelt.
- Je nach Projekt werden **Fachexpert:innen temporär eingebunden**, u. a. aus dem ITSL der Universität Zürich oder aus kantonalen Stellen.
- Die operative Projektbegleitung erfolgt durch das Sandbox-Team in Abstimmung mit den Projektträgern und der Steuerungsgruppe.

Phase II (2024–2026):

- In der Fortsetzungsphase wurde ein leicht erhöhtes Budget gewährt, insbesondere zur Bewältigung der zusätzlichen Projektanzahl (6 statt 5) und zur Stärkung von Kommunikation, Ethikberatung und Evaluierung.
- Eine Beteiligung des Bundes oder von EU-Mitteln ist auch in Phase II nicht vorgesehen.
- **Synergien** mit **europäischen Netzwerken** (z. B. AI-on-Demand, AI-Sandbox-Netzwerk der EU-Kommission) sollen dennoch genutzt werden (vgl. BAKOM 2025: 35).

Governance-Modell

Die Innovation-Sandbox Zürich beruht auf einem **mehrstufigen Governance-Modell**. Ziel ist eine **praxisnahe Steuerung**, bei der öffentliche Stellen, Wissenschaft und Wirtschaft **gleichberechtigt** miteinbezogen sind (vgl. Kanton Zürich 2024: 6–8).

Die zentrale Koordination liegt beim **Amt für Wirtschaft und Arbeit des Kantons Zürich**, das die operative Verantwortung trägt und als neutraler Mittler zwischen Verwaltung, Wirtschaft und Forschung fungiert. Unterstützt wird das Projekt durch eine **interdisziplinäre Steuerungsgruppe**, in der alle Trägerinstitutionen vertreten sind – darunter auch der Kanton Schwyz und die Metropolitankonferenz Zürich (vgl. BAKOM 2025: 34).

Die Steuerungsgruppe ist zuständig für:

- Projektselektion (nach definierten Kriterien),
- Fortschrittsbegleitung und Qualitätssicherung,
- Abstimmung rechtlicher Fragen (in Kooperation mit Datenschutzaufsicht),
- strategische Weiterentwicklung der Sandbox.

Jedes Pilotprojekt wird durch das Kernteam der Sandbox **individuell begleitet**, um technologische Fragestellungen mit **regulatorischer Orientierung** zu verbinden. Je nach Bedarf werden **externe Expert:innen** miteingebunden – u. a. aus dem *Center for Information Technology, Society, and Law (ITSL)* der Universität Zürich oder aus spezialisierten kantonalen Fachstellen (z. B. Datenschutzaufsicht, Schulaufsicht). Diese integrierte Fachberatung stellt sicher, dass alle Sandbox-Projekte **rechtskonform, nachvollziehbar und ethisch reflektiert** umgesetzt werden.

Die Sandbox ist als Multi-Stakeholder-Kooperation organisiert und folgt einem *Co-Creation-Modell*, in das Forschungseinrichtungen, Unternehmen und Start-ups dauerhaft miteingebunden sind. Dabei steht das gemeinsame Lernen an realen Fällen im Vordergrund, und man folgt keinem strengen Top-down-Ansatz in der Umsetzung.

Die Sandbox legt großen Wert auf **offene Kommunikation**: Projektfortschritte, Herausforderungen und Lessons Learned wurden regelmäßig publiziert und über Veranstaltungen, Medienberichte und Online-Kanäle zugänglich gemacht – mit dem Ziel, regulatorisches Lernen **nicht nur intern**, sondern im gesamten Innovationsökosystem zu verankern (vgl. SECO 2022: 24; von Thiessen 2024).

Mit dem Übergang in **Phase II (2024–2026)** wurde das Governance-Modell gestärkt – etwa durch:

- themenspezifische Fachgruppen (z. B. zu Ethik, Recht, Inklusion),
- strukturierte Austauschformate mit Bundesstellen,
- Vorbereitung einer potenziellen Institutionalisierung (z. B. als dauerhaftes KI-Reallabor auf kantonaler oder regionaler Ebene).

Evaluations- und Skalierungsstrategie

Die Sandbox wurde von Beginn an als **Lernumgebung** konzipiert, um vertrauenswürdige KI-Anwendungen zu fördern und verwertbare Erkenntnisse für künftige gesetzgeberische Entscheidungen zu generieren (vgl. Kanton Zürich 2024: 18 f.; SECO 2022: 22).

1) Evaluation auf Projektebene

Zum Monitoring und zur Evaluation müssen im Rahmen jedes bewilligten Projekts die Ergebnisse dokumentiert werden, u. a. in Form von:

- rechtlichen Einschätzungen (z. B. Datenschutz, Zuständigkeiten),
- Lessons-Learned-Berichten,
- konkreten Handlungsempfehlungen oder Leitfäden,

- öffentlich zugänglichen Prototypen oder Methodenpapieren.

Diese Ergebnisse werden auf der Projektwebsite veröffentlicht, in Fachveranstaltungen präsentiert und gezielt für Behörden, Unternehmen und Forschungspartner aufbereitet (vgl. Kanton Zürich 2024: 20).

2) Evaluation auf Programmebene

Nach der ersten Projektphase wurde die Sandbox evaluiert. Dabei standen folgende Evaluierungsfragen im Vordergrund:

- Erreichte die Sandbox die richtigen Zielgruppen?
- Konnten regulatorische Unsicherheiten verringert werden?
- Welche Formate funktionierten für Wissensaufbau und Governance?

Die Ergebnisse wurden in einem **Abschlussbericht für Phase I** gebündelt und bildeten die Entscheidungsgrundlage für die Planung und Umsetzung von Phase II (vgl. Kanton Zürich 2024: 5 ff.). Sichtbare Erfolge waren u. a.:

- eine wachsende Zahl qualitativ hochwertiger Projekteinreichungen,
- Nutzung der Sandbox-Leitfäden durch weitere Kantone,
- positive Rückmeldungen von KMU, die durch die Sandbox regulatorisches Know-how aufbauen konnten.

3) Skalierungsstrategie (Phase II & darüber hinaus)

Phase II (2024–2026) dient nicht nur der thematischen Vertiefung, sondern auch der Vorbereitung einer möglichen **institutionellen Verstetigung**:

- Entwicklung dauerhafter Prüf- und Beratungsstrukturen für KI-Projekte,
- Etablierung eines öffentlich finanzierten, interkantonalen Reallabors,
- Ausbau des Netzwerks mit Bundesstellen und europäischen Partnern,
- Übertragung des Sandbox-Prinzips auf weitere Anwendungsfelder (z. B. Energie, Justiz, Gesundheit).

Die Skalierung erfolgt dabei nicht primär aufgrund einer Budgetvergrößerung, sondern über **Wissenstransfer, Kooperation und strukturelle Verankerung**. Die gewonnenen Erkenntnisse werden aktiv in nationale Debatten eingespeist – etwa in die BAKOM-Auslegeordnung zur KI-Regulierung oder in die Diskussion um ein Schweizer Pendant zur europäischen KI-Verordnung (vgl. BAKOM 2025: 35).

Ergebnisse / Lessons Learned

Die Innovation-Sandbox Zürich hat in ihrer ersten Phase (2022–2024) zentrale Erkenntnisse zum Zusammenspiel von Technologieentwicklung, Regulierung und öffentlicher Verwaltung hervorgebracht. Die folgenden Lessons Learned gelten als richtungsweisend für vergleichbare Vorhaben in der Schweiz und international (vgl. Kanton Zürich 2024: 18 ff.; SECO 2022: 24):

1. **Die Operationalisierung von Regulatory Sandboxes ist auch innerhalb des bestehenden Rechtsrahmens möglich. Auch dabei bleibt regulatorisches Lernen nicht aus:** Trotz fehlender Experimentierklausel konnten KI-Projekte in sensiblen Feldern wie Mobilität, Bildung oder Verwaltung rechtskonform umgesetzt werden – durch frühzeitige rechtliche Beratung, „Privacy by Design"-Ansätze und behördenübergreifende Abstimmung. Regulierung erwies sich nicht als Innovationsbremse, sondern als strukturierender Rahmen für die Entwicklung von innovativen, vertrauenswürdigen KI Lösungen (vgl. BAKOM 2025: 34).
2. **Verwaltende Stelle als Intermediär im Innovationsökosystem:** Transaktionskosten und Zutrittsbarrieren für beteiligte Unternehmen niedrig halten, Informationen zur Verfügung stellen und Kommunikation mit Behörden.
3. **Co-Kreation erhöht Akzeptanz und Umsetzbarkeit**
   Die enge Zusammenarbeit von Entwickler:innen, Anwender:innen, Behörden und Jurist:innen führte zu höherer Akzeptanz der Ergebnisse und zu praxistauglichen Empfehlungen. Die partizipative Governance bewährte sich besonders bei sensiblen Themen wie Kinder- und Bildungsdaten oder autonomen Systemen in der Industrie.
4. **Eine breite Einbindung von unterschiedlichen Fachkompetenzen schafft positive Synergieeffekte, erfordert aber Koordination**
   Die breite Einbindung unterschiedlicher Fachkompetenzen in eine Regulatory Sandbox ermöglicht einen systemischen Blick auf KI und Regulierung. Gleichzeitig wird dadurch deutlich, dass Projektvorhaben klare Zuständigkeiten und eine stabile Koordination benötigen, um effektiv umgesetzt werden zu können – z. B. bei der Abstimmung zwischen Datenschutz-, Schul- und Verwaltungsrecht.
5. **Bedarf an struktureller Verstetigung wächst**
   Behörden und Unternehmen signalisierten, dass punktuelle Sandbox-Projekte wertvoll sind – aber langfristig eine **institutionalisierte, zugängliche Testumgebung** mit klaren Prozessen, Beratungsangeboten und Evaluationsstandards nötig wäre. Die Sandbox wurde deshalb in Phase II weiterentwickelt und für mögliche dauerhafte Strukturen vorbereitet.
6. **Übertragbarkeit auf nationale oder europäische Regulierung**
   Mehrere Leitfäden und Empfehlungen aus der Sandbox flossen in nationale Strategieprozesse ein (z. B. BAKOM-Auslegeordnung). Gleichzeitig wurden Schnittstellen zur europäischen KI-Verordnung identifiziert, etwa bei der Entwicklung eines Leitfadens zur Klassifizierung autonomer Systeme im Kontext der europäischen Hochrisiko-Kategorisierung.
7. **Wettbewerbsverzerrungen durch Transparenz im Outcome und open-access bzgl. der Erkenntnisse bzw. Exit-Reports verhindern**
   Nur unter dieser Voraussetzung ist es zulässig, dass der Staat selektiv mit einzelnen Unternehmen in einer Sandbox kooperiert (Ausnahme: Top-secret-Bereiche).

Relevanz für Österreich

Die Innovation-Sandbox Zürich liefert ein erprobtes, anschlussfähiges Modell für den österreichischen Kontext – insbesondere im Hinblick auf die Umsetzung einer praxisnahen, regional verankerten KI-Sandbox

Regulatory Sandbox ist auch innerhalb des bestehenden Rechtsrahmens möglich

Die Zürcher Sandbox zeigt, dass auch ohne Reallaborgesetz oder Experimentierklausel eine rechtssichere Erprobung komplexer KI-Systeme möglich ist – durch gezielte Governance, klare Use Cases und frühzeitige rechtliche Begleitung. Für Österreich bedeutet das: Es braucht nicht zwingend eine gesetzliche Reform, um erste Piloten umzusetzen – sondern eine gut gesteuerte, regulierungskompatible Teststruktur mit klaren Rollen, Zuständigkeiten und Vertrauensmechanismen (z. B. Einbindung der Datenschutzbehörde, sektorale Rechtsberatung).

Regionalisierung als Stärke – föderale Anschlussfähigkeit nutzen
Die Sandbox war kantonal getragen, aber interkantonal vernetzt – ein Modell, das gut auf die föderale Struktur Österreichs übertragbar ist. Anstatt auf eine zentrale Sandbox hinzuarbeiten, könnte Österreich eine **mehrstufige Architektur** entwickeln: Ein national koordinierter Rahmen (z. B. über BMDW, BMIMI oder FFG), ergänzt durch regionale Pilot-Sandboxes – etwa in Wien (Digitale Verwaltung), Oberösterreich (Industrie-KI), Steiermark (Mobilität) oder Salzburg (Gesundheit). Die Zürcher Erfahrung zeigt: Lokale Nähe zu Verwaltungen, Hochschulen und KMU erhöht die Relevanz und Umsetzbarkeit deutlich.

Fokus auf Public-Interest-KI und sektorübergreifende Anwendungen
Die Zürcher Sandbox adressierte gezielt Sektoren mit **gesellschaftlichem Nutzen** – Mobilität, Bildung, Verwaltung, Infrastruktur. Für Österreich wäre ein ähnlicher Fokus strategisch sinnvoll, etwa im Kontext von „Public Interest AI“: KI zur Vereinfachung behördlicher Verfahren, zur Förderung von Barrierefreiheit oder zur Unterstützung von Schulen. Gerade im öffentlichen Sektor lassen sich regulatorische Herausforderungen gut systematisch bearbeiten – mit Beteiligung von Ministerien, Gemeinden und Plattformen wie GovTech4Impact oder Open Commons Linz.

Methodisch übertragbar: Co-Kreation, Leitfäden, regulatorisches Lernen

Besonders relevant für Österreich ist der methodische Ansatz: Co-Kreation statt Top-down, frühzeitige Klärung rechtlicher Fragen im Dialog zwischen Entwickler:innen und Behörden, und Veröffentlichung verwertbarer Ergebnisse (z. B. Datenschutz-Leitfäden, interaktive Werkzeuge). Diese Form von „regulatorischem Lernen“ ist für österreichische KMU zentral – besonders im Hinblick auf neue Anforderungen durch KI-Regulierung und Compliance. Eine österreichische Sandbox könnte hier gezielt Schulungs- und Begleitangebote integrieren – etwa über Wirtschaftskammern oder Fachverbände.

Impuls für strategische Governance und langfristige Strukturen

Die Zürcher Sandbox zeigt auch, dass eine Sandbox nicht nur als Projekt, sondern als **strategisches Steuerungsinstrument** verstanden werden kann – um sektorale Expertise zu bündeln, Lernprozesse auf kantonaler Ebene zu ermöglichen und Schnittstellen zwischen Innovation und Recht dauerhaft zu verankern. Für Österreich ergibt sich daraus die Option, mit einer ersten, schlank angelegten Sandbox zu starten – diese aber von Anfang an mit Blick auf eine spätere Institutionalisierung zu konzipieren. Die Rolle einer zentralen Koordinierungsstelle (z. B. bei der FFG oder einer künftigen KI-Aufsichtsstruktur) sollte dabei früh geklärt werden.

Referenzen

BAKOM – Bundesamt für Kommunikation (2025): Auslegeordnung zur Regulierung von künstlicher Intelligenz. Bericht an den Bundesrat vom 12.02.2025. Bern.

Greater Zurich Area (2024): AI sandbox for Greater Zurich area has a positive impact. News-Meldung vom 10.09.2024. Online verfügbar unter: https://www.greaterzuricharea.com/en/news/ai-sandbox-for-greater-zurich-area-has-a-positive-impact [abgerufen am 12.07.2025].

Kanton Zürich – Amt für Wirtschaft und Arbeit (2024): Play & Learn. Abschlussbericht zur Innovation-Sandbox für Künstliche Intelligenz. Phase I (2022–2024). Zürich. Online verfügbar unter: https://www.innovationsandbox.ai [abgerufen am 12.07.2025].

SECO – Staatssekretariat für Wirtschaft (2022): Prüfauftrag zu Regulatory Sandboxes. Grundlagenbericht der Wirtschaftspolitik. Nr. 35. Bern.

Volz, Sebastian (2022): KI-Sandboxen für die Schweiz? In: Schweizerische Zeitschrift für Wirtschaftsrecht (SZW), 1/2022, S. 51–68.

von Thiessen, Raphael (2024): Projektpräsentation zur Innovation-Sandbox Zürich. Vortrag im Rahmen der Metropolitankonferenz Zürich, März 2024 (unveröffentlichtes Präsentationsmaterial, zitiert mit Genehmigung).

14.3 REALLABOR AI4U

Land / Region

Deutschland – Baden-Württemberg, Schwerpunktregion: Rhein-Neckar (Mannheim, Reutlingen, Ulm)

Sektor / Branche

Das Reallabor „AI4U – Künstliche Intelligenz für digitale personalisierte Gesundheitsförderung" ist sektorspezifisch ausgerichtet und fokussiert auf das **Gesundheitswesen**, insbesondere den Bereich der **psychischen Gesundheit** bei Jugendlichen und jungen Erwachsenen. Es wird vom **Zentralinstitut für Seelische Gesundheit Mannheim** getragen und durch das **Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg** gefördert.

Zentrale Anwendungsbereiche sind:

- digitale Prävention psychischer Erkrankungen (z. B. depressive Störungen, Angst),
- mobile, KI-gestützte Gesundheitsanwendungen (z. B. via Smartphone-Sensorik),
- personalisierte Interventionssysteme auf Basis verhaltensbasierter Datenauswertung,
- niederschwellige, datenschutzkonforme Tools zur Früherkennung und Selbsthilfe.

Die Sandbox zielt auf eine sektorspezifische Öffnung des Gesundheitsbereichs für digitale KI-Innovationen, die hohe Anforderungen an ethische, rechtliche und technische Standards stellen. Sie spricht insbesondere:

- Start-ups im Bereich Mental Health Tech,
- Forschungseinrichtungen mit anwendungsnaher Digital-Health-Expertise,
- Krankenkassen und Versorgungsträger mit Innovationsinteresse im Bereich Prävention an.

Der sektorale Fokus auf psychische Gesundheit reflektiert eine politische Priorität Baden-Württembergs im Bereich Gesundheitsstandortentwicklung und wird im Rahmen des Forums Gesundheitsstandort BW strategisch begleitet.

Ausgangssituation

Psychische Erkrankungen zählen zu den häufigsten Gesundheitsproblemen bei Jugendlichen und jungen Erwachsenen. Bereits vor der COVID-19-Pandemie berichtete etwa jede:r fünfte Jugendliche in Deutschland von depressiven Symptomen oder stressbedingten Beschwerden. Trotz zunehmender Nachfrage fehlt es an niedrigschwelligen, wirksamen und personalisierten Präventions- und Interventionsformaten, die jugendliche Lebenswelten direkt adressieren.

Ein zentrales Innovationshemmnis besteht im Mangel an evidenzbasierten digitalen Tools, die nicht nur informierend oder standardisierend wirken, sondern individualisierte Unterstützung leisten. Der Einsatz von **KI** in diesem Bereich gilt als vielversprechend, wirft jedoch **ethische, datenschutzrechtliche und gesellschaftliche Fragestellungen** auf, insbesondere beim Einsatz im sensiblen Feld psychischer Gesundheit. Viele bestehende mHealth-Anwendungen

sind intransparente „Black Boxes“, selten partizipativ entwickelt, und bieten keine adaptive, alltagsintegrierte Nutzung (Baumeister et al., 2020). Die zielgerichtete Integration von KI in digitaler Gesundheitsförderung steht daher noch ganz am Anfang – vor allem für vulnerable Gruppen wie Jugendliche. Es besteht momentan ein Mangel an datensensiblen, ethisch verantworteten und partizipativ entwickelten KI-Lösungen zur personalisierten Förderung psychischer Gesundheit bei Jugendlichen. Gleichzeitig herrscht regulatorische Unsicherheit hinsichtlich der Anwendung von KI im Gesundheitsbereich, insbesondere in Bezug auf Datenschutz, Einwilligung und Transparenz.

Das zentrale Innovationsziel von AI4U bestand daher darin, ein datenschutzkonformes, anwendungsnahes und wissenschaftlich evaluiertes digitales System zu entwickeln, das:

- Stimmungen kontinuierlich und niederschwellig erfasst (ökopsychologisches „Mood Tracking“),
- individuelle Mikrointerventionen über KI-generierte Feedbackschleifen anbietet, und
- in einem partizipativen Reallaborrahmen mit Jugendlichen und psychosozialen Praxispartnern entwickelt und getestet wird.

Diese Zielstellung ist eng eingebettet in die Digitalisierungsstrategie des Landes Baden-Württemberg. Seit 2015 unterstützt das Ministerium für Wissenschaft, Forschung und Kunst gezielt Reallabore als Orte des wissenschaftlich fundierten und gesellschaftlich rückgekoppelten Experiments. Mit AI4U wird diese Strategie erstmals im Feld der **psychischen Gesundheitsförderung mit KI-Fokus** operationalisiert – als Pilotvorhaben, das technologische Innovation mit sozialer Verantwortung verbindet (MWK BW, 2021; Abu-Omar et al., 2023).

Rechtlicher Rahmen

Das Reallabor **AI4U** operiert im rechtlichen Rahmen der allgemeinen Gesetzgebung zur Digitalisierung und Gesundheitsforschung in Deutschland und Baden-Württemberg. Eine formalisierte **Experimentierklausel** im engeren Sinn (wie etwa in der Verkehrstechnik oder Umweltgesetzgebung) existiert für das Vorhaben nicht. Dennoch nutzt AI4U gezielt die **regulatorischen Spielräume**, die sich insbesondere aus der Datenschutz-Grundverordnung (DSGVO), dem Landesdatenschutzgesetz Baden-Württemberg sowie forschungsethischen Standards ergeben.

Datenschutzrechtlicher Rahmen

AI4U arbeitet mit besonders sensiblen personenbezogenen Daten, namentlich **Gesundheits- und Verhaltensdaten** von Jugendlichen. Entsprechend unterliegt das Projekt den strengen Anforderungen aus:

- **Art. 9 DSGVO** (Verarbeitung besonderer Kategorien personenbezogener Daten),
- **§§ 12–22 LDSG BW** (Datenverarbeitung im öffentlichen Auftrag),
- sowie ethischen Standards für medizinische Forschung (z. B. Deklaration von Helsinki).

Ein Schwerpunkt ist die **rechtskonforme Gestaltung von Einwilligungsprozessen** für Minderjährige. Dies wird in AI4U durch altersgerechte Informationsmaterialien, transparente Nutzungserklärungen und durch den Einbezug von Erziehungsberechtigten umgesetzt.

KI-spezifische Regulierung

Zum Projektstart 2021 existierte kein spezifisches Regelwerk zur Regulierung von künstlicher Intelligenz im Gesundheitswesen. AI4U antizipiert jedoch zentrale Anforderungen aus der (2024 in Kraft getretenen) **europäischen KI-Verordnung**, darunter:

- Anforderungen an **transparente, nachvollziehbare Algorithmen** (Art. 13–15 KI-VO),
- Dokumentationspflichten für **risikobehaftete Systeme**,
- und Vorgaben zu **Forschungsausnahmen**, die künftig auch als rechtliche Grundlage für Reallabore fungieren könnten.

In Baden-Württemberg ist vorgesehen, Erkenntnisse aus Projekten wie AI4U **für regulatorisches Lernen** zu nutzen (vgl. Landtag BW, 2024, Drucksache 17/7537). AI4U erfüllt damit eine indirekte Rolle als Regulatory Sandbox im Sinne des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK), auch wenn kein sektorales Reallaborgesetz vorliegt.

Förder- und Strukturrecht

Die rechtliche Ermöglichung von AI4U basiert auf der institutionellen Förderkompetenz des **Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK)**. Grundlage ist die dort verankerte Reallabor-Strategie zur Digitalisierung und nachhaltigen Entwicklung (MWK BW, 2021). Die Förderung erfolgte auf Projektbasis ohne spezielle regulatorische Ausnahmeregelung, jedoch mit:

- ethischer Begleitforschung,
- interdisziplinärer Projektsteuerung,
- sowie Zustimmung der jeweils zuständigen Datenschutzbeauftragten.

Beteiligte Akteure

AI4U ist ein interdisziplinär angelegtes Kooperationsprojekt, das wissenschaftliche, zivilgesellschaftliche und praxisnahe Akteure aus Bildung, Gesundheit und Technologie vereint. Ziel ist die gemeinschaftliche Entwicklung und Evaluation einer KI-gestützten Anwendung zur Förderung psychischer Gesundheit bei Jugendlichen. Die Beteiligung erfolgt auf mehreren Ebenen: in der Forschung, der praktischen Implementierung, der Technologieentwicklung sowie im Transfer in pädagogische Kontexte.

Öffentliche und fördernde Stellen

- **Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK)**
  Förderinstitution des Projekts im Rahmen der Digitalisierungsstrategie des Landes; zuständig für Reallaborpolitik, Forschung und Wissenschaftstransfer.
- **Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL)**
  Integration in bildungspolitische Rahmenbedingungen, Unterstützung bei Dissemination und schulischer Anbindung.

Wissenschaftliche Trägerinstitutionen

- **Zentralinstitut für Seelische Gesundheit (ZI) Mannheim**
  Hauptverantwortlich für die Projektkoordination und psychologische Expertise. Zuständig für die theoretisch-konzeptionelle Fundierung, empirische Erhebung sowie die Implementierung der Anwendung.
- **Universität Ulm – Institut für Psychologie und Pädagogik (AG Qualitative Sozialforschung)**
  Begleitet das Projekt methodisch mit qualitativer Forschung, insbesondere im Bereich partizipativer Co-Design-Prozesse und Evaluationsdesigns.
- **Hochschule Reutlingen**
  Beteiligt an der technischen Entwicklung der App sowie an Fragen der nutzerzentrierten Gestaltung und digitalen Didaktik.

Zivilgesellschaftliche und pädagogische Partner

- **Jugendstiftung Baden-Württemberg**
  Bindeglied zwischen Forschung und jugendlicher Lebenswelt. Verantwortlich für Zielgruppenkommunikation, partizipative Entwicklung und Zugänge zu Schulen und Einrichtungen.
- **War Child Deutschland gGmbH**
  Expertise in psychosozialer Jugendarbeit und traumasensibler Methodik. Beteiligung an der Entwicklung sicherer und niedrigschwelliger Interaktionsformate.
- **Dachverband der Jugendgemeinderäte Baden-Württemberg**
  Beteiligung von Jugendvertretungen an der Konzeptentwicklung und Feedbackprozessen.
- **Landesarbeitsgemeinschaft für Erziehungsberatung BW & Bundesarbeitsgemeinschaft für Erziehungsberatung (bke)**
  Fachexpertise zur Einbindung der App in bestehende Beratungssettings.
- **Netzwerk Schulsozialarbeit BW**
  Umsetzung und Pilotierung im schulischen Feld. Unterstützung bei Zugängen zur Zielgruppe im Alltag.

Technologische Partner

- **movisens GmbH (Karlsruhe)**
  Entwicklung von Sensoriklösungen und Echtzeit-Monitoring. Technologischer Partner zur datenbasierten Erhebung und KI-gestützten Intervention.

Wissenschaftsmanagement und Ethik

- Interne Projektsteuerung durch die beteiligten Hochschulen
- Ethikberatung durch projektinterne Gremien und institutionelle Ethikkommissionen (ZI, Universität Ulm)
- Datenschutzkoordination in Abstimmung mit den jeweiligen Landesdatenschutzstellen

Gegenstand der Erprobung

Das Reallabor **AI4U** verfolgt das Ziel, eine KI-gestützte digitale Intervention zur Förderung psychischer Gesundheit bei Jugendlichen zu entwickeln, unter realen Bedingungen zu testen und wissenschaftlich zu evaluieren. Die Erprobung erfolgt in einem partizipativen, transdisziplinären Rahmen und adressiert sowohl technologische als auch pädagogisch-psychosoziale Innovationsfragen. Im Zentrum steht die Co-Entwicklung einer mHealth-Anwendung, die individuelle Stimmungsverläufe erfasst, auswertet und in Echtzeit mit passgenauen Interventionen reagiert.

Technologischer Innovationskern

- Entwicklung einer **KI-basierten App**, die kontinuierliches **Stimmungstracking** (Ecological Momentary Assessment) ermöglicht.
- Verwendung von **Sensoriklösungen** (z. B. durch Partner movisens GmbH) zur Erhebung von Verhaltens- und Kontextdaten (z. B. Aktivitätslevel, Tageszeit, Umgebungsparameter).
- Anwendung eines lernenden Algorithmus zur **personalisieren Auswahl von Mikrointerventionen**, z. B. Atemübungen, Reflexionsimpulse, Entspannungsangebote.
- Gestaltung eines **datenschutzkonformen, transparenten Feedbacksystems** unter Beachtung der Vorgaben der europäischen KI-Verordnung und der DSGVO.

Psychosozialer und partizipativer Fokus

- Durchführung von **Co-Design-Workshops mit Jugendlichen** zur Bedarfserhebung, Zieldefinition, Formatentwicklung und Prototypentestung.
- Einbindung schulischer, psychosozialer und jugendpolitischer Akteur:innen (z. B. Schulsozialarbeit, Jugendgemeinderäte, Erziehungsberatung) in die Entwicklung und Erprobung.
- Fokus auf **Barrierefreiheit, Niedrigschwelligkeit und Alltagstauglichkeit** der Anwendung in unterschiedlichen Lebenskontexten (z. B. Schule, Familie, Freizeit).

Ethik- und Regulierungsfragen

- Untersuchung der **Grenzen und Potenziale von KI im Bereich präventiver Gesundheitsinterventionen** mit besonderem Augenmerk auf Autonomie, Transparenz und potenzielle Stigmatisierung.
- Aufbau eines projektinternen **Ethik- und Datenschutzmonitorings**, das Rückkopplungsschleifen mit Praxisakteur:innen und Betroffenen vorsieht.
- Wissenschaftliche Begleitung durch qualitative und quantitative Methoden zur Bewertung von Akzeptanz, Wirksamkeit und regulatorischer Anschlussfähigkeit.

Realexperiment und Transfer

- Testbetrieb der Anwendung in verschiedenen realen Settings (z. B. Schulen, Jugendzentren, Onlineplattformen).

- Entwicklung von modularen Nutzungsszenarien für verschiedene Zielgruppen und pädagogische Kontexte.
- Vorbereitung der **Skalierbarkeit und Übertragbarkeit**, auch im Hinblick auf regulatorische Herausforderungen und langfristige Implementierungsmöglichkeiten im Rahmen digitaler Versorgungsstrukturen.

Dauer & Ablauf

Das Reallabor **AI4U** wurde als ein auf dreieinhalb Jahre angelegtes Forschungs- und Entwicklungsprojekt konzipiert. Die Projektlaufzeit erstreckt sich von **Januar 2021 bis Juni 2024**. Der Ablauf gliedert sich in mehrere Phasen, die iterativ aufgebaut und jeweils wissenschaftlich begleitet wurden.

Projektstruktur in vier Phasen

Phase	Zeitraum	Inhalte und Maßnahmen
I	Q1–Q3 2021	*Vorbereitungsphase:* Literatur- und Bedarfsanalyse, Expert:innen-Interviews, juristische und ethische Prüfung
II	Q4 2021 – Q2 2022	*Co-Design-Phase:* Fokusgruppen mit Jugendlichen, Workshops mit Praxisakteur:innen, erste Mock-Ups
III	Q3 2022 – Q2 2023	*Entwicklung & Testung:* App-Prototyping, technische Implementierung, Pilotversuche in Bildungseinrichtungen
IV	Q3 2023 – Q2 2024	*Evaluation & Transfer:* Wirksamkeitsstudien, Dissemination, Transferstrategie, Skalierungsszenarien

Besondere Merkmale des Projektablaufs

- **Iteratives Vorgehen:** Die Entwicklung erfolgte zirkulär – mit Feedbackschleifen zwischen Technologie, Zielgruppe und psychosozialer Praxis.
- **Praxisintegration:** Reallaborsettings wurden bewusst in reale Alltagssituationen von Jugendlichen eingebettet (z. B. Schulsozialarbeit, außerschulische Bildung).
- **Flexibilisierung durch Pandemiebedingungen:** Aufgrund von COVID-19-bedingten Einschränkungen erfolgten Teile der Entwicklung und Evaluation digital bzw. hybrid.
- **Projektbegleitende Reflexion:** Durch qualitative Begleitforschung wurde der Ablauf kontinuierlich dokumentiert, reflektiert und angepasst.

Finanzierung und Ressourcen

Die Finanzierung des Reallabors **AI4U** erfolgte im Rahmen der Reallaborförderlinie des **Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK)**. Die Zuwendung wurde im Kontext der Digitalisierungsstrategie des Landes bewilligt, mit dem Ziel, nachhaltige Forschungs- und Innovationsformate an der Schnittstelle zwischen Wissenschaft, Gesellschaft und Technologie zu ermöglichen.

Öffentliche Projektförderung

- **Fördersumme**: ca. **800.000 EUR**
- **Förderzeitraum**: Januar 2021 bis Juni 2024
- **Förderinstitution**: MWK Baden-Württemberg
- **Rechtsgrundlage**: Forschungsförderung im Sinne von § 44 LHO BW, ohne spezielle gesetzliche Experimentierklausel

Die Landesförderung wurde in vollem Umfang für Forschungs-, Entwicklungs- und Beteiligungskosten bereitgestellt. Dazu zählten Personalstellen, Technikentwicklung, empirische Erhebungen, Projektmanagement sowie Disseminationsmaßnahmen.

Genutzte Ressourcen und Unterstützungsstrukturen

Ressourcentyp	Konkrete Nutzung im Projektkontext
Wissenschaftliches Personal	Projektstellen an ZI Mannheim, Universität Ulm, Hochschule Reutlingen
Infrastrukturen	Forschungsräume, Server und App-Testumgebungen an beteiligten Hochschulen und Partnerinstitutionen
Technologieressourcen	Kooperation mit **movisens GmbH** für mobile Sensorik und App-basierte Datenerhebung
Ethik- und Datenschutz	Nutzung institutioneller Ethikkommissionen, juristischer Beratung durch Datenschutzaufsicht
Zivilgesellschaftliches Netzwerk	Bereitstellung von Zugängen zu Zielgruppen durch Partner wie Jugendstiftung BW, War Child, Schulsozialarbeit BW
Disseminationsressourcen	Öffentlichkeitsarbeit über Social Media, Workshops, Fortbildungen, Online-Plattformen

Besonderheiten der Mittelverwendung

- Die Mittel wurden projektbezogen, nicht institutionell gebunden, und in Verantwortung der Projektkoordination (ZI Mannheim) verwaltet.

- Die Projektförderung enthielt keine Kapitalisierung von Produkten oder wirtschaftliche Verwertungspflichten. Ziel war die Entwicklung eines frei nutzbaren, gemeinwohlorientierten digitalen Instruments.
- Die Mittelverwendung erfolgte im Einklang mit den Reallabor-Prinzipien: transdisziplinär, partizipativ, prozessoffen und wissensgenerierend.

Governance-Modell

Das Reallabor **AI4U** wurde als kooperatives, wissenschaftsgeleitetes und transdisziplinäres Projekt konzipiert, dessen Governance-Struktur bewusst auf **partizipative Steuerung**, **ethische Überprüfung** und **transparente Koordination** ausgelegt ist. Die Steuerungsarchitektur zielt darauf, sowohl die regulatorischen als auch die ethisch-gesellschaftlichen Anforderungen im Bereich künstlicher Intelligenz (KI) und psychischer Gesundheit zu adressieren – unter Berücksichtigung der hohen datenschutzrechtlichen Sensibilität des Feldes.

Projektkoordination und Managementstruktur

- **Federführung und Projektleitung:** Zentralinstitut für Seelische Gesundheit (ZI Mannheim)
- **Forschungskoordination:** Universität Ulm, AG Qualitative Sozialforschung
- **Technikkoordination:** Hochschule Reutlingen und movisens GmbH
- Das operative Projektmanagement lag beim ZI Mannheim, das sowohl Budgetverwaltung als auch Kommunikationsprozesse zwischen den Partnerinstitutionen koordinierte.

Gremienstruktur und partizipative Einbindung

- **Projektbeirat:** Zusammensetzung aus Expert:innen aus Psychologie, Bildung, Datenschutz und Digital Health; beratende Funktion bei ethischen, methodischen und konzeptionellen Fragestellungen.
- **Jugendliche Beteiligung:** Aktive Einbindung jugendlicher Zielgruppen über Workshops, Fokusgruppen und Feedbackphasen (Co-Design-Ansatz).
- **Facharbeitskreise:** Temporäre Einheiten zur Begleitung von Pilotphasen, bestehend aus Partnern aus Schulsozialarbeit, Erziehungsberatung, Jugendpolitik und Medizininformatik.

Ethik und Datenschutz

- **Ethikprüfung:** Über die institutionellen Ethikkommissionen des ZI Mannheim und der Universität Ulm
- **Datenschutzaufsicht:** Interne datenschutzrechtliche Beratung; Kontakt zur Landesdatenschutzbehörde Baden-Württemberg im Rahmen der Konzeption
- **Verarbeitungsprinzipien:** „Privacy by Design“, „Privacy by Default“, altersgerechte Einwilligungsprozesse, explizite Pseudonymisierung von Gesundheitsdaten

Kommunikation und Feedbacksysteme

- **Regelmäßige Jour Fixe:** Monatliche digitale Treffen des Kernteams zur Synchronisierung von Forschungs-, Technik- und Disseminationssträngen
- **Qualitative Reflexionsrunden** mit Praxisakteur:innen zur kontinuierlichen Adaption der Anwendung
- **Dokumentation:** Fortschritt und Anpassungen wurden in einem Living Document festgehalten, das als internes Wissensmanagement-Instrument diente.

Evaluations- und Skalierungsstrategie

Das Reallabor **AI4U** wurde von Beginn an als wissenschaftlich begleiteter Erprobungsraum konzipiert. Die Evaluation diente dabei nicht nur der Wirkungsmessung im engeren Sinne, sondern erfüllte drei zentrale Funktionen:

1. **Wirkungsevaluation:** Nachweis von Akzeptanz, Effektivität und Nutzung der digitalen Intervention.
2. **Lernbegleitung:** Reflexive Analyse und Rückkopplung im Entwicklungsprozess (formative Evaluation).
3. **Regulatorisches Lernen:** Ableitung von Anforderungen und Grenzen für zukünftige Implementierungen von KI im Gesundheitskontext.

Die Evaluation folgte einem **Mixed-Methods-Ansatz**, um sowohl quantitativ belastbare als auch qualitativ tiefenanalytische Erkenntnisse zu generieren. Besonders hervorgehoben wurde die partizipative Evaluation durch die Einbindung jugendlicher Nutzer:innen in Feedback- und Validierungsprozesse.

Skalierungsperspektiven

AI4U ist als skalierbares Modell angelegt. Die Übertragbarkeit betrifft mehrere Ebenen:

- **Geografisch:** Ausdehnung auf weitere Regionen in Baden-Württemberg, v. a. ländliche Räume mit Versorgungsengpässen
- **Institutionell:** Einbettung in schulische Strukturen, Jugendhilfeeinrichtungen und kommunale Gesundheitsprogramme
- **Technologisch:** Adaptierbarkeit des KI-Frameworks für andere Zielgruppen (z. B. junge Erwachsene in Ausbildung, vulnerabel Beschäftigte)
- **Politisch-regulatorisch:** Einbindung in die strategische Diskussion zu Digital Public Health und KI-Governance im Rahmen der KI-Verordnung (KI-VO)

Die Ergebnisse der Evaluation werden auch als **Beitrag zu regulatorischem Lernen** gewertet, etwa hinsichtlich der Anforderungen an Transparenz, Datenschutz und Erklärbarkeit von KI-Systemen im sensiblen Anwendungsfeld psychischer Gesundheit.

Ergebnisse / Lessons Learned

Da das Reallabor **AI4U** sich zum Zeitpunkt der Analyse (Frühjahr 2025) in der Abschlussphase befindet, liegen noch keine umfassenden Abschlussberichte oder Publikationen mit quantitativen Ergebnissen vor. Jedoch lassen sich aus den öffentlich zugänglichen Materialien und den dokumentierten Prozessen erste qualitative Erkenntnisse und strukturierte Lessons Learned ableiten.

Partizipative Entwicklung als zentraler Erfolgsfaktor

Ein zentrales Ergebnis der bisherigen Projektarbeit ist die **Bedeutung partizipativer Gestaltungsansätze**. Die aktive Einbindung von Jugendlichen – der primären Zielgruppe – in die App-Entwicklung wurde als essenziell für Akzeptanz, Passung und Nutzungswahrscheinlichkeit der Anwendung identifiziert. Dies wurde durch Co-Design-Workshops, Fokusgruppen und wiederholte Prototypenfeedbacks realisiert.

Ethik- und Datenschutzfragen als kontinuierliche Herausforderung

Das Projektteam hebt hervor, dass **datenschutzrechtliche und ethische Aspekte nicht als nachgelagerte Compliance-Aufgaben**, sondern als integraler Bestandteil der Produktentwicklung behandelt werden müssen. Dabei erwies sich die frühzeitige Einbindung von Datenschutzexpert:innen und Ethikkommissionen als hilfreich für die Akzeptanz des Projekts in der pädagogischen und psychosozialen Praxis.

Technologische und methodische Erkenntnisse

- Der Einsatz **ökopsychologischer Sensorik** zur Stimmungsverfolgung wurde als technisch machbar, aber sensibel in Bezug auf Einwilligung und Erklärungspflicht empfunden.
- **KI-basierte Personalisierung** von Mikrointerventionen benötigt adaptive Algorithmen, die erklärbar und transparent agieren – gerade im Umgang mit minderjährigen Nutzer:innen.
- Die Verbindung von **App-basierten Interventionen mit pädagogischen Settings** (z. B. Schulsozialarbeit) wurde als effektiver Kanal für die Nutzung identifiziert.

Transdisziplinäre Zusammenarbeit als Strukturprinzip

Die Zusammenarbeit zwischen medizinisch-psychologischer Forschung, Technikentwicklung, Jugendbildung und zivilgesellschaftlichen Partnern gilt als Erfolgsfaktor für eine kontextsensitive und praxisnahe Ausgestaltung der Anwendung. Die Erfahrung zeigt, dass derartige Kooperationen ausreichend moderiert und strukturiert werden müssen, um produktiv zu sein.

Beitrag zum regulatorischen Lernen

Auch wenn AI4U kein offizielles Reallabor mit Experimentierklausel ist, liefert es praxisnahe Erkenntnisse zur Umsetzung von:

- **Datenschutz in KI-Systemen für Jugendliche,**
- **Erklärbarkeit und Vertrauensbildung bei KI-Anwendungen im Public-Health-Bereich,**
- **Beteiligung vulnerabler Gruppen an der Entwicklung digitaler Systeme.**

Diese Einsichten werden nicht zuletzt im Rahmen der strategischen Weiterentwicklung von Public-Mental-Health-Angeboten auf Landesebene und der Diskussion um die Implementierung der **EU-KI-Verordnung** als relevant eingestuft.

Relevanz für Österreich

AI4U bietet für die Entwicklung und Implementierung von **KI-bezogenen Regulatory Sandboxes in Österreich** mehrere zentrale Anknüpfungspunkte. Insbesondere für die in Österreich aktuell diskutierte Ausgestaltung einer KI Sandbox im Sinne von Art. 57 der europäischen KI-Verordnung (2024) liefert AI4U ein relevantes Praxisbeispiel aus dem Bereich **psychische Gesundheit, Bildung und Public Health**, das sowohl regulatorisch als auch technologisch wichtige Erfahrungen ermöglicht.

Übertragbare Prinzipien für den österreichischen Kontext:

Element	Potenzielle Anschlussfähigkeit in Österreich
Partizipatives Design	Die intensive Beteiligung Jugendlicher im AI4U-Modell entspricht dem Anspruch der europäischen KI-Verordnung an benutzerzentrierte Entwicklung und kann als Modell für andere Zielgruppen (z. B. Schüler:innen, Lehrpersonal, Patient:innen) in Österreich adaptiert werden.
Datenschutzorientierung	AI4U demonstriert, wie auch bei sensiblen Daten (Gesundheit, Minderjährige) DSGVO-konforme Innovation ermöglicht werden kann – eine zentrale Herausforderung für die Konzeption einer Sandbox in Österreich.
Transdisziplinäre Governance	Die Reallaborstruktur mit Einbindung von Wissenschaft, Praxis und Zivilgesellschaft bietet ein übertragbares Steuerungsmodell für österreichische Sandbox-Formate.
Kooperation mit Technologiepartnern	Die Einbindung von KMU wie movisens GmbH ist ein Modellfall für die Beteiligung anwendungsnaher Unternehmen an Forschungs- und Testumgebungen.

Beitrag zu regulatorischem Lernen und Umsetzung der europäischen KI-Verordnung

Gemäß der KI-VO (Art. 57) sind Mitgliedstaaten verpflichtet, spätestens bis **August 2026** eine nationale KI-Sandbox zur Verfügung zu stellen. AI4U zeigt exemplarisch:

- **Wie KI-basierte Systeme im Hochrisikobereich** (psychische Gesundheit, Jugendliche) ethisch und datenschutzkonform gestaltet und getestet werden können.
- **Welche Schnittstellen zwischen App-Entwicklung, Aufsicht und Praxis** notwendig sind, um Vertrauen und Skalierung zu ermöglichen.

- **Wie regulatorische Unsicherheit proaktiv bearbeitet** werden kann – durch begleitende Governance, partizipative Ausgestaltung und Evaluation unter realen Bedingungen.

AI4U kann daher als funktionale Vorlage oder Inspiration für eine österreichische KI-Sandbox dienen, insbesondere:

- im Bereich psychosoziale Versorgung, E-Mental Health und Bildungstechnologien,
- im Hinblick auf **praxisnahe Gestaltung von Testumgebungen**.

Referenzen

AI4U-Projektteam. (2023a). Das Projekt und seine Partner. https://ai4u-training.de/das-projekt-kooperationspartner/

AI4U-Projektteam. (2023b). Das Projekt und seine Ziele. https://ai4u-training.de

AI4U-Projektteam. (2023c). Projektbeschreibung und Mittelverwendung. https://ai4u-training.de

Abu-Omar, K., Popp, J., Bergmann, M., Messing, S., Till, M., & Gelius, P. (2023). Gesundheitsförderung im Reallabor? Prävention und Gesundheitsförderung, 19(1), 40–47. https://doi.org/10.1007/s11553-023-01023-w

Baumeister, H., Bengel, J., Härter, M., Reif, A., & Hölzel, L. (2020). Digitale Interventionen in der Versorgung psychischer Störungen: Potenziale und Herausforderungen. Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz, 63, 131–139. https://doi.org/10.1007/s00103-020-03090-1

Europäische Kommission. (2024). Verordnung über Künstliche Intelligenz – AI Act. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206

Landtag von Baden-Württemberg. (2024). Reallabore: Stand und Perspektive in Baden-Württemberg (Drucksache 17/7537). https://www.landtag-bw.de

Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg. (2021a). Förderrichtlinie Reallabore. https://mwk.baden-wuerttemberg.de

Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg. (2021b). Reallabore als Instrument zur Umsetzung nachhaltiger Entwicklung. https://mwk.baden-wuerttemberg.de

Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg. (2021c). Reallabore in der Digitalisierungsstrategie BW – Projektförderübersicht. https://mwk.baden-wuerttemberg.de

movisens GmbH. (2023). Digitale Lösungen für psychologische Forschung und Intervention. https://www.movisens.com

Zentralinstitut für Seelische Gesundheit. (2023a). Künstliche Intelligenz für psychische Gesundheitsförderung. https://www.zi-mannheim.de

Zentralinstitut für Seelische Gesundheit. (2023b). Projektbeschreibung KI-gestützte Gesundheitsförderung. https://www.zi-mannheim.de

14.4 SANDKËSCHT – COMPLIANCE SANDBOX FÜR KI- UND DATENBASIERTE SYSTEME

Land / Region

Luxemburg

Sektor / Branche

Die luxemburgische Sandbox ist sektorübergreifend konzipiert und adressiert technologische Vorhaben mit erheblichem Datenschutzbezug. Schwerpunkte liegen insbesondere auf datenintensiven KI-Anwendungen mit erhöhtem Regulierungsbedarf. Zielbranchen sind unter anderem:

- Gesundheitswesen (z. B. patientennahe KI-Assistenzsysteme),
- Finanz- und Versicherungswesen (z. B. algorithmische Risikomodelle, Betrugserkennung),
- Verwaltung & E-Government (z. B. datengestützte Entscheidungsunterstützung),
- Industrie & digitale Plattformdienste (z. B. autonome Systeme, algorithmische Steuerung).

Besonderes Augenmerk gilt Vorhaben, bei denen eine **grundrechtlich sensible Datenverarbeitung** geplant ist, wie etwa biometrische Verfahren, automatisierte Profilbildung oder KI-gestützte Entscheidungsfindung (vgl. CNPD 2024a; LIST 2024).

Ausgangssituation

Luxemburg positioniert sich seit mehreren Jahren als digitaler Innovationsstandort – insbesondere im Bereich **FinTech, digitale Verwaltung und KI**. Gleichzeitig stellt die zunehmende Verbreitung algorithmischer Systeme neue Anforderungen an Datenschutz, Transparenz und Rechenschaftspflicht. Vor diesem Hintergrund wurde deutlich, dass sowohl öffentliche als auch private Akteure frühzeitig rechtliche Unsicherheiten identifizieren und adressieren müssen, bevor KI-Systeme in produktiven Einsatz gehen (vgl. CNPD 2024a; Paperjam 2024a).

Die luxemburgische Datenschutzaufsicht CNPD reagierte darauf mit dem Aufbau einer sogenannten „Sandkëscht“, einer datenschutzrechtlich begleiteten Testumgebung, in der Organisationen neue datenbasierte Systeme (insbesondere KI-Anwendungen) **vor der Einführung evaluieren können**. Ziel ist es, datenschutzkonforme Innovation zu ermöglichen, ohne auf regulatorische Klarheit verzichten zu müssen.

Der offizielle Start der Sandbox erfolgte am **21. Mai 2024**, zunächst mit dem Fokus auf die DSGVO. Perspektivisch soll das Format auch zur Vorbereitung auf die Anforderungen der europäischen KI-Verordnung beitragen, insbesondere im Hinblick auf Marktüberwachung und risikobasierte Prüfpflichten (vgl. CNPD 2024a; LIST 2024; Paperjam 2024b).

Rechtlicher Rahmen

Die luxemburgische KI-Sandbox *Sandkëscht* wurde auf Basis der **Datenschutz-Grundverordnung (DSGVO)** eingerichtet. Sie stützt sich insbesondere auf die Beratungs- und Begleitfunktionen der nationalen Datenschutzbehörde **Commission nationale pour la protection des données (CNPD)** gemäß Art. 57 DSGVO. Eine spezielle gesetzliche Grundlage für die Sandbox existiert derzeit nicht; Ausnahmen vom geltenden Recht sind nicht vorgesehen (vgl. CNPD 2024a).

Die Teilnahme erfolgt im Rahmen eines **nichtproduktiven Testverfahrens**, bei dem datenintensive Systeme (insbesondere KI-Anwendungen) unter kontrollierten Bedingungen hinsichtlich ihrer Datenschutzkonformität geprüft werden. Zentrale Prüffelder sind:

- Rechtmäßigkeit und Transparenz der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO),
- Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25 DSGVO),
- Risikoabschätzungen gemäß Art. 35 DSGVO für besonders risikobehaftete Systeme (z. B. Profiling, biometrische Verfahren).

Die Sandbox ist ausdrücklich nicht als Ausnahmeregelung, sondern als **kooperative Compliance-Unterstützung** konzipiert (vgl. CNPD 2024a; Paperjam 2024b).

Mit Blick auf die seit 2024 in Kraft befindliche **europäischen KI-Verordnung** sieht die CNPD die *Sandkëscht* als vorbereitende Maßnahme zur Umsetzung des künftigen regulatorischen Auftrags gemäß Art. 53 KI-VO. Die Datenschutzbehörde wird in diesem Zusammenhang eine Schlüsselrolle bei der **Marktüberwachung von KI-Systemen** übernehmen und bereitet sich organisatorisch und methodisch auf diese erweiterten Aufgaben vor (vgl. Paperjam 2024a; LIST 2024).

Ein nationaler Rechtsrahmen zur operativen Umsetzung der europäischen KI-Verordnung in Luxemburg befindet sich mit Stand Juli 2025 **in Ausarbeitung**. Die *Sandkëscht* wird daher bereits als Vorläufer einer später formalisierten KI-Sandbox verstanden.

Beteiligte Akteure

Die *Sandkëscht* wird von der **CNPD** getragen, der unabhängigen Datenschutzaufsichtsbehörde Luxemburgs. Die CNPD ist zentrale Koordinations- und Umsetzungsstelle der Sandbox und verantwortlich für die rechtliche Begleitung aller teilnehmenden Organisationen (vgl. CNPD 2024a).

Die **CNPD** übernimmt dabei mehrere Rollen:

- **Projektselektion** auf Basis definierter Kriterien (Innovationsgehalt, Datenschutzbezug, gesellschaftlicher Nutzen),
- **Begleitung und Bewertung** der datenschutzrechtlichen Herausforderungen im Projektverlauf,
- **Methodenentwicklung** zur Strukturierung des Sandbox-Prozesses (Dauer, Phasen, Berichtspflichten),

- **strategische Weiterentwicklung** im Kontext der europäischen KI-Verordnung und künftiger nationaler Regulierungsstrukturen (vgl. Paperjam 2024b).

Teilnahmeberechtigt sind laut Ausschreibung **alle Organisationen mit Sitz oder substantieller Tätigkeit in Luxemburg**, unabhängig von Größe, Sektor oder Rechtsform. Besonders angesprochen werden:

- Start-ups und KMU mit datenbasierten Produkten (z. B. im Finanz-, Gesundheits- oder Mobilitätsbereich),
- öffentliche Stellen, die datengetriebene Entscheidungsunterstützungssysteme pilotieren wollen,
- größere Unternehmen mit komplexen datenschutzrechtlichen Fragestellungen bei KI-Systemen (vgl. CNPD 2024a).

Die **Projekte werden individuell begleitet**, es erfolgt keine kollektive Kohorte wie in klassischen Forschungsprojekten. Der Eintritt erfolgt auf Antrag, nach Vorprüfung und Auswahl durch die CNPD. Die Zusammenarbeit ist projektbezogen, mit **individuell zugeschnittenem Prüfplan** je nach Technologie und Risiko (vgl. CNPD 2024a).

Neben der CNPD als federführender Institution sind weitere strategische Partner eingebunden:

- das **Ministerium für Digitalisierung**, das das Projekt im Rahmen seiner nationalen Datenstrategie begleitet,
- das **Wirtschaftsministerium**, das für die künftige Marktüberwachung von KI-Systemen zuständig sein wird,
- Forschungseinrichtungen wie das **Luxembourg Institute of Science and Technology (LIST)**, die an begleitenden Analysen mitwirken (vgl. LIST 2024).

Die Sandbox ist zudem über internationale Netzwerke (z. B. EDPB, GPA) mit anderen Datenschutzaufsichten und europäischen Regulierungsinitiativen vernetzt. In Fachforen wie **ISACA Luxembourg (Juni 2025)** oder **NEXUS2050** wurde das Modell öffentlich vorgestellt und weiterentwickelt (vgl. CNPD 2025).

Gegenstand der Erprobung

Die *Sandkëscht* ist als datenschutzrechtlich begleitete Testumgebung konzipiert, in der Organisationen geplante datenbasierte Technologien **vor dem produktiven Einsatz auf ihre DSGVO-Konformität** prüfen lassen können. Die Erprobung erfolgt in einem kontrollierten, nichtöffentlichen Umfeld, unter enger Begleitung der CNPD (vgl. CNPD 2024a).

Zugelassen werden Anwendungen, bei denen ein **klar identifizierbarer datenschutzrechtlicher Klärungsbedarf** besteht, z. B. bei:

- automatisierter Entscheidungsfindung mit individueller Wirkung (Art. 22 DSGVO),
- der Verarbeitung besonders sensibler personenbezogener Daten (Art. 9 DSGVO),
- biometrischen Systemen, Verhaltensprofilen oder algorithmischem Scoring,

- komplexen Systemarchitekturen mit mehreren Datenverantwortlichen oder Auftragsverarbeitern.

Die teilnehmenden Projekte müssen einen erkennbaren Innovationsbeitrag leisten:

- neue technische Verfahren (z. B. multimodale KI, generative Modelle),
- neue organisatorische Konstellationen (z. B. Datentreuhänder, sektorübergreifende Anwendungen),
- gesellschaftlicher Mehrwert (z. B. Nachhaltigkeit, digitale Inklusion) (vgl. CNPD 2024a; Paperjam 2024a).

Die Erprobung gliedert sich in drei Hauptphasen (vgl. CNPD 2024a):

1. **Initialanalyse und Roadmap-Entwicklung:** Feststellung des rechtlichen Risikoprofils und Planung der Prüfung,
2. **Umsetzung & Maßnahmenbegleitung:** Validierung technischer und organisatorischer Schutzmaßnahmen im Sandbox-Modus,
3. **Ergebnisanalyse & Abschlussbewertung:** Erarbeitung einer abschließenden datenschutzrechtlichen Einschätzung („Gap Analysis“, Exit Report).

Mit Stand Juli 2025 wurden zwei Pilotprojekte öffentlich erwähnt. Konkrete Inhalte wurden nicht detailliert kommuniziert, die CNPD verweist jedoch auf Anwendungsfelder wie:

- KI-gestützte Sprachanalyse zur Kundeninteraktion im Dienstleistungsbereich,
- algorithmische Risikomodelle im Finanzsektor (vgl. CNPD 2025, ISACA-Präsentation).

Darüber hinaus wurde betont, dass die *Sandkëscht* bewusst als **lernorientiertes Modell** ausgelegt ist: Neben der individuellen Beratung steht der Aufbau regulatorischer Erfahrungswerte insbesondere mit Blick auf die bevorstehenden Pflichten aus der europäischen KI-Verordnung im Fokus.

Dauer & Ablauf

Die *Sandkëscht* wurde im **Mai 2024** offiziell von der **CNPD** gestartet. Sie ist als **laufende Struktur mit kontinuierlicher Antragstellung** angelegt und nicht als einmaliges Pilotprogramm. Organisationen können sich jederzeit mit einem geeigneten Projekt bewerben; die Auswahl erfolgt auf Basis definierter Kriterien (vgl. CNPD 2024a).

Die Teilnahme an der Sandbox erfolgt nach einem mehrstufigen Verfahren, das in **drei Phasen** organisiert ist und eine Gesamtdauer von **9 bis 18 Monaten** umfassen kann:

1. **Initialphase (3–6 Monate):**
    - Analyse des geplanten Systems und der datenschutzrechtlichen Herausforderungen,
    - Entwicklung einer individuellen Prüfstrategie (Roadmap),
    - gemeinsame Zieldefinition und Risikoeinschätzung durch CNPD und Organisation.

2. **Umsetzungsphase (3–6 Monate):**
    - Erprobung technischer und organisatorischer Maßnahmen,
    - kontinuierliche Abstimmung mit der CNPD bei offenen Punkten,
    - optional: Ergänzung durch Folgenabschätzung oder Datenflussanalyse.
3. **Abschlussphase (3–6 Monate):**
    - Bewertung der verbleibenden Risiken (Gap Analysis),
    - Dokumentation des Erprobungsergebnisses (Exit Report),
    - Entscheidung über potenzielle produktive Umsetzung außerhalb der Sandbox.

Die Gesamtzeit richtet sich nach **Komplexität und Reifegrad** des jeweiligen Projekts. In Ausnahmefällen kann die Dauer angepasst oder verlängert werden, etwa bei interorganisationalen Anwendungen oder neuartigen Verarbeitungstechniken (vgl. CNPD 2024a; CNPD 2025).

Die CNPD hat angekündigt, die operativen Erfahrungen aus den ersten Projekten ab **Herbst 2025 systematisch auszuwerten**, um daraus standardisierte Prozessbausteine für die spätere Umsetzung der **europäischen KI-Verordnung** zu entwickeln (vgl. CNPD 2025, NEXUS2050).

Finanzierung und Ressourcen

Die *Sandkëscht* wird vollständig durch öffentliche Mittel getragen und ist institutionell bei der **CNPD** angesiedelt. Sie ist Teil der strategischen Aktivitäten der Behörde im Bereich datenschutzfreundlicher Innovation und wird aus dem **regulären Jahresbudget der CNPD** finanziert (vgl. CNPD 2024a).

Im Jahr 2024 verfügte die CNPD über ein Budget von rund **10,3 Mio. EUR**, mit einem Personalstand von 67 Mitarbeitenden (Stand: Oktober 2024). Die Finanzierung der Sandbox erfolgt dabei nicht als gesonderter Fonds, sondern innerhalb der vorhandenen Ressourcen und durch **Umverteilung innerhalb der Behörde** (vgl. Herrmann 2024, S. 6–7).

Die teilnehmenden Organisationen erhalten **keine monetäre Förderung**, sondern profitieren von:

- kostenfreier projektbezogener Beratung durch die CNPD,
- individueller Risikobewertung und Handlungsempfehlungen,
- strukturierter Begleitung durch das Sandbox-Verfahren,
- Sichtbarkeit als Teil eines offiziell betreuten Regulierungsformats.

Die personellen Ressourcen für die Sandbox werden intern durch ein kleines, interdisziplinäres Team bereitgestellt, das juristische, technische und strategische Expertise bündelt. Zusätzlich wird bei Bedarf auf Fachpersonal innerhalb der CNPD (z. B. IT-Spezialist:innen, Audit-Fachkräfte) zurückgegriffen. Für besonders komplexe Fragestellungen kann die Behörde externe Expertise einbinden (vgl. CNPD 2025).

Eine Ausweitung der Ressourcen ist mittelfristig vorgesehen, da die CNPD gemäß europäischer KI-Verordnung künftig auch als **zuständige Marktüberwachungsbehörde** für KI-Systeme tätig sein soll. Die Sandbox dient in diesem Kontext bereits heute als **institutioneller Aufbauprozess** für neue Prüf- und Begleitfunktionen (vgl. Paperjam 2024b).

Governance-Modell

Die *Sandkëscht* wird zentral von der **CNPD** verantwortet und operativ gesteuert. Die CNPD agiert dabei in einer **Doppelrolle**: als unabhängige Aufsichtsbehörde im Bereich Datenschutz und als proaktiv begleitende Partnerin im Innovationskontext (vgl. CNPD 2024a).

Die Governance der Sandbox folgt einem **integrierten Ansatz**, der auf Individualisierung, Transparenz und Verlässlichkeit ausgelegt ist. Wesentliche Merkmale:

Einzelfallbezogene Steuerung

Jedes Sandbox-Projekt wird individuell geprüft, ausgewählt und begleitet. Es gibt kein standardisiertes Kohortenverfahren. Die CNPD entscheidet im Rahmen eines internen Auswahlprozesses über die Aufnahme in die Sandbox. Grundlage sind formale und inhaltliche Kriterien, u. a. Innovationsgrad, datenschutzrechtlicher Klärungsbedarf, gesellschaftlicher Nutzen und Sitz der Organisation in Luxemburg (vgl. CNPD 2024a).

Operative Umsetzung durch internes Expert:innen-Team

Die Koordination erfolgt durch ein interdisziplinäres Team innerhalb der CNPD, das juristische, technische und strategische Kompetenz vereint. Die Begleitung der Projekte erfolgt entlang eines standardisierten Verfahrensmodells mit definierten Phasen (vgl. Punkt 8). Zusätzlich werden projektspezifische Fachkräfte aus der CNPD eingebunden – etwa für Risikoanalysen, technische Prüfungen oder Kommunikation (vgl. Herrmann 2024).

Transparente Kommunikation und Dokumentation

Die Ergebnisse der einzelnen Sandbox-Projekte werden in Form von Exit-Berichten und öffentlichen Empfehlungen dokumentiert. Dabei wird auf Schutz sensibler Informationen und eine angemessene Anonymisierung geachtet. Ziel ist es, **Best Practices und regulatorische Klarheit** auch über die Einzelprojekte hinaus zu fördern (vgl. CNPD 2024a; Paperjam 2024b).

Strategische Weiterentwicklung in Richtung Europäische KI-Verordnung

Im Rahmen der nationalen Vorbereitung auf die Umsetzung der **europäischen KI-Verordnung** übernimmt die CNPD eine koordinierende Rolle bei der Konzeption künftiger Regulierungsstrukturen. Die Sandbox dient dabei als **lernorientierter Vorläufer**, in dem methodische, prozessuale und personelle Anforderungen für eine KI-VO-konforme Sandbox-Architektur erprobt werden (vgl. CNPD 2025; LIST 2024).

Evaluations- und Skalierungsstrategie

Die *Sandkëscht* verfolgt eine **doppelte Evaluationslogik**: einerseits die projektbezogene Analyse einzelner Anwendungen im Hinblick auf Datenschutzkonformität, andererseits die strategische Weiterentwicklung des Formats im Rahmen der nationalen KI-Governance (vgl. CNPD 2024a).

1) Evaluation auf Projektebene

Jedes teilnehmende Projekt wird durch die CNPD entlang eines standardisierten Ablaufs begleitet. Am Ende steht ein sogenannter **Exit Report**, der die datenschutzrechtlichen Risiken, die umgesetzten Maßnahmen sowie offene Punkte dokumentiert. Die CNPD nutzt diese Reports zur Ableitung von Empfehlungen – sowohl für die teilnehmende Organisation als auch für künftige Fälle mit ähnlichem Profil (vgl. CNPD 2024a; CNPD 2025).

2) Meta-Evaluation des Sandbox-Modells

Parallel zu den Einzelprojekten evaluiert die CNPD laufend:

- die Wirksamkeit des Verfahrensmodells,
- die Eignung der eingesetzten Methoden zur Risikobewertung,
- die Anschlussfähigkeit an künftige KI-VO-Vorgaben.

Die CNPD hat angekündigt, ab **Herbst 2025** einen systematischen Review-Prozess durchzuführen, in dem die Erfahrungen aus den ersten beiden Jahren strukturiert aufgearbeitet und in ein konsolidiertes Verfahren überführt werden sollen (vgl. CNPD 2025).

3) Strategische Skalierung im Vorfeld der europäischen KI-Verordnung

Im Zuge der bevorstehenden nationalen Umsetzung der **KI-VO** (spätestens bis 2026) soll die Sandbox strukturell weiterentwickelt werden. Mögliche Schritte sind:

- Ausweitung auf andere Risikoklassen gemäß KI-VO (über reine Datenschutzfragen hinaus),
- institutionelle Kopplung mit Marktüberwachungsfunktionen (Art. 53 KI-VO),
- Ergänzung durch technologische Prüfkompetenzen (z. B. Robustheit, Nachvollziehbarkeit).

Die CNPD strebt dabei keine umfassende Neuorganisation an, sondern eine **schrittweise Integration** des bestehenden Modells in künftige aufsichtsrechtliche Strukturen – im Dialog mit anderen Behörden, Ministerien und europäischen Partnerinstitutionen (vgl. LIST 2024; Paperjam 2024b).

Ergebnisse / Lessons Learned

Da sich die *Sandkëscht* Mitte 2025 noch in der frühen Implementierungsphase befindet, liegen nur eingeschränkt quantitative Ergebnisse vor. Dennoch lassen sich aus den ersten Pilotprojekten sowie aus dem strukturellen Aufbau mehrere übergreifende Erkenntnisse ableiten (vgl. CNPD 2025; Herrmann 2024):

1) Datenschutzkonformität ist realisierbar – aber aufwendig

Die ersten Anwendungsfälle zeigen, dass die datenschutzkonforme Umsetzung komplexer KI-Systeme grundsätzlich möglich ist. Allerdings erfordert dies **intensive Abstimmung**, insbesondere bei automatisierten Entscheidungsprozessen, multiplen Datenverantwortlichen oder sensiblen Datenkategorien wie Biometrie oder Gesundheitsdaten.

2) Frühzeitige Begleitung erhöht Compliance und Vertrauen

Die begleitende Rolle der CNPD wurde von den teilnehmenden Organisationen als **vertrauensbildend und risikoreduzierend** beschrieben. Durch die strukturierte Vorabprüfung konnten Unsicherheiten beseitigt, technische Nachbesserungen früh eingeleitet und Haftungsrisiken minimiert werden (vgl. CNPD 2024a; Paperjam 2024b).

3) Einzelfallzentrierung erhöht Qualität, begrenzt aber Skalierung

Das Modell der *Sandkëscht* basiert auf einer intensiven Einzelfallbegleitung. Dies gewährleistet hohe Qualität, limitiert aber die Anzahl paralleler Projekte. Eine künftige Skalierung – etwa unter dem Dach der KI-VO – wird Anpassungen beim Ressourcenmanagement und der Verfahrensstruktur erfordern.

4) KI-VO-Kompatibilität braucht institutionelle Koordination

Die CNPD erkennt an, dass eine KI-VO-konforme Sandbox über reine Datenschutzfragen hinausgeht (z. B. technische Robustheit, Risikobewertung, Transparenzpflichten). Erste Koordinierungsgespräche mit weiteren Behörden sind angelaufen. Die Sandbox dient dabei als **institutionelles Lerninstrument**, um neue Kompetenzen und Schnittstellen frühzeitig aufzubauen (vgl. LIST 2024; CNPD 2025).

5) Nachfrage vorhanden, sektorübergreifende Relevanz erkennbar

Laut CNPD gingen seit 2024 mehrere qualifizierte Projektanträge ein, u. a. aus dem Finanzsektor, dem öffentlichen Dienstleistungsbereich und der Industrie. Dies bestätigt die **hohe Relevanz datenschutzkonformer Innovationsformate** über Sektorgrenzen hinweg und besonders für kleine und mittlere Unternehmen, die auf Orientierung und Rechtssicherheit angewiesen sind.

Relevanz für Österreich

1) Rechtskonforme Innovation ist auch ohne Gesetzesänderung möglich

Die Sandbox zeigt, dass eine datenschutzrechtlich begleitete Erprobung von KI-Systemen **innerhalb bestehender Rechtsrahmen** (DSGVO) realisierbar ist. Auch in Österreich könnte etwa die Datenschutzbehörde oder ein zuständiges Ministerium niedrigschwellige Prüfformate als vorbereitenden Zwischenschritt vor einer umfassenden KI-VO-Sandbox schaffen.

2) Rollenklarheit der Datenschutzaufsicht wird zentral

Luxemburg zeigt, wie eine Datenschutzbehörde **proaktiv regulatorische Innovationsräume** im Sinne eines kooperativen Compliance-Modells gestalten kann. Für Österreich ergibt sich daraus eine strategische Frage: Soll die Datenschutzbehörde auch an einer nationalen KI-Sandbox mitwirken oder nur ex post kontrollieren? In diesem Fall wurde die starke Einbindung als Erfolgsfaktor beschrieben.

3) Einzelfallbasierte Formate eignen sich besonders für KMU

Das Modell der individualisierten Sandbox-Begleitung bietet **niederschwellige Einstiegspunkte für KMU**, die sonst selten aktiv an regulatorischen Prozessen teilnehmen. Österreich könnte davon profitieren, indem es zielgerichtet Use Cases mit hoher Relevanz für kleine Unternehmen oder öffentliche Dienstleister anspricht. KMU brauchen jedoch auch in diesem Fall ausreichende Unterstützung.

4) Sandbox als Vorbereitung auf Marktüberwachung nach KI-VO

Die *Sandkëscht* fungiert bereits als **institutionelles Lernfeld** für die künftige Marktüberwachung von KI-Systemen gemäß Art. 64 KI-VO. Auch Österreich wird diese Aufgaben auf nationaler Ebene umsetzen müssen. Die frühzeitige Etablierung einer „Pre-AI-Act-Sandbox" kann helfen, interne Strukturen, Prüfprozesse und Rollenverteilungen rechtzeitig zu erproben. Auch wenn mit dem starken Fokus auf Datenschutz in diesem Fall nicht alle Handlungsfelder einer KI-Sandbox erfüllt sind, scheint der dezidierte Fokus auf ein Handlungsfeld ein guter Start zu sein.

5) Übertragbarkeit auf sektorale oder föderale Sandbox-Modelle

Die *Sandkëscht* ist behördlich getragen, aber sektoroffen – ein Modell, das sich gut mit der föderalen Struktur Österreichs kombinieren lässt. Denkbar wäre etwa eine **datenschutzorientierte Sandbox auf Bundesebene** (z. B. für Verwaltung und Gesundheit) in Verbindung mit regionalen Sandboxes (z. B. in Wien oder der Steiermark für Industrie oder Bildung).

Referenzen

CNPD – Commission nationale pour la protection des données (2024a): Lancement de la « Sandkëscht » – la CNPD lance un environnement de test pour les projets innovants à fort enjeu en matière de protection des données. Pressemitteilung vom 21. Mai 2024. Online verfügbar unter: https://cnpd.public.lu/de/actualites/national/2024/05/lancement-sandkescht.html [abgerufen am 12.07.2025].

CNPD – Commission nationale pour la protection des données (2025): Présentation de la Sandbox Sandkëscht. Vortrag bei der ISACA Luxembourg Chapter General Assembly, Juni 2025 (nicht veröffentlicht, zitiert nach mündlicher Präsentation).

Herrmann, Alain (2024): How can compliance sandboxes help the industry? Vortrag beim Münchner Datenschutz-Tag am 29.11.2024, CNPD Luxembourg.

LIST – Luxembourg Institute of Science and Technology (2024): What Luxembourg intends to do about AI. Online verfügbar unter: https://www.list.lu/fr/media/presse/what-luxembourg-intends-to-do-about-ai/ [abgerufen am 12.07.2025].

Paperjam (2024a): With REMI, Luxembourg launches its AI sandbox. Artikel vom 22. Mai 2024. Online verfügbar unter: https://en.paperjam.lu/article/with-remi-luxembourg-launches-its-ai-sandbox [abgerufen am 12.07.2025].

Paperjam (2024b): AI sandboxing could be a strategic lever for Luxembourg. Artikel vom 17. Juni 2024. Online verfügbar unter: https://en.paperjam.lu/article/ai-sandboxing-could-be-a-strategic-lever-for-luxembourg [abgerufen am 12.07.2025].

14.5 RESÜMEE

Die vier analysierten Sandbox-Modelle (Spanien, Schweiz, Deutschland und Luxemburg) unterscheiden sich in Aufbau, Zielrichtung und institutioneller Anbindung deutlich. Gleichzeitig lassen sich zentrale Muster und wiederkehrende Gestaltungsprinzipien erkennen, die für die Konzeption einer österreichischen KI-Sandbox besonders relevant sind.

1. Unterschiedliche Ausgangsbedingungen – aber ähnliche Zielsetzung

Ob als nationaler KI-Pilot (Spanien), regionales Innovationsformat (Zürich), themenspezifisches Reallabor (Baden-Württemberg) oder Compliance-orientierte Behörden-Sandbox (Luxemburg): Allen Projekten liegt ein gemeinsames Ziel zugrunde: die sichere und verantwortungsvolle Erprobung neuer KI-Systeme unter realitätsnahen Bedingungen mit dem Ziel, regulatorische Klarheit zu schaffen.

Für Österreich ergibt sich daraus:

- Eine Sandbox muss nicht zwingend umfassend und zentralisiert starten. Auch regionale oder thematisch fokussierte Formate können strategisch wirksam sein.
- Die Zielsetzung sollte stets regulatorisches Lernen und Innovationsunterstützung verbinden und idealerweise entlang konkreter Anwendungsfälle organisiert sein.

2. Governance entscheidet über Qualität und Wirkung

Die Analyse zeigt: Eine funktionierende Sandbox braucht eine klare Governance-Struktur mit definierten Rollen, transparenter Steuerung und fähigen Mittlerinstitutionen. Erfolgreich waren insbesondere Modelle mit **multi-aktoraler Steuerung** und **evidenzbasierter Rückkopplung**, etwa in Spanien (FG1/FG2-Modell) oder Zürich (interdisziplinäre Steuerungsgruppe).

Für Österreich besonders relevant:

- Eine Governance-Struktur sollte föderale und sektorale Zuständigkeiten koordinieren – idealerweise durch eine neutrale Stelle mit Vermittlungsfunktion.
- Der Aufbau sollte Co-Creation ermöglichen, nicht nur Top-down-Verwaltung. Beteiligung von KMU, Forschung, Aufsicht und Zivilgesellschaft ist kein Add-on, sondern Erfolgsbedingung.

3. Rechtsrahmen: Möglichst klar, aber nicht zwingend neu

Weder in der Schweiz noch in Luxemburg basierte die Sandbox auf einer speziellen Experimentierklausel. Stattdessen wurde der bestehende Rechtsrahmen produktiv mit Fokus auf Rechtssicherheit und Vertrauensbildung ausgelegt. Spanien hingegen nutzte gezielt europäische Mittel und politische Rahmungen, um rechtliche Unsicherheiten koordiniert zu adressieren.

Daraus folgt für Österreich:

- Eine erste Sandbox muss nicht auf eine Gesetzesreform warten. Auch unter geltendem Recht ist Innovation möglich, wenn Governance, Transparenz und Dokumentation stimmen.

- Mittelfristig wäre eine gesetzliche Grundlage sinnvoll, insbesondere für sektorübergreifende Vorhaben oder Ausnahmen vom Standardprozess (z. B. gemäß Art. 53–57 KI-VO).

4. Sektorale Ausrichtung: Fokus schafft Tiefe – Offenheit schafft Breite

Die Spannbreite reicht von sektorspezifischer Ausrichtung (AI4U: psychische Gesundheit) bis zu offenen Kohortenformaten (Spanien). Erfolgreiche Sandboxes wählten eine **sorgfältige Balance** zwischen Fokussierung und Transferpotenzial.

Für die österreichische Ausgestaltung bedeutet das:

- Ein erster Pilot sollte einen klaren thematischen Fokus haben (z. B. Public Sector AI, Gesundheit, Industrie 4.0) und idealerweise dort eingesetzt werden, wo hoher gesellschaftlicher Nutzen und regulatorischer Orientierungsbedarf zusammentreffen.
- Gleichzeitig sollte die Struktur übertragbar bleiben, etwa durch modulare Kohorten, optionale Beteiligungsformate oder sektorübergreifende Leitfäden.

5. Evaluationskultur und Wissensverwertung sind erfolgskritisch

Alle vier Fallbeispiele legen Wert auf strukturierte Evaluation. Sei es durch Exit Reports (Luxemburg), Good Practice Guides (Spanien), öffentlich dokumentierte Lessons Learned (Zürich) oder partizipative Wirksamkeitsstudien (AI4U). Die Sandbox dient hier nicht nur der Unterstützung Einzelner, sondern dem **Aufbau kollektiver Lernprozesse**.

Konsequenz für Österreich:

- Eine KI-Sandbox muss von Beginn an mit einer Evaluationslogik verknüpft sein – nicht nur zur Erfolgsmessung, sondern zur Skalierung und Regulierungsvorbereitung.
- Ergebnisoffenheit, Feedbackschleifen und transparente Kommunikation sind auch gegenüber Öffentlichkeit, Politik und europäischer Ebene entscheidend.

6. Ressourcen und Kontinuität: Qualität braucht Zeit und Kompetenz

Alle Sandboxes zeigen: Wirksames regulatorisches Testen ist ressourcenintensiv. Neben finanziellen Mitteln braucht es **interdisziplinäres Personal**, technische Infrastrukturen und rechtliche Begleitung. Die Projekte wurden über mehrere Jahre aufgebaut, oft mit modularer Weiterentwicklung (Zürich, Spanien).

Für Österreich ist daher wichtig:

- Eine mehrjährige Grundfinanzierung ist notwendig, mindestens für Konzeption, erste Testzyklen und Evaluation.
- Personal sollte projektübergreifend verfügbar sein und im besten Fall in einer zentralen Koordinationsstruktur mit juristischer, technischer und sektorspezifischer Kompetenz.

Zusammenfassend lässt sich festhalten:

Eine österreichische KI-Sandbox kann von den hier analysierten Modellen erheblich profitieren, indem Prinzipien abgeleitet und kombiniert werden:

- **Kooperatives Governance-Modell** mit klarer Zuständigkeit und Partizipation,
- **Rechtskompatibles Design** auch ohne umfassende neue Gesetzgebung,

- **Thematische Fokussierung** mit sektoraler Anschlussfähigkeit,
- **Verbindliche Evaluationsstrukturen** zur Wissensgenerierung und Skalierung,
- **Ressourcensicherung** zur Qualitätssicherung und institutionellen Verstetigung.

Diese Elemente bilden das Fundament für ein wirksames, anschlussfähiges und zukunftsorientiertes Sandbox-Modell im Sinne der europäischen KI-Verordnung und darüber hinaus für eine innovationsfreundliche, grundrechtsbasierte KI-Governance in Österreich.

15 Anhang 2: Fragenkatalog

1. Konzeptionelle Grundlagen und Begriffsverständnis
1.1 Was sind Regulatory Sandboxes und wie unterscheiden sie sich von Reallaboren und Testumgebungen?
1.2 Welche Typen von Regulatory Sandboxes existieren (z. B. mit/ohne Experimentierklausel, sektoral vs. sektorübergreifend)?
1.3 Welche Zielsetzungen verfolgen Regulatory Sandboxes (z. B. Technologieerprobung, Politiklernen, Regulierungsinnovation)?

2. Rechtlich-institutioneller Rahmen
2.1 Welche gesetzlichen und regulatorischen Rahmenbedingungen bestehen derzeit in Österreich für RS?
2.2 Welche Lücken bestehen (z. B. fehlende Experimentierklauseln, kein Reallaborgesetz)?
2.3 Welche Unterschiede zeigen sich im Vergleich zu Ländern wie Deutschland, Spanien oder der Schweiz?

3. Internationale Good Practices
3.1 Welche internationalen Beispiele für RS gelten als „Good Practices“?
3.2 Welche Governance- und Beteiligungsmodelle haben sich international bewährt?
3.3 Welche Lehren lassen sich aus internationalen Umsetzungen für Österreich ziehen?

4. Spezifika für den KI-Bereich
4.1 Warum ist der KI-Bereich besonders sensibel für regulatorische Fragen (z. B. Datenschutz, ethische Risiken, Blackbox-Problematik)?
4.2 In welchen Sektoren zeigt sich besonderes Potenzial für KI-Sandboxes (z. B. Medizintechnik, Industrie, Medien, Mobilität)?
4.3 Welche Arten von KI-Anwendungen sind besonders sandbox-relevant (z. B. generative KI, hochriskante Systeme)?

5. Design- und Strukturfragen von RS
5.1 Welche Optionen bestehen für Struktur, Ablauf, Evaluation und Skalierung von RS?
5.2 Wie kann eine RS so gestaltet werden, dass sie Innovation ermöglicht und gleichzeitig regulatorisch anschlussfähig bleibt?
5.3 Welche Rollen spielen Risikomanagement, Überwachung und Lernprozesse im Sandbox-Design?

6. Anspruchsgruppen und Governance
6.1 Welche Anspruchsgruppen (Verwaltung, Unternehmen, Forschung, Gesellschaft) sollten in RS eingebunden werden?
6.2 Wie kann eine funktionale Governance-Struktur für eine nationale KI-Sandbox in

Österreich aussehen?
6.3 Welche Beteiligungs- und Koordinationsformen haben sich bewährt?

7. Europäische Rahmenbedingungen und Koordination
7.1 Welche Anforderungen ergeben sich aus der EU-KI-Verordnung für nationale Sandboxes?
7.2 Welche Möglichkeiten bestehen zur Abstimmung mit europäischen Initiativen (z. B. EU SIRE, SME Digital)?

8. Strategische Optionen und Empfehlungen
8.1 Welche Handlungsoptionen bestehen für Österreich zur Etablierung von KI-Sandboxes?
8.2 Welche Szenarien oder Idealtypen lassen sich als Modelle für eine nationale Sandbox-Struktur entwickeln?

16 Anhang 3: Details zum Co-Creation Process

Workshop 1: Regulatory Sandboxes im Bereich KI – Grundlagen und praktische Beispiele

Zeit und Ort

- Dienstag, 20.05.2025 von 13:30 bis 16:00
- Der Workshop fand als Online-Veranstaltung statt. Der MS-Teams-Link findet sich unten.

Workshop-Ziele

- Aktive Wissensvermittlung zum Thema Regulatory Sandboxes im Bereich KI mit praktischen Beispielen
- Exploration von relevanten Themen/Herausforderungen im Bereich Regulierung für die einzelnen Sparten der WKO
- Erste Identifikation von möglichen Themen und Unternehmen für potenzielle österreichische Use Cases

Ablauf

Thema	Zeit
Begrüßung der Teilnehmer:innen, Vorstellung der Workshop-Agenda, Housekeeping Rules	13:30 – 13:35
Kurze Vorstellung des Projekts (PPT)	13:35 – 13:40
Slido-Abfrage zum Vorwissen betreffend Reallaboren und Regulatory Sandboxes	13:40 – 13:50
Impulsreferat „Regulatorische Freiräume für KI: Chancen und Herausforderungen der Sandbox-Modelle“ (PPT Präsentation)	13:50 – 14:10
Diskussion (Q&A)	14:14 – 14:20
Impulsreferat „Regulatory Sandboxes im Bereich KI in der Praxis – internationale Beispiele und Übertragbarkeit auf Österreich“ (PPT Präsentation)	14:20 – 14:40
Diskussion (Q&A)	14:40 – 14:50
Pause	14:50 – 15:00

Moderierte Gruppendiskussion mit digitalem Whiteboard (Sammlung von Herausforderungen und Themen im Bereich Regulierung; Sammlung von relevanten Unternehmen für Interviews sowie Brainstorming über potenzielle Use Cases)	15:00 – 15:45
Abschluss (Resümee und Vorstellung der nächsten Schritte)	15:45 – 16:00

Teilnehmer:innen

Am Workshop haben Vertreter:innen der folgenden Organisationen teilgenommen:

- WKO, Sparte Industrie
- WKO, Sparte Information und Consulting
- WKO, Sparte Gewerbe & Handwerk
- WKO, Sparte Handel
- WKO, Sparte Transport und Verkehr
- WKO, Sparte Tourismus und Freizeitwirtschaft

Workshop 2: Regulatory Sandboxes im Bereich KI – Herausforderungen und mögliche Themen

Zeit und Ort

- Donnerstag, 12.06.2025 von 9:00 bis 11:00
- Der Workshop fand als Online-Veranstaltung statt.

Workshop-Ziele

- Strukturierte Diskussion von möglichen Themen für eine Regulatory Sandbox im Bereich KI
- Strukturierte Diskussion von Herausforderungen im Bereich Regulierung vor allem für Unternehmen

Ablauf

Thema	Zeit
Begrüßung der Teilnehmer:innen, Vorstellung der Workshop-Agenda, Housekeeping Rules	9:00 – 9:05
Kurze Vorstellung des Projekts (PPT)	9:05 – 9:10

Vorstellung der Draft-Themenmatrix	9:10 – 9:30
Moderierte Breakout-Session mit digitalem Whiteboard – Runde 1 (Feedback zur Draft-Themenmatrix sowie allfällige Modifikation und Ergänzung)	9:30 – 10:00
Pause	10:00 – 10:10
Präsentation der bereits identifizierten Herausforderungen	10:10 – 10:20
Moderierte Breakout-Session mit digitalem Whiteboard – Runde 2 (regulatorische Herausforderungen im Bereich KI für Unternehmen)	10:20 – 10:50
Abschluss (Resümee und Vorstellung der nächsten Schritte)	10:50 – 11:00

Teilnehmer:innen

Am Workshop haben Vertreter:innen der folgenden Organisationen teilgenommen:

- DIH Süd
- Industriellenvereinigung (IV)
- ONDEWO GmbH
- TRUSTIFAI
- IDea_Lab, Universität Graz
- Rundfunk und Telekom Regulierungs-GmbH
- Deine KI Agentur
- IB Lab GmbH
- alpLytics
- Medicus AI GmbH
- Data Protection Consulting e.U.

Workshop 3: World-Café – Regulatory Sandboxes im Bereich künstliche Intelligenz – Innovation und Regulierung im Dialog

Zeit und Ort

- Donnerstag, 26.06.2025 von 9:00 bis 11:00
- Der Workshop fand als Online-Veranstaltung statt.

Workshop-Ziele

Im Rahmen des World-Cafés wurden gemeinsam die folgenden Fragen diskutiert:

- Wie können Regulatory Sandboxes die Entwicklung und Markteinführung vertrauenswürdiger KI-Systeme fördern?
- Welche Chancen und Herausforderungen sehen Unternehmen, Start-ups, Behörden und die Zivilgesellschaft in der praktischen Umsetzung?
- Wie gelingt der Wissenstransfer zwischen Innovatoren und Regulierungsbehörden?
- Was sind zentrale Erfolgsfaktoren für eine effektive Sandbox-Gestaltung in Österreich und Europa?

Ablauf

Thema	Zeit
Begrüßung der Teilnehmer:innen, Vorstellung der Workshop-Agenda, Housekeeping Rules	9:00 – 9:05
Kurze Vorstellung des Projekts (PPT)	9:05 – 9:10
Impulsreferat und kurze Vorstellung der Tische	9:10 – 9:25
Aufteilung auf die Tische	9:25 – 9:30
Online World-Café – Runde 1	9:30 – 10:00
Pause – Wechsel zwischen den Tischen	10:00 – 10:10
Online World-Café – Runde 2	10:10 – 10:40
Plenum – kurze Vorstellung der Ergebnisse pro Tisch	10:40 – 10:55
Abschluss (Resümee und Vorstellung der nächsten Schritte)	10:55 – 11:00

Teilnehmer:innen

Am Workshop haben Vertreter:innen der folgenden Organisationen teilgenommen:

- Bundeskanzleramt
- Austrian Society for Artificial Intelligence (ASAI)
- Arbeiterkammer Wien
- eutema GmbH
- Bundesministerium für Wirtschaft, Energie und Tourismus
- Austrian Institute of Technology / FAIR-AI Leitprojekt
- Fachverband Metalltechnische Industrie (FMTI)
- ARGE Sicherheit und Wirtschaft

- Austromed
- SunRise AI Solutions GmbH
- Alina Savara, ISPA
- Wirtschaftskammer Wien
- appliedAI Initiative
- Erste Bank
- Dachverband der Elektro- und Elektronikindustrie (FEEI)
- AI ACT Now

POLICIES Research Report Series

Research Reports des Instituts für Wirtschafts- und Innovationsforschung der JOANNEUM RESEARCH geben die Ergebnisse ausgewählter Auftragsforschungsprojekte des POLICIES wieder. Weitere .pdf-Files der Research Report Series können unter http://www.joanneum.at/policies/rp heruntergeladen werden.

Für weitere Fragen wenden Sie sich bitte an policies@joanneum.at.

© 2016, JOANNEUM RESEARCH Forschungsgesellschaft mbH – Alle Rechte vorbehalten.

JOANNEUM RESEARCH
Forschungsgesellschaft mbH

POLICIES
Institut für
Wirtschafts- und
Innovationsforschung

Leonhardstraße 59
8010 Graz

Tel. +43 316 876-14 88
Fax +43 316 876-14 80

policies@joanneum.at
www.joanneum.at/policies

JOANNEUM RESEARCH
Forschungsgesellschaft mbH

POLICIES
Institut für
Wirtschafts- und
Innovationsforschung

Haus der Forschung
Sensengasse 1
1090 Wien

Tel. +43 1 581 75 20
Fax +43 1 581 75 20-28 20

policies@joanneum.at
www.joanneum.at/policies