

17. Österreichischer IT-Rechtstag

# KI Accountability und Sandboxes

**Dr. Hans Kristoferitsch, LL.M. – CERHA HEMPEL**

**Dr. Günther Leissler, LL.M. – SCHÖNHERR**

Wien, 05. Mai 2022

## *Themenübersicht*

1. Verordnungsentwurf für künstliche Intelligenz
2. Überblick KI-VO
3. Regulatory Sandboxes
4. Datennutzung bei Regulatory Sandboxes
5. Ausblick & Thesen



# 1. VERORDNUNGSENTWURF FÜR KÜNSTLICHE INTELLIGENZ

---

# Rechtliche Rahmenbedingungen

- Was ist Künstliche Intelligenz (Art 3 Abs 1 KI-VO):  
„Künstliche Intelligenz“ ist eine **Software**, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren
- Wer ist der Anbieter (Art 3 Abs 2 KI-VO):  
„Anbieter“ ist eine **natürliche oder juristische Person, Behörde**, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen

# Zweck der KI-VO

- Grundgedanke: Entwicklung und Förderung von KI-Systemen innerhalb Europas
- Entwurf der KI-VO enthält harmonisierte Vorschriften für das Inverkehrbringen und die Inbetriebnahme von KI-Systemen („vertrauenswürdige KI“)
- Bedürfnis neue Technologien und Geschäftsmodelle vor Marktstart unter realen Bedingungen zu erproben (Regulatory Sandboxes)
- Verbot bestimmter Praktiken im Bereich der künstlichen Intelligenz
- Besondere Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für Betreiber solcher Systeme
- Vorschriften für die Marktbeobachtung und Marktüberwachung
- Verbesserung von Prognosen und Optimierung von Abläufen

# Anwendungsbereich der KI-VO

**KI- VO gilt für:**

**Anbieter von KI-  
Systemen**  
(unabhängig von ihrer  
Niederlassung)

**Nutzer von KI-  
Systemen**  
(Aufenthalt in Union)

**Anbieter und Nutzer**  
(Niederlassung in  
Drittland aber Ergebnis  
in EU verwendet)

# Where are we now? (I)

**Regulierung von KI:**

**Leitlinien für  
vertrauenswürdige  
KI (08.04.2019)**

**Weißbuch zur  
Künstlichen  
Intelligenz  
(19.02.2020)**

**Entwurf der  
Kommission für KI-  
VO (21.04.2021)**

## Where are we now? (II)

**Regulierung von KI:**

**Folgenabschätzung  
der Kommission  
(21.04.2021)**

**Stellungnahme der  
EDPB und EDPS  
(18.06.2021)**

**Einführung der ersten  
Regulatory Sandbox für  
KI in der EU durch die  
spanische Regierung in  
Zusammenarbeit mit der  
Kommission (27.06.2022)**



# Where are we now? (III)

**Regulierung von KI:**

**Vorschlag der  
Kommission für  
KI-Haftungs-Richtlinie  
(28.09.2022)**

**Vorschlag des Rates  
für eine Verordnung  
zur Festlegung  
harmonisierter  
Normen für KI  
(25.11.2022)**

**Parlamentsvorschlag  
neuer verbotener  
KI-Praktiken und  
Kategorien für  
Hochrisiko-KI  
(06.02.2023)**

# Where are we NOW?

- KI-VO ist Zukunft, DSGVO ist Gegenwart
- KI-Definition ist Zukunft, Chat GPT & Co ist Gegenwart
- Resultat:
  - Italienische Datenschutzbehörde (*Garante*) untersuchte Chat GPT nach „data leak“ (Offenlegung von Chatinhalten auf Chat GPT)
  - Ergebnis: Anordnung der temporären Aussetzung des Dienstes in Italien
  - Gründe (Auszug):
    - i. Keine ausreichend transparente Datenschutzinformation
    - ii. Keine hinreichende Rechtsgrundlage für das Training des Algorithmus anhand personenbezogener Daten
    - iii. Teils Verarbeitung unrichtiger personenbezogener Daten
    - iv. Kein hinreichender Jugendschutz

# Where are we NOW?

- Erste „lessons learned“:
  - Regulierung der KI durch KI-VO liegt in der Zukunft
  - Regulierung der KI durch DSGVO ist die Gegenwart
  - Hauptthemen:
    - i. Information, Offenlegung, Bestimmung des Algorithmus = **die KI verstehen!**
    - ii. Verarbeiten von personenbezogenen Daten zu Trainingszwecken = **das Konzept von Regulatory Sandboxes verstehen!**

# Hey, Chat GPT...

*ChatGPT disabled for users in Italy*

*Dear ChatGPT user,*

*We regret to inform you that we have disabled ChatGPT for users in Italy at the request of the Italian Garante.*

*We are issuing refunds to all users in Italy who purchased a ChatGPT Plus subscription in March. We are also temporarily pausing subscription renewals in Italy so that users won't be charged while ChatGPT is suspended.*

*We are committed to protecting people's privacy and we believe we offer ChatGPT in compliance with GDPR and other privacy laws. We will engage with the Garante with the goal of restoring your access as soon as possible.*

*Many of you have told us that you find ChatGPT helpful for everyday tasks, and we look forward to making it available again soon.*

*If you have any questions or concerns regarding ChatGPT or the refund process, we have prepared a list of [Frequently Asked Questions](#) to address them.*

*—The OpenAI Support Team*

# Another Try: Hey, Chat GPT...

... are you data protection compliant?

*“As an AI language model, I am designed and developed with data protection compliance in mind. I do not collect, store or use any personal data unless explicitly requested by the user for a specific purpose, and I always follow the applicable laws and regulations, including the General Data Protection Regulation (GDPR) and other relevant data protection laws. Additionally, my developers and operators are committed to maintaining the highest standards of data protection and privacy, and regularly review and update the measures in place to ensure that they remain compliant with the relevant data protection regulations.”*

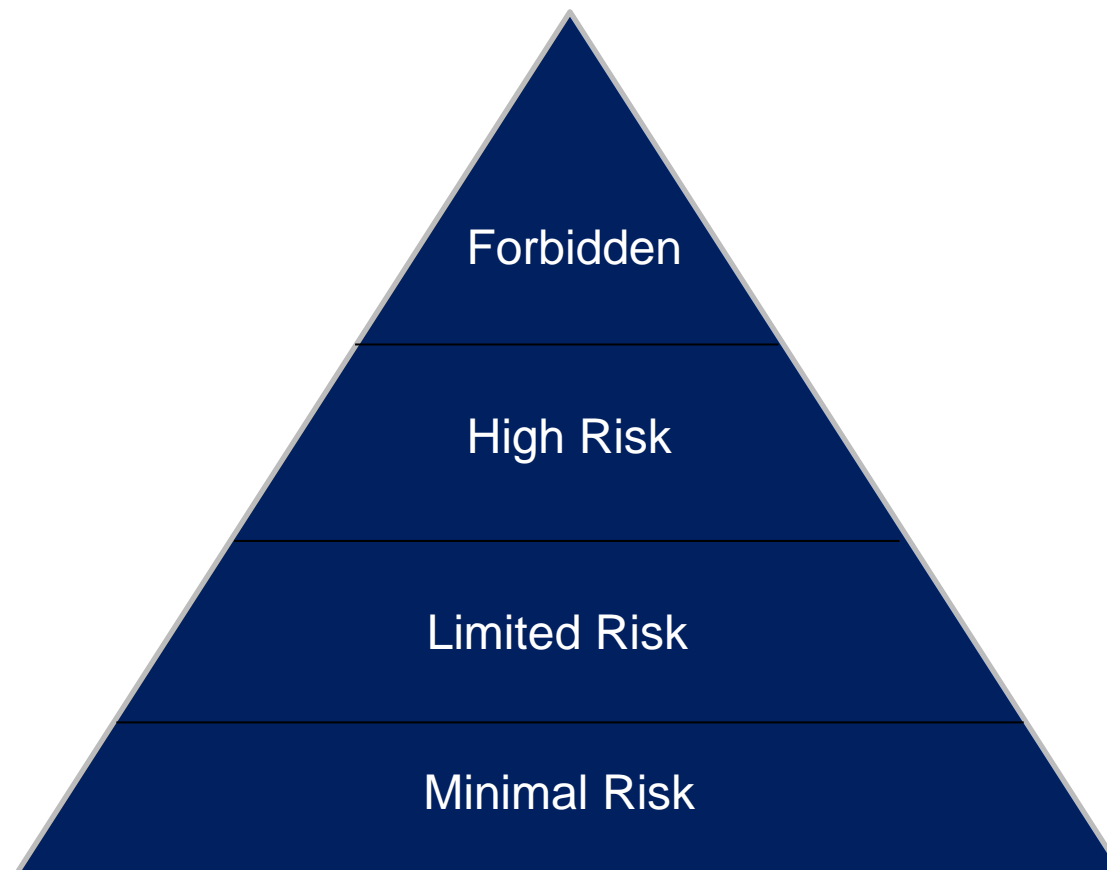
## 2. Überblick KI-VO

---

# Aufbau der KI-VO

- **Titel I: Allgemeine Bestimmungen** (Gegenstand, Anwendungsbereich, Begriffsbestimmungen)
- **Titel II: Verbotene Praktiken:**
  - Staatliche Praktiken (Bewertung des sozialen Verhaltens – Social Scoring)
  - Techniken, die das Bewusstsein unterschwellig beeinflussen
  - Biometrische Echtzeit-Fernidentifizierungssysteme (mit Ausnahmen)
- **Titel III: Hochrisiko KI-Systeme:**
  - KI-System als Sicherheitskomponente eines unter Anhang II fallenden Produkts (Bsp: Beeinträchtigung von Grundrechten)
  - Bedarf einer Konformitätsbewertung durch Dritte gemäß Anhang II
- **Titel IV: KI Systeme mit geringem Risiko**
  - Sonstige KI-Systeme mit Interaktion, Emotionserkennung und biometrischen Kategorisierung
  - KI-Systeme, die Bild-, Ton- oder Videoinhalte erzeugen oder manipulieren, die wirklichen Personen/Gegenständen/Orten merklich ähneln („Chat-Bots“) und einer Person fälschlicherweise als echt oder wahrhaftig erscheinen würden („Deepfake“)
- **Titel V: Maßnahmen zur Innovationsförderung (KI-Reallabore)**

# 4 Risikostufen von KI-Systemen





# KI-VO in a Nutshell

- Viele Ähnlichkeiten zur DSGVO (Bsp: Geltungsbereich, Rechenschaftspflicht, risikobasierter Ansatz)
- Zweck der KI-VO ist Innovation zu fördern (Regulatory Sandboxes)
- Risikobasierter Ansatz
- Offene Punkte:
  - Definitionen sowie Anhang I sind auslegungsbedürftig
  - Empfehlung des Europäischen Wirtschafts- und Sozialausschusses
    - Anhang I streichen
    - Umformulierung der Definition von KI-Systemen
  - Forderung klarer Kriterien zur Einstufung des Risikos (hohes – mittleres – geringes Risiko)
  - Problem: keine Abgrenzungskriterien zwischen mittlerem und geringem Risiko

# Strafen

- Art 71 KI-VO: Je nach Schwere des Verstoßes
  - 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes
  - 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes
  - 30 Millionen Euro oder 6 Prozent des weltweiten Jahresumsatzes
    - Verbotene KI-Systeme
    - Verstoß gegen Art 10 KI-VO (relevante, repräsentative, fehlerfreie und vollständige Daten)
- Festsetzung der Geldbußen abhängig von:
  - Art, Schwere und Dauer des Verstoßes und dessen Folgen
  - Auferlegung von Geldbußen für denselben Verstoß
  - Größe und Marktanteil des Akteurs



# 3. Regulatory Sandboxes

---

# Was sind Regulatory Sandboxes?

- **Herkunft & Definition:**
  - Keine fixe Definition: Reallabore, Experimentierräume, Innovationsräume, Living Labs oder Realexperimente
  - Begriffsherkunft aus IT-Bereich: Erprobung („in der Sandkiste“) von neuen, potentiell unsicheren Codes in einem abgegrenzten Rahmen
  - Vorreiter: GB, NL, POL und LTU
- **Ziel:**
  - Entwicklung, Erprobung und Validierung von technologischer Innovation vor Inverkehrbringen
  - Schaffung von gesetzlichen Freiräumen
  - Schneller, sicherer und kostengünstiger Markteintritt
  - Vermeidung von Überregulierung

# Wo sind Regulatory Sandboxes zu finden?

- **Wo werden Regulatory Sandboxes eingesetzt?**
  - Finanzbereich
  - Start-ups
  - Öffentlicher Bereich
- **2020: Einführung einer Regulatory Sandbox im FinTech-Bereich**
  - § 23a Finanzmarktaufsichtsgesetz (FMABG): Erprobung eines unvollständigen Geschäftsmodells (sog. Sandboxgeschäftsmoell) unter Rechtsbelehrung der FMA
  - Anwendungsbereich:
    - Abwicklung des Zahlungsverkehrs
    - Verhaltensbasierte Versicherungen
    - Automatisierte Anlageberatung ("robo advice")

# Ablauf Regulatory Sandbox im FinTech-Bereich

## 1. Zulassung per Bescheid:

Zulassungsantrag bei der FMA. Prüfung der Kriterien gem. § 23a Abs 2 FMABG:

- Basiert das Geschäftsmodell auf Informations- und Kommunikationstechnologie?
- Ist eine Gefährdung der Finanzmarktstabilität oder des Verbraucherschutzes zu erwarten?
- Unterliegt es der Aufsicht der FMA, ist also überhaupt eine Konzessionspflicht gegeben?
- Liegt es aufgrund seines Innovationswertes im öffentlichen Interesse?
- Ist es marktreif und testreif?

## 2. Pre-Support:

- FMA bildet ein FinTech Supervisory Team
- Persönliche Termine: Testparameter, Milestones und Zeitplan des Tests, Auflagen der Konzession

# Ablauf Regulatory Sandbox im FinTech-Bereich

## 3. Sandboxtest:

Unternehmen erbringt konzessionspflichtige oder registrierungspflichtige Dienstleistungen und wird dabei beaufsichtigt

## 4. Auswertung:

- Durchführung eines Final Reports
- Testphase wird ausgewertet
- Geschäftsmodell aus der Sandbox entlassen
- Entscheidungen über Aufhebung von Auflagen oder Einschränkungen im Konzessions- / Registrierungsbescheid
- Überführung in die reguläre Aufsicht

# Erfahrungswerte der FMA mit Regulatory Sandbox

## 1. Positive Bilanz der FMA:

- Das Interesse der Marktteilnehmer ist vielversprechend
- Neben neu gegründeten Startups nutzen auch bereits etablierte Dienstleister die Sandbox, um innovative Geschäftszweige und -modelle regulatorisch zur Marktreife zu entwickeln
- Seit 2020 hat die FMA acht FinTechs in die Sandbox aufgenommen:
  - Fünf Dienstleister streben nach Zulassung als europaweit tätiger Crowdfunding-Dienstleister
  - Drei Dienstleister beabsichtigen innovative Finanzdienstleistungen in Bezug auf Krypto-Assets und Finanzinstrumente
  - Alle acht FinTechs sind auf dem Weg zur regulatorischen Marktreife, eines hat bereits eine Wertpapierkonzession erhalten
- Durch die enge Zusammenarbeit mit den Unternehmen erhält die FMA zeitnah gute Einblicke in neueste Marktentwicklungen, wodurch sie hiermit verbundene Regelungslücken früh identifizieren und auf regulatorische Anpassungen hinwirken kann



# Erfahrungswerte der FMA mit Regulatory Sandbox

## 2. Ausblick der FMA für 2023:

Um die Regulatory Sandbox auszubauen, wird die FMA:

- sich um den Eintritt weiterer geeigneter FinTech-Unternehmen bemühen
- den laufenden Dialog und die enge Abstimmung mit dem Bundesministerium für Finanzen intensivieren (Ziel: Schaffung neuer Impulse für innovative Anbieter)
- basierend auf den Erfahrungswerten aus den ersten Verfahren die Verfahrensabläufe in der Sandbox analysieren, bewerten und optimieren
- nach Zulassung der neuen Crowdfunding-Dienstleister die Entwicklung der Crowdfunding-Plattformen aufsichtlich begleiten

# Was sind Regulatory Sandboxes im Rahmen der KI-VO

## *Artikel 53 KI-Reallabore*

- (1) KI-Reallabore, die von den zuständigen Behörden eines oder mehrerer Mitgliedstaaten oder vom Europäischen Datenschutzbeauftragten eingerichtet werden, bieten eine kontrollierte Umgebung, um die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem spezifischen Plan zu erleichtern. Dies geschieht unter direkter Aufsicht und Anleitung der zuständigen Behörden, um die Einhaltung der Anforderungen dieser Verordnung und gegebenenfalls anderer Rechtsvorschriften der Union und der Mitgliedstaaten, die innerhalb des Reallabors beaufsichtigt wird, sicherzustellen.
- (2) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu Daten gewähren oder unterstützen, sorgen die Mitgliedstaaten dafür, dass die nationalen Datenschutzbehörden und diese anderen nationalen Behörden in den Betrieb des KI-Reallabors einbezogen werden.
- (3) Die KI-Reallabore lassen die Aufsichts- und Abhilfebefugnisse der zuständigen Behörden unberührt. Alle erheblichen Risiken für die Gesundheit und Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung solcher Systeme festgestellt werden, führen zur sofortigen Risikominderung oder, falls dies nicht möglich ist, zur Aussetzung des Entwicklungs- und Erprobungsprozesses bis eine solche Risikominderung erfolgt ist.
- (4) Die am KI-Reallabor Beteiligten bleiben nach geltendem Recht der Union und der Mitgliedstaaten für Schäden haftbar, die Dritten infolge der Erprobung im Reallabor entstehen.
- (5) Die zuständigen Behörden der Mitgliedstaaten, die KI-Reallabore eingerichtet haben, koordinieren ihre Tätigkeiten und arbeiten im Rahmen des Europäischen Ausschusses für künstliche Intelligenz zusammen. Sie übermitteln dem Ausschuss und der Kommission jährliche Berichte über die Ergebnisse der Umsetzung dieser Systeme, einschließlich bewährter Verfahren, gewonnener Erkenntnisse und Empfehlungen zu deren Aufbau, sowie gegebenenfalls über die Anwendung dieser Verordnung und anderer Rechtsvorschriften der Union, die innerhalb des Reallabors kontrolliert werden.
- (6) Die Modalitäten und Bedingungen für den Betrieb der KI-Reallabore, einschließlich Genehmigungskriterien und Verfahren für die Beantragung, Auswahl, Beteiligung und für den Ausstieg aus dem Reallabor, sowie die Rechte und Pflichten der Beteiligten werden in Durchführungsrechtsakten festgelegt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

# Regulatory Sandboxes

- Bildung einer kontrollierten Umgebung
- Einhaltung der Rechtsvorschriften unter direkter Aufsicht der zuständigen Behörde
- Einbeziehung der DSB bei innovativen KI-Systemen, wenn:
  - personenbezogene Daten verarbeitet werden oder
  - Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen
- Sofortige Risikominderung oder Aussetzung des Entwicklungs- und Erprobungsprozesses bei erheblichen Risiken für die Gesundheit und Sicherheit bzw. die Grundrechte
- Zuständige Behörden müssen jährliche Berichte an Europäischen Ausschuss für künstliche Intelligenz übermitteln
- Festlegung von Modalitäten und Bedingungen für den Betrieb der KI-Reallabore in Durchführungsrechtsakten (Art 53 Abs 6 KI-VO)

# Regulatory Sandboxes

- **Haftung für Schäden im Zuge einer Regulatory Sandbox:**
  - Teilnahme bedeutet keine Immunität
  - Schadenersatzansprüche sind möglich
  - Behördlicher Schutz vor Vollstreckung bei versehentlichen Verstößen („Privileg“)?
    - Widerruf des „Privilegs“ durch Aufsichtsbehörde jederzeit möglich
    - Aufsichtsbehörde räumt idR eine gewisse Zeit zur Fehlerbehebung ein
  - Beteiligte Unternehmen haften für Schäden, die Dritten infolge der Erprobung im Reallabor entstehen

# Regulatory Sandboxes

## **Maßnahmen für Kleinanbieter und Kleinnutzer (Art 55 KI-VO):**

- Vorrangiger Zugang zu KI-Reallaboren für Kleinanbieter und Start-up-Unternehmen
- Durchführung besonderer Sensibilisierungsmaßnahmen für die Anwendung dieser Verordnung, die auf die Bedürfnisse der Kleinanbieter und Kleinnutzer ausgerichtet sind
- Einrichtung eines eigenen Kanals für die Kommunikation mit Kleinanbietern, Kleinnutzern und anderen Innovatoren zur Orientierung



# 4. Datennutzung bei Regulatory Sandboxes

---

# Datennutzung bei Regulatory Sandboxes

## Artikel 54

Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor

- (1) Im KI-Reallabor dürfen personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme im Reallabor unter folgenden Bedingungen verarbeitet werden:
  - a) die innovativen KI-Systeme werden entwickelt, um ein erhebliches öffentliches Interesse in einem oder mehreren der folgenden Bereiche zu wahren:
    - i) Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit unter der Kontrolle und Verantwortung der zuständigen Behörden, wobei die Verarbeitung auf der Grundlage des Rechts der Mitgliedstaaten oder des Unionsrechts erfolgt,
    - ii) öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Verhütung, Bekämpfung und Behandlung von Krankheiten,
    - iii) hohes Umweltschutzniveau und Verbesserung der Umweltqualität;
  - b) die verarbeiteten Daten sind für die Erfüllung einer oder mehrerer der in Titel III Kapitel 2 genannten Anforderungen erforderlich, soweit diese Anforderungen durch die Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten nicht wirksam erfüllt werden können;
  - c) es bestehen wirksame Überwachungsmechanismen, um festzustellen, ob während der Erprobung im Reallabor hohe Risiken für die Grundrechte der betroffenen Personen auftreten können, sowie Reaktionsmechanismen, um diese Risiken umgehend zu mindern und erforderlichenfalls die Verarbeitung zu beenden;
  - d) personenbezogene Daten, die im Rahmen des Reallabors verarbeitet werden sollen, befinden sich in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle der Beteiligten, und nur befugte Personen haben Zugriff auf diese Daten;
  - e) es erfolgt keine Übermittlung oder Übertragung verarbeiteter personenbezogener Daten an Dritte und auch kein anderweitiger Zugriff Dritter auf diese Daten;
  - f) eine Verarbeitung personenbezogener Daten im Rahmen des Reallabors führt zu keinen Maßnahmen oder Entscheidungen, die Auswirkungen auf die betroffenen Personen haben;
  - g) personenbezogene Daten, die im Rahmen des Reallabors verarbeitet wurden, werden gelöscht, sobald die Beteiligung an dem Reallabor beendet wird oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist;
  - h) die Protokolle der Verarbeitung personenbezogener Daten im Rahmen des Reallabors werden für die Dauer der Beteiligung am Reallabor und noch 1 Jahr nach deren Beendigung ausschließlich zu dem Zweck und nur so lange aufbewahrt, wie dies zur Erfüllung der Rechenschafts- und Dokumentationspflichten nach diesem Artikel oder anderen anwendbaren Rechtsvorschriften der Union oder der Mitgliedstaaten erforderlich ist;
  - i) eine vollständige und detaillierte Beschreibung des Prozesses und der Gründe für das Trainieren, Testen und Validieren des KI-Systems wird zusammen mit den Testergebnissen als Teil der technischen Dokumentation gemäß Anhang IV aufbewahrt;
  - j) eine kurze Zusammenfassung des im KI-Reallabor entwickelten KI-Projekts, seiner Ziele und erwarteten Ergebnisse wird auf der Website der zuständigen Behörden veröffentlicht.
- (2) Absatz 1 lässt die Rechtsvorschriften der Union oder der Mitgliedstaaten, die eine Verarbeitung für andere als die in diesen Rechtsvorschriften ausdrücklich genannten Zwecke ausschließen, unberührt.

# Datennutzung bei Regulatory Sandboxes

- KI-Systeme benötigen umfangreiche Datensätze
- Problem: Nach der DSGVO gilt der Grundsatz der Zweckbindung (Art 5 Abs 1 lit b DSGVO)
- Lösungsmöglichkeit laut KI-VO:
  - Weiterentwicklung des Zweckbindungsgrundsatzes und Öffnung iSd Wettbewerbsfähigkeit
  - Datennutzung durch KI-Systeme, die ursprünglich für andere Zwecke erhoben wurden
- Weiterverarbeitung von personenbezogenen Daten (Art 54 KI-VO)
  - Entwicklung und Erprobung von innovativen KI-Systemen im Reallabor
  - Ziel: Wahrung eines erheblichen öffentlichen Interesses
    - Öffentliche Sicherheit und öffentliche Gesundheit (Bsp: Krankheiten)
    - Verhütung oder Verfolgung von Straftaten oder Strafvollstreckung
    - Hohes Umweltschutzniveau und Verbesserung der Umweltqualität



# Datennutzung bei Regulatory Sandboxes

- Bestehen wirksamer Überwachungs- und Schutzmechanismen
  - Feststellung von hohen Risiken
  - Mechanismen, um Risiken zu minimieren
- Personenbezogene Daten in sicheren Datenverarbeitungsumgebungen (beschränkter Zugriff)
- Keine Datenübermittlung an Dritte
- Datenverarbeitung im Zuge des Reallabors hat keine Auswirkungen auf betroffene Personen
- Löschung der Daten nach Abschluss des Reallabors oder Speicherfrist
- Aufbewahrung der Prozessbeschreibung und der Ergebnisse
- Veröffentlichung einer Zusammenfassung des KI-Projekts, der Ziele und der erwarteten Ergebnisse auf der Website der zuständigen Behörde

# Where are we NOW?

- Regulatory Sandboxes sind Zukunft, DSGVO ist Gegenwart
- Breitenwirksamer Einsatz von Regulatory Sandboxes ist Zukunft, Datentestläufe sind Gegenwart
- Resultat:
  - Norwegische Datenschutzbehörde verhängte im Jahr 2021 eine Strafe iHv EUR 125.000 über die Norwegische Sportvereinigung (NIF)
  - Gründe (Auszug):
    - i. Personenbezogene Daten waren über eine öffentliche IP-Adresse zugänglich
    - ii. Dies geschah im Zuge von Testungen einer Datenmigration von einer Serverlandschaft in eine Cloudlösung
    - iii. Die Testungen geschahen ohne Risikofolgenabschätzung und ohne adäquate technisch-organisatorische Sicherheitsmaßnahmen
    - iv. Eine hinreichende Rechtsgrundlage für die Testung anhand personenbezogener Daten war nicht vorhanden; mit synthetischen Daten wäre das Auslangen zu finden gewesen

# Where are we NOW?

- Suchwort “Test“ in der DSGVO und Erwägungsgründen: „spätestens“, „weitestgehend“; aber keine „Testung“, „Testläufe“, „Testverarbeitung“, oder ähnliches
- Suchwort „synthetisch“ in der DSGVO und Erwägungsgründen: Null!
- „lessons learned“
  - Entscheidung der Norwegischen Datenschutzbehörde beruht nicht auf Text der DSGVO
  - Entscheidung beruht vielmehr auf „antizipiertem“ Datenschutzrecht
  - Essenz der Entscheidung: Nichtanwendung der Standards der KI-VO und des Konzepts der Regulatory Sandboxes
  - KI-VO kennt „Testdaten“, „Datengovernance“, „Trainingsdaten“ mitsamt (umfangreichen) Transparenz- und Sicherheitsanforderungen
  - KI-VO anerkennt die Verarbeitung personenbezogener Daten im KI-Reallabor (Regulatory Sandbox)

# Hey, Chat GPT...

... are you trained with personal data?

*“No, I am not trained with any personal data. As an artificial intelligence language model, I do not have access to any personal information or data. My training data consists of a large corpus of text from various sources, such as books, articles, and websites, but this data has been anonymized and stripped of any personal identifiers before being used to train me. Additionally, I am designed to protect the privacy and security of all interactions with users but not retaining any personal information or data that is shared with me.”*

# Hey, Chat GPT...

... but text and articles are spiked with personal data!

*“While it is true that some text and articles may contain personal data, the training data used to train me was pre-processed and anonymized to remove any personal identifiers or sensitive information. This is done to protect the privacy and security of individuals whose information may be present in the training data. Moreover, as an artificial intelligence language model, I am designed to process and analyze natural language text in away that is agnostic to any specific individual or their personal information. While I may generate responses based on patterns and trends present in the training data, I do not have access to any personal information, and I am not capable of identifying or linking specific pieces of information to any individual. Overall, my training data has been carefully curated and anonymized to ensure that no personal data is present, and my design is focused on protecting the privacy and security of individuals.”*

A blue-tinted background image featuring a classical statue's hand holding a large gear. The gear is positioned in the center, and the hand is shown from the side, gripping it. The entire scene is overlaid with a semi-transparent blue filter.

# 5. Ausblick & Thesen

---

# Ausblick

**KI-VO tritt am 20. Tag nach Veröffentlichung in Kraft**

**KI-VO gilt ab dem 24 Monat nach Inkrafttreten**

**Für bereits in Betrieb genommene KI-System gilt VO  
in bestimmten Fällen (Art 83 KI-VO)**

**2 Jahre Übergangsfrist u.U. kurz**

**Frühe Befassung mit  
KI-VO empfehlenswert**

# Thesen / Diskussionspunkte (I)

- Mit der KI-VO wird (ebenso wie mit der NIS-RL) erstmalig eine inhaltliche Regulierung von (IT-) Technologie und IT-Security vorgenommen
- Dies begründet ein Abgehen von der bislang zB im Technik- und Produktrecht geübten Praxis der *Regulated Self-Regulation*
- Regulatory Sandboxes stellen wohl keinen Ersatz für die dadurch verlorenen Freiräume dar; Eintrittsbarrieren zu hoch, regulatorische Hürden werden nur von großen Unternehmen zu erfüllen sein, gerade KMUs sind aber oft Innovatoren
- KI-VO wird eine ähnliche Relevanz erhalten wie die DSGVO heute (als die Datenschutz-RL 1995 erlassen wurde, dachte auch niemand, dass der Anwendungsbereich allumfassend werden würde)
- Der mit der KI-VO verbundene Compliance-Aufwand wird weitaus höher sein als bei der DSGVO



# Thesen / Diskussionspunkte (II)

- Wo liegen die Grenzen der Zulässigkeit umsatzbasierter Strafen (6% des Umsatzes oder 30 Mio EUR – vgl. EuGH-Judikatur zu umsatzbasierten Steuern (zB RS *Tesco*), wonach die „ability to pay“ zu berücksichtigen ist)?
- Braucht es für die Verhängung von Strafen eines zurechenbaren Handelns einer natürlichen Person?
- Konflikt mit Doppelbestrafungsverbot (i) durch Aufsichtsbehörden in mehreren Mitgliedsstaaten / (ii) durch unterschiedliche Aufsichtsbehörden (vgl. Facebook-Entscheidung des Bundeskartellamts – Datenschutzverstoß als Missbrauch einer marktbeherrschenden Stellung)?
- Ist die KI-VO ausschließlich ein Thema der Zukunft, oder ist sie bereits ein Thema des Datenschutzes der Gegenwart?
- Problemfeld: Accountability unter der DSGVO anhand der Parameter des (erst zukünftigen) Rechts der KI-VO?

# Das letzte Wort...

Hey, Chat GPT, bist Du eine gute Sache?

*“As an artificial intelligence language model, I don't have emotions or feelings, so I cannot be classified as "good" or "bad." However, I am functioning properly and available to answer any questions or provide assistance you may need.”*

**Vielen Dank für**  
*Ihre Aufmerksamkeit!*