

NUTZUNG VON KI IM FINANZSEKTOR

Thematischer Überblick: Informationsdokument der FMA zur Darstellungen des regulatorischen Rahmens betreffend die Erbringung regulierter Finanzdienstleistungen mittels Künstlicher Intelligenz im Kontext der Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz

FMA KI-Circle

Version 1.0

Stand 11.09.2026

Disclaimer: Dieses Dokument stellt keine Verordnung dar und hat keinen eigenständigen normativen Gehalt. Es soll für die beaufsichtigten Unternehmen Know-how aufbereiten und die Entwicklung eines gemeinsamen Verständnisses fördern. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Dokument nicht abgeleitet werden.

1 EXECUTIVE SUMMARY

- **Die Aufsicht betreffend die Nutzung von KI durch Finanzmarktteilnehmer ist bereits derzeit im institutionellen Zuständigkeitsbereich der FMA**
 - Der Einsatz von KI im Kontext der Erbringung regulierter Finanzdienstleistungen muss bereits derzeit den der FMA zum Vollzug übertragenen technologieneutralen Anforderungen des Finanzmarktaufsichtsrechts (bspw. sektorale Governance-, Wohlverhaltens und Vertriebsregeln sowie horizontale Anforderungen durch den Digital Operational Resilience Act, DORA) genügen.
 - Die uneingeschränkte Letztverantwortung des Leitungsorgans zum Management von IKT-Risiken umfasst sowohl die sich aus der unternehmensinternen Nutzung durch KI ergebenden IKT-Risiken sowie Änderungen des Risikoprofils bestehender IKT-Infrastruktur durch neue externe Bedrohungen (zB verstärkte Cyberangriffe unterstützt durch leistungsstarke KI-Modelle). Leitungsorganen obliegt es (bspw. iRd Business Continuity Managements und IKT-Drittanbietermanagements) Anpassungen zu veranlassen, wenn durch KI-Integration neue Abhängigkeiten entstehen.
- **Der Artificial Intelligence Act (AI Act) ist die horizontale europäische Produktregulierung für KI und tritt neben die bestehenden finanzmarktrechtlichen Anforderungen**
 - Der AI Act geht von einem risikobasierten Ansatz aus und legt spezifische Pflichten für die jeweiligen Akteure der KI-Wertschöpfungskette fest. Zur Erleichterung der praktischen Implementierung des AI Acts erlässt die Europäische Kommission (AI Office) Leitlinien.
 - Zentral ist die Abgrenzung regulierter KI-Systeme von herkömmlichen Softwaresystemen und Programmieransätzen (bspw. Systeme zur Verbesserung der mathematischen Optimierung wie z.T. Methoden der linearen / logistischen Regression) - der sachliche Anwendungsbereich des AI Act ist jeweils im Einzelfall zu prüfen.
 - Abhängig vom inhärenten Risiko des KI-Systems kann zwischen verbotenen KI-Praktiken, Hochrisiko-KI-Systemen und transparenzpflichtigen KI-Systeme unterschieden werden. In Abhängigkeit von der konkreten Ausgestaltung können Hochrisiko-KI-Systeme (auch) transparenzpflichtige KI-Systeme sein. Darüber hinaus sieht der AI Act Regelungen für KI-Modelle mit allgemeinem Verwendungszweck vor.
- **Die praktische Anwendung des AI Act im Kontext regulierter Finanzdienstleistungen erfordert regelmäßig eine materielle Prüfung anhand des Finanzmarktrechts**
 - Durch die Europäischen Aufsichtsbehörden (EBA, ESMA und EIOPA) wurden bereits umfangreiche Produkte betreffend die Interaktion von KI bzw. dem AI Act mit dem Finanzmarktrecht erarbeitet.

- Die Einstufung, ob ein KI-System eine verbotene KI-Praktik darstellt (oder z.B. ein erlaubtes Hochrisiko-KI-System) erfordert regelmäßig eine materielle Prüfung anhand des anwendbaren Finanzmarktaufsichtsrechts und Soft Law (bspw. hinsichtlich der Frage, ob es sich im Konkreten um verbotenes "Social Scoring" oder eine erlaubte Verwendung personenbezogener Finanzdaten handelt).
- Zwischen AI Act und Finanzmarktaufsichtsrecht besteht hinsichtlich der KI-Systeme die mit der Erbringung von Finanzdienstleistungen in direkten Kontakt stehen eine enge inhaltliche Verzahnung. Durch die Bezugnahme des AI Act auf sektorales Finanzmarktrecht findet z.T. eine Integration / Derogation von Bestimmungen statt.
- **Die nationale Begleit- und Umsetzungsgesetzgebung zum AI Act ist derzeit ausständig - eine unmittelbare Zuständigkeit der FMA betreffend den AI Act ist jedoch absehbar**
 - Die Mitgliedstaaten hatten bis zum 02.08.2025 die zuständigen nationalen Marktüberwachungsbehörden zum Vollzug des AI Act zu designieren - dies ist bis dato in Österreich mangels nationaler Begleit- / Durchführungsgesetzgebung nicht erfolgt.
 - Der AI Act sieht für nationale Finanzaufsichtsbehörden eine Zuständigkeit betreffend die Beaufsichtigung von Hochrisiko-KI-Systemen, die in direktem Zusammenhang mit der Erbringung regulierter Finanzdienstleistungen stehen, vor. Von dieser Regelung kann mittels Mitgliedstaatenwahlrecht abgewichen werden.
 - Die EZB ist keine AI Act Marktüberwachungsbehörde, die AI Act - Vollzugszuständigkeit obliegt daher auch hinsichtlich signifikanter Kreditinstitute (nur) nationalen Behörden.
 - Die FMA wurde bereits der Kommission als für den Schutz der Grundrechte zuständige Behörde (Art. 77 AI Act) notifiziert.
- **Zur Implementierung von KI-Systemen in Instituten, die zur Erbringung regulierter Finanzdienstleistungen berechtigt sind, bedarf es eines holistischen Ansatzes der sowohl AI Act wie auch finanzmarktrechtliche Anforderungen abbildet**
 - Es bedarf der vorausschauenden Vorbereitung angemessener Strategien, Prozesse und Verfahren jener Finanzmarktteilnehmer, die den Einsatz von KI-Systemen erwägen. Diesbezüglich sind sowohl die regulatorischen Anforderungen des Finanzmarktrechts wie auch jene des AI Act abzubilden.
 - Kenntnis bzw. aktives Monitoring der Leitlinien und Auslegungshilfen der Europäischen Aufsichtsbehörden (EBA, EIOPA, ESMA) und der Europäischen Kommission (AI Office) sowie der in Erarbeitung begriffenen einschlägigen harmonisierten Europäischen Normen wird empfohlen.
 - Die zuständigen Aufsichtsabteilungen der FMA stehen ihren Beaufsichtigten gerne für inhaltliche Fragen zur Verfügung. Der frühzeitige und aktive Dialog zwischen Beaufsichtigten und Aufsicht wird seitens der FMA proaktiv unterstützt!

INHALTSVERZEICHNIS

1	Executive Summary	2
2	Kontext & Status Quo	5
3	KI-Nutzung im Kontext des traditionellen Finanzmarktrechts	5
3.1	Exkurs: Nutzung von KI-Systemen im Kontext digitaler operativer Resilienz	7
3.2	Mapping Exercises der Europäischen Aufsichtsbehörden	10
3.2.1	EBA: AI Act implications for the EU banking and payment sector	10
3.2.2	EIOPA: Opinion on AI Governance and Risk Management	11
3.2.3	ESMA: Public statement und TRV	12
3.3	Conclusio	12
4	KI-Nutzung im Kontext produktspezifischer Regulierung durch den Artificial Intelligence Act	13
4.1	Exkurs: Nationale Zuständigkeit zum Vollzug des AI Acts	15
4.2	Definition: KI-System	15
4.2.1	Maschinengestütztes System.....	16
4.2.2	Autonomie.....	16
4.2.3	Anpassungsfähigkeit.....	16
4.2.4	Explizite / implizite Ziele von KI-Systemen.....	16
4.2.5	Ableiten	16
4.3	Risikoperspektive: Klassifikation von KI-Systemen nach Risikostufen	20
4.3.1	Verbotene KI-Praktiken (Inakzeptables Risiko)	21
4.3.2	Hochrisiko-KI-Systeme (hohes Risiko)	22
4.3.3	Grenze zwischen verbotenen KI-Praktiken und Hochrisiko-KI-Systemen.....	24
4.3.4	Transparenzpflichten (begrenztes Risiko / Transparenzrisiko)	28
4.4	Akteur-Perspektive	29
4.4.1	Im Überblick: Anforderungen an den Betrieb von Hochrisiko-KI-Systemen.....	29
4.4.2	Übersicht spezifischer Anbieterpflichten	30
4.4.3	Übersicht spezifischer Betreiberpflichten.....	31
4.4.4	Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme	31
4.4.5	Strafbestimmung.....	31

2 KONTEXT & STATUS QUO

Die FMA ist Österreichs unabhängige, weisungsfreie und integrierte Aufsichts- und Abwicklungsbehörde. Als integrierte Behörde umfasst der institutionelle Aufgabenbereich der FMA gemäß § 1 f FMABG¹ den gesamten österreichischen Finanzmarkt. In dieser Funktion obliegt ihr der Vollzug von sektorübergreifendem und -spezifischem Finanzmarktrecht. Absehbar wird hierzu auch die technologiespezifische **Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz** (*Artificial Intelligence Act, AI Act*)² zählen.

Aufgrund der rapiden fortschreitenden Entwicklung und zunehmend verbreiteten Nutzung von Künstlicher Intelligenz (KI) ergeben sich grundlegende aufsichtsrechtliche Fragen für beaufsichtigte Institute. Zielsetzung dieser Publikation ist es daher, einschlägige **Informationen strukturiert aufzubereiten**, die **Aufsichtssubjekte der FMA bei der Vorbereitung auf die Anforderungen des AI Act zu unterstützen** sowie die **Interaktion mit bestehendem Finanzmarktrecht** darzustellen. Dies umfasst einerseits die systematische Darstellung der neuen regulatorischen Vorgaben sowie andererseits die Verdeutlichung ihrer Wechselwirkungen mit dem bestehenden sektoralen Aufsichtsrecht. Dieses Dokument stellt keine Verordnung dar und hat keinen eigenständigen normativen Gehalt. Es soll für die beaufsichtigten Unternehmen Know-how aufbereiten und die Entwicklung eines gemeinsamen Verständnisses fördern. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Dokument nicht abgeleitet werden.

3 KI-NUTZUNG IM KONTEXT DES TRADITIONELLEN FINANZMARKTRECHTS

Finanzmarktrecht ist, sofern durch den Gesetzgeber keine anderslautende Regelung getroffen wird, grundsätzlich technologieneutral. Die Einhaltung der aufsichtlichen Anforderungen ist daher - unabhängig von der genutzten Technologie - durch das beaufsichtigte Institut sicherzustellen. Die Möglichkeiten und Modalitäten zur Nutzung von KI im Anwendungsbereich einschlägiger finanzmarktrechtlicher Bestimmungen sind daher materiell an diesen zu messen. Auch ohne eine produktspezifische Regulierung von KI unterliegen solche Systeme daher bereits gegenwärtig den technologieneutral formulierten Verpflichtungen des bestehenden Finanzmarktrechts.

¹ Bundesgesetz über die Errichtung und Organisation der Finanzmarktaufsichtsbehörde (*Finanzmarktaufsichtsgesetz – FMABG*), BGBl. I Nr. 97/2001 idF BGBl. I Nr. 5/2026.

² *Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABl. Nr. L 2024/1689 vom 12.07.2024, idF der Berichtigung ABl. Nr. L 2025/90802 vom 09.10.2025.*

Beispiel: Vertrieb von Versicherungsprodukten im KI-Kontext

Die Richtlinie (EU) 2016/97 über Versicherungsvertrieb (*Insurance Distribution Directive, IDD*)³ legt in Art. 17 Abs. 1⁴ fest, dass Versicherungsvertrieber bei ihrer Versicherungsvertriebstätigkeit gegenüber ihren Kunden stets ehrlich, redlich und professionell in deren bestmöglichem Interesse zu handeln haben. Diese rechtliche Anforderung ist unabhängig von der im Versicherungsvertrieb eingesetzten Technologie zu erfüllen. Die *EIOPA Opinion on AI Governance and Risk Management*⁵ legt fest, wie den gegenständlichen Anforderungen der IDD im Kontext der Nutzung von KI entsprochen werden kann. Rz. 3.13 ff der *Opinion on AI Governance and Risk Management* gibt einen Überblick über unterschiedliche Gesichtspunkte, an die zur Einhaltung der Vertriebsvorschriften angeknüpft werden kann (u.a. "human oversight", "data governance", "explainability" und "metrics"). Darüber hinaus wird festgehalten, dass hinsichtlich sog. "differential pricing practices" auch im KI-Kontext die aufsichtlichen Erwartungshaltungen des *EIOPA Supervisory statement on differential pricing practices in non-life insurance lines of business*⁶ zu beachten sind.

Beispiel: Anlageberatung zu Finanzinstrumenten durch KI

§ 48 WAG 2018⁷ normiert, dass dem Regulierungsrahmen unterliegende Rechtsträger (bspw. Kreditinstitute oder Wertpapierfirmen) Kunden rechtzeitig vor der Beratung darüber zu informieren haben, ob die Beratung "unabhängig" erfolgt. Weiters sind Informationen im Hinblick auf das einbezogene Produktuniversum und ob eine regelmäßige Eignungsbeurteilung durchgeführt wird, zu erteilen. Diese Anforderung besteht unabhängig von der technischen Ausgestaltung der Dienstleistung: Sie gilt für persönliche Beratung durch einen Menschen genauso wie einen "Robo-Advisor". Ebenso technologieneutral gilt der übrige relevante Conduct-Regulierungsrahmen, wie die Pflichten zum Handeln im besten Interesse des Kunden gemäß

³ Richtlinie (EU) 2016/97 über Versicherungsvertrieb (*Insurance Distribution Directive, IDD*), ABl. Nr. L 26 vom 02.02.2016 S. 19, idF der DelVO (EU) 2024/896 zur Änderung der Richtlinie (EU) 2016/97 durch technische Regulierungsstandards zur Anpassung der Grundbeträge in Euro für die Berufshaftpflichtversicherung und die finanzielle Leistungsfähigkeit von Versicherungsvermittlern, Rückversicherungsvermittlern und Versicherungsvermittlern in Nebentätigkeit, ABl. Nr. L 2024/896 vom 20.03.2024.

⁴ Die gegenständliche Richtlinienbestimmung wurde in Österreich in § 128 Abs. 1 Versicherungsaufsichtsgesetz 2016 (VAG 2016), BGBl. I Nr. 34/2015, idF BGBl. I Nr. 6/2026, umgesetzt.

⁵ EIOPA, *Opinion on AI Governance and Risk Management*, 06.08.2025, EIOPA-BoS-25-360, Rz. 3.12, abrufbar unter: www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en (zuletzt abgerufen am 31.07.2026).

⁶ EIOPA, *Supervisory statement on differential pricing practices in non-life insurance lines of business*, 22.02.2023, EIOPA-BoS-23/076, abrufbar unter: www.eiopa.europa.eu/system/files/2023-03/EIOPA-BoS-23-076-Supervisory-Statement-on-differential-pricing-practices_0.pdf (zuletzt abgerufen am 31.07.2026).

⁷ Wertpapieraufsichtsgesetz 2018 (WAG 2018), BGBl. I Nr. 107/2017, idF BGBl. I Nr. 5/2026.

§§ 47 ff WAG 2018. Im Gegensatz dazu bezieht sich § 55 WAG 2018 auf "natürliche Personen", die eine Anlageberatung erbringen und ist damit nicht technologieneutral formuliert.

Speziell zum Thema "Robo-Advice" und damit technologieneutrale Bestimmungen in diesem Kontext konkretisierend, wurden Anforderungen an (semi-)automatisierte Systeme zur Erbringung der Anlageberatung und Portfolioverwaltung durch ESMA u.a. in den ESMA-Leitlinien zu einigen Aspekten der MiFID II-Anforderungen an die Geeignetheit⁸ dargestellt. Diese umfassen bspw. Erläuterungen zum System und dem Grad der Involvierung und Kontrolle natürlicher Personen im Prozess.

3.1 EXKURS: NUTZUNG VON KI-SYSTEMEN IM KONTEXT DIGITALER OPERATIONALER RESILIENZ

Neben dem sektoralen Finanzmarktrecht ergeben sich auch Überschneidungen mit sektorübergreifendem Aufsichtsrecht, insb. der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (*Digital Operational Resilience Act, DORA*)⁹. Gegenstand der DORA ist jedoch im Gegensatz zum AI Act nicht die produktbezogene Regulierung von KI, sondern die Festlegung des aufsichtlichen Rechtsrahmens betreffend IKT-Risiken, Betriebsstabilität und digitale operationelle Resilienz. KI-Systeme im Sinne des AI Acts sind in diesem Zusammenhang insb. als Teil der von DORA erfassten Netzwerk- und Informationssysteme von Relevanz.¹⁰

DORA untergliedert sich insbesondere in vier regulatorische Blöcke, welche in unterschiedlicher Ausprägung auch das Design, den Betrieb und die Nutzung von KI-Systemen von Finanzmarktteilnehmern determinieren:

- **IKT-Risikomanagement;**
- **Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle;**
- **Testen der digitalen operationalen Resilienz;**
- **Management des IKT-Drittparteienrisikos.**

Eine detaillierte Darstellung der Berührungspunkte würde den gegenständlichen Rahmen deutlich

⁸ ESMA, Leitlinien zu einigen Aspekten der MiFID II-Anforderungen an die Geeignetheit, 03.04.2023, ESMA35-43-3172, abrufbar unter: www.esma.europa.eu/sites/default/files/2023-04/ESMA35-43-3172_Guidelines_on_certain_aspects_of_the_MiFID_II_suitability_requirements_DE.pdf (zuletzt abgerufen am 31.07.2026).

⁹ Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (*Digital Operational Resilience Act, DORA*), ABl. Nr. L 333 vom 27.12.2022 S. 1, idF der Berichtigung ABl. L 2024/90822 vom 19.12.2024.

¹⁰ Vgl. BaFin, Orientierungshilfe zu IKT Risiken beim Einsatz von KI in Finanzunternehmen, abrufbar unter: www.bafin.de/SharedDocs/Downloads/DE/Anlage/neu/dl_Anlage_orientierungshilfe_IKT_Risiken_bei_KI.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 31.07.2026).

übersteigen, zur Illustration der Querschnittsmaterie ist jedoch exemplarisch auf folgende Themenkomplexe hinzuweisen:

- Art. 5 Abs. 2 Bst. a DORA definiert die *Letztverantwortung des Leitungsorgans* hinsichtlich des Managements der IKT-Risiken des Finanzunternehmens. Der Grundsatz der **uneingeschränkten und letztlichen Verantwortung des Leitungsorgans** für das Management der IKT-Risiken bedingt im Kontext der sich **aus der Nutzung von KI ergebenden IKT-Risiken**, dass diese eine zentrale und aktive Rolle beim Management und der Anpassung des IKT-Risikorahmen einzunehmen und für eine adäquate Ressourcenausstattung Sorge zu tragen haben.¹¹ Entscheidungen zum Einsatz von (insb.) nicht-deterministischen KI-Systemen für die Erbringung regulierter Finanzdienstleistungen österreichischer Institute sind informiert und unter Einbindung des Leitungsorgans zu treffen.¹²
- Um sachlich fundierte Entscheidungen betreffend die sich aus der Nutzung von KI ergebenden IKT-Risiken oder neue, durch KI-Systeme bedingte Bedrohungslagen treffen zu können, bedarf es adäquater unternehmensinterner Kompetenzen. Zur Sicherstellung eines dem IKT-Risikoprofil und dem Grundsatz der Verhältnismäßigkeit entsprechenden Know-hows sind gemäß DORA *laufende Schulungsprogramme* für Mitarbeiter, IKT-Drittdienstleister und insb. auch für Leitungsorgane (vgl. Art. 5 Abs. 4 DORA) einzurichten.
- KI bedingte IKT-Risiken sind im IKT-Risikomanagementrahmens gemäß Art. 6 DORA abzubilden und damit ein *Teil des Gesamtrisikomanagementsystems*. In diesem Kontext sind auch spezifische, durch den Einsatz von KI-Systemen bedingte IKT-Risiken angemessen zu berücksichtigen. Dies umfasst exemplarisch die Überwachung von Modelldrift¹³, Angriffsversuche auf Training oder Prompts¹⁴, Prüfung ob das implementierte Berechtigungskonzept für Nutzer auch beim Zugriff auf Unternehmensdaten durch KI-Systeme beachtet wird, etc.
- Die vollständige *Identifikation aller im Unternehmen im Einsatz befindlichen KI-Assets* als Teil der IKT-Assets (vgl. Art. 6 Abs. 2 DORA) ist die Basis, um diese angemessen zu schützen. Bei KI-Systemen stellt dies durch die inhärente Komplexität oftmals eine spezielle Herausforderung dar, da diese in der Regel aus unterschiedlichsten Assets bestehen (z.B. Trainingsdatensätze, RAG-Datenbanken¹⁵, GPU-Infrastruktur, API-Schnittstellen zu anderen Systemen, diverse vor- und nachgeschaltete Tools, udgl). In diesem Zusammenhang ist insbesondere auf die

¹¹ Vgl. ErwG. 45 f DORA.

¹² Anm.: In Instituten, in denen ein Aufsichtsrat eingerichtet ist, empfiehlt sich zur Sicherstellung der effektiven Wahrnehmung der gesetzlich vorgesehenen Überwachungsfunktion dessen proaktive Einbindung.

¹³ Anm.: Zur Erklärung siehe bspw. Stanford University, What is Model Drift?, abrufbar unter: <https://hai.stanford.edu/ai-definitions/what-is-model-drift> (zuletzt abgerufen am 31.07.2026).

¹⁴ Anm.: Zur Erklärung siehe bspw. Stanford University, What is Prompt Injection?, abrufbar unter: <https://hai.stanford.edu/ai-definitions/what-is-prompt-injection> (zuletzt abgerufen am 31.07.2026).

¹⁵ Anm.: Zur Erklärung siehe bspw. Stanford University, What is RAG (Retrieval-Augmented Generation)?, abrufbar unter: <https://hai.stanford.edu/ai-definitions/what-is-rag> (zuletzt abgerufen am 31.07.2026).

Anforderungen der Delegierte Verordnung (EU) 2024/1774¹⁶ zum Management von IKT-Assets (Art. 4 und 5 der Delegierte Verordnung (EU) 2024/1774) sowie zur IKT-Betriebssicherheit (Art. 8 ff der Delegierte Verordnung (EU) 2024/1774) hinzuweisen.¹⁷

- Weitere Berührungspunkte mit DORA ergeben sich insbesondere im *Drittparteienmanagement*, welches im Kontext der Nutzung von KI eine besondere Herausforderung darstellt, wie im nachfolgenden Beispiel illustriert wird.

Beispiel: Cyberbedrohungen und -absicherung durch Frontier-AI Modelle

Im April 2026 veröffentlichte das AI-Security Institute der britischen Regierung das Testergebnis einer neuen Generation von KI-Modellen, die nun fähig waren, komplexe Cyberangriffe selbstständig durchzuführen und Schwachstellen in IKT-Lösungen besser als je zuvor aufzudecken.¹⁸ Für Finanzinstitute ergeben sich daraus zwei unmittelbare Konsequenzen:

Erstens steigt die Angriffsfläche dramatisch, da auch weniger qualifizierte Angreifer durch den Einsatz von Frontier-KI-Modellen komplexe Angriffe auf die Softwareinfrastruktur von Finanzinstituten durchführen und Sicherheitslücken entdecken können.

Zweitens bieten dieselben Modelle gleichzeitig die Möglichkeit, die eigene Verteidigungsfähigkeit erheblich zu verbessern – sofern die Finanzinstitute diese gezielt und dem Rechtsrahmen entsprechend einsetzen. Die eigene Verteidigungsfähigkeit kann beispielsweise durch KI-basierte Qualitätsprüfungen von selbst erstellten Software Quellcode erhöht werden. In diesem Kontext gilt es abzuwägen, ob die neuesten KI-Modelle, die ausschließlich von kommerziellen Cloud-Providern angeboten werden, dazu genutzt werden sollen, oder diese Möglichkeit bewusst nicht in Anspruch genommen wird - in beiden Fällen bestehen erhebliche IKT-Risiken: Im ersten Fall wird Cloud-Providern vertraulicher Quellcode des Finanzinstituts offengelegt. Im zweiten Fall können möglicherweise entscheidende Sicherheitslücken nicht gefunden werden.

Mögliche Strategien zur Risikomitigierung können in diesem Kontext bspw. hybride Ansätze bieten: Vertraulicher unternehmensinterner Quellcode wird durch lokal betriebene KI-Modelle getestet, in Verwendung befindlicher Open Source Quellcode wird durch leistungsfähige, extern betriebene KI-Modelle geprüft.

¹⁶ *Delegierte Verordnung (EU) 2024/1774 zur Ergänzung der Verordnung (EU) 2022/2554 durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens*, ABl. L 2024/1774 vom 25.06.2024 idF der Berichtigung ABl. L 2025/90420 vom 15.05.2025.

¹⁷ Anm.: Es bedarf daher insb. der eindeutigen Kennung jedes IKT-Assets, der klaren Festlegung der Identität der Eigentümer von IKT-Assets, die Unternehmensfunktionen oder -dienstleistungen, die durch das IKT-Asset unterstützt werden udgl.

¹⁸ AISI, *Our evaluation of Claude Mythos Preview's cyber capabilities*, 13.04.2026, abrufbar unter: <https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities> (zuletzt abgerufen am 31.07.2026)

Basis derartiger strategischer Entscheidungen und deren konkreter Umsetzung im IKT-Risikomanagement ist eine umfassende Datenklassifizierung.

3.2 MAPPING EXERCISES DER EUROPÄISCHEN AUFSICHTSBEHÖRDEN

Zur Schaffung eines besseren Verständnisses betreffend die Auswirkungen des AI Acts auf das sektorale Aufsichtsrecht erfolgten bereits umfangreiche Arbeiten der Europäischen Aufsichtsbehörden (*European Supervisory Authorities, ESAs*)¹⁹:

3.2.1 EBA: AI ACT IMPLICATIONS FOR THE EU BANKING AND PAYMENT SECTOR²⁰

Die EBA fokussierte sich bei ihrem Abgleich auf Hochrisiko-KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden (daher Hochrisiko-KI-Systeme gemäß Art. 6 Abs. 2 iVm Anhang III Abs. 5 Buchstabe c AI Act). Das Ergebnis des Assessments fiel differenziert aus:

- **"Fully aligned"**: Nur ein Bruchteil der AI Act - Anforderungen ist bereits in identer Weise durch einen finanzmarktrechtlichen Rechtsakt abgedeckt. Konkret wurde ein derartiges Alignment nur bezüglich des in Art. 86 AI Act stipulierten Rechts auf Erläuterung der Entscheidungsfindung im Einzelfall betreffend Hochrisiko-KI-Systeme des Anhangs III AI Act im Vergleich zum Rechtsrahmen der Richtlinie (EU) 2023/2225²¹ festgestellt.²²
- **"Partially aligned"**: Bei einem vergleichsweise kleinen Teil der Verpflichtungen aus dem AI Act reguliert der finanzmarktrechtliche Rechtsrahmen ähnliche Sachverhalte, jedoch bestehen Unterschiede hinsichtlich des Anwendungsbereichs, der Terminologie oder der Umsetzungsanforderungen. Dies betrifft beispielsweise die Anforderungen an die Genauigkeit, Robustheit und Cybersicherheit gemäß Art. 15 AI Act im Vergleich zur DORA. Darüber hinaus bestehen Schnittmengen zwischen AI Act und den EBA-Leitlinien für die

¹⁹ Hierbei handelt es sich um die Europäischen Aufsichtsbehörden als Teil des Europäischen Finanzaufsichtssystems (*European System of Financial Supervision, ESFS*). Das sind die Europäische Bankenaufsichtsbehörde (*European Banking Authority, EBA*), die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (*European Insurance and Occupational Pensions Authority, EIOPA*) sowie die Europäische Wertpapier- und Marktaufsichtsbehörde (*European Securities and Markets Authority, ESMA*).

²⁰ EBA, AI Act: Implications for the EU banking and payments sector, abrufbar unter: eba.europa.eu/sites/default/files/2025-11/d8b999ce-a1d9-4964-9606-971bbc2aaf89/AI%20Act%20implications%20for%20the%20EU%20banking%20sector.pdf (zuletzt abgerufen am 31.07.2026).

²¹ Richtlinie (EU) 2023/2225 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 2008/48/EG (*Consumer Credit Directive, CCD*), ABl. Nr. L 2023/2225 vom 30.10.2023.

²² Vgl. Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz / Research Institute (RI) – Digital Human Rights Center, Das Recht auf Erklärung im AI Act - Leitfaden für Unternehmen, 2025, abrufbar unter: www.sozialministerium.gv.at/dam/sozialministeriumat/Anlagen/Services/Studien/Final_Aufkl%C3%A4rung-4.0_Unternehmensleitfaden_April2025_2026-01-22.pdf (zuletzt abgerufen am 31.07.2026), sowie Aufklärung 4.0 – Entscheidungen der KI als Mensch verstehen: Bericht über die theoretischen Grundlagen des Rechts auf Erläuterung der Entscheidungsfindung im Einzelfall nach Artikel 86 AI Act, 28.02.2025, abrufbar unter: www.sozialministerium.gv.at/dam/jcr:53b900a6-8630-4c96-8ddc-d4b4a0893447/Final_Aufkl%C3%A4rung_4.0_Grundlagenbericht_April2025_2026-01-28.pdf (zuletzt abgerufen am 31.07.2026). Die gegenständlichen Publikationen behandeln als Use Cases u.a. die Preisbildung betreffend Lebens- und Krankenversicherungen sowie Bonitätsprüfungen, enthalten Musterformulare zur Umsetzung des Rechtsanspruchs bzw. der ordnungsgemäßen Beauskunftung von Anfragen gemäß Art. 86 AI Act und sind ebenso in englischer Sprache verfügbar.

Kreditvergabe und Überwachung²³ sowie für Institute mit IRB-Ansatz²⁴ zur Berechnung des Kreditrisikos.

- **"Complementary"**: Ein großer Teil der AI Act-Verpflichtungen befasst sich mit Themenkomplexen, welche ebenso in bestehende Anforderungen des Finanzdienstleistungsrechts abgebildet sind, durch den AI Act kommen jedoch neue regulatorische Dimensionen bzw. Ziele hinzu. An dieser Stelle ist beispielhaft das im AI Act vorgesehene Risikomanagement-Rahmenwerk (vgl. Art. 9 AI Act) betreffend Hochrisiko-KI-Systeme zu nennen.²⁵
- **"Not present in Financial Services Law"**: Der Verpflichtung aus dem AI Act steht keine entsprechende vergleichbare Bestimmung des finanzmarktrechtliche Rechtsrahmens gegenüber. Dies betrifft u.a. die gemäß Art. 27 AI Act erforderliche Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme (*Fundamental Rights Impact Assessment, FRIA*).

Die durch die EBA durchgeführte Erhebung stellt für sich keine unmittelbare aufsichtliche Guidance betreffend den Einsatz von KI im Bankensektor und Zahlungsverkehr dar, ist jedoch als Produkt geeignet Kredit- und Finanzinstituten die Einordnung der unmittelbaren Betroffenheit zu erleichtern.

3.2.2 EIOPA: OPINION ON AI GOVERNANCE AND RISK MANAGEMENT

Die EIOPA veröffentlichte Guidance zur Auslegung von sektoralem Aufsichtsrecht im Kontext von KI-Systemen, unter Ausnahme von verbotenen Praktiken im KI-Bereich (Art. 5 AI Act) sowie Hochrisiko-KI-Systemen (Art. 6 AI Act).²⁶ Sie enthält aufsichtsrechtliche Erwartungshaltungen in Bezug auf Governance- und Risikomanagementsysteme, die Unternehmen nach einem risikobasierten und verhältnismäßigen Ansatz entwickeln sollten, um einen verantwortungsvollen Einsatz von KI-Systemen sicherzustellen.²⁷

²³ EBA, Leitlinien für die Kreditvergabe und Überwachung, 29.05.2020, EBA/GL/2020/06, abrufbar unter: www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/Translations/886677/Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring_COR_DE.pdf (zuletzt abgerufen am 31.07.2026).

²⁴ Anm.: Hierbei handelt es sich um den Internal Ratings Based Approach (IRB Approach), siehe FMA, Glossar: IRB-Ansatz zur Berechnung des Kreditrisikos, abrufbar unter: www.fma.gv.at/glossar/irb-ansatz-zur-berechnung-des-kreditrisikos/ (zuletzt abgerufen am 31.07.2026).

²⁵ In diesem Zusammenhang ist anzumerken, dass der Risikobegriff des AI Act (als produktbezogene Regulierung) ein produktspezifischer ist und demnach die konkrete unternehmensinterne Umsetzung im Risikomanagement diesem Umstand Rechnung zu tragen hat.

²⁶ EIOPA, Opinion on AI Governance and Risk Management, EIOPA-BoS-25-360, Rz. 2.6.

²⁷ EIOPA, Opinion on AI Governance and Risk Management, EIOPA-BoS-25-360, Rz. 2.9.

3.2.3 ESMA: PUBLIC STATEMENT UND TRV

Die ESMA veröffentlichte bereits 2024 das *Public Statement: On the use of Artificial Intelligence (AI) in the provision of retail investment services*.²⁸ Diese Veröffentlichung verfolgt den Zweck als erste Orientierungshilfe für Unternehmen zu dienen, welche regulatorischen Anforderungen der Richtlinie 2014/65/EU über Märkte für Finanzinstrumente (*Markets in Financial Instruments Directive II, MiFID II*)²⁹ im Kontext der Nutzung von KI insbesondere von Relevanz sind. Durch die ESMA werden in diesem Zusammenhang insb. folgende Themenbereiche hervorgehoben: "Client Best Interest and Information to clients", "Organisational requirements – Governance, Risk Management, Knowledge and competence and Staff training", "Conduct of business requirements" und "Record Keeping".³⁰ Die ESMA wies weiters auf die inhärenten Risiken³¹ beim Einsatz von KI-Systemen hin.

Neben der aufsichtlichen Guidance befasst sich die ESMA fortlaufend mit der Marktentwicklung und dem Einsatz von KI-Systemen. Diese Entwicklungen werden im Rahmen ihrer Tätigkeiten zur Förderung der Transparenz, Robustheit und Verlässlichkeit der Finanzmärkte und insb. im ESMA *Report on Trends, Risks and Vulnerabilities* (TRV) berücksichtigt.³²

3.3 CONCLUSIO

KI ist bereits derzeit durch das traditionelle Finanzmarktrecht (mit)reguliert - reguliert wird jedoch oft ein anderer Gesichtspunkt:

Überschneidungen mit dem sektoralen Aufsichtsrecht bestehen bspw. hinsichtlich der finanzmarktrechtlichen Vorschriften betreffend Governance (insbesondere Risikomanagement), Vertriebsvorschriften aber auch hinsichtlich des auf Finanzmarktteilnehmer anwendbaren Rechtsrahmens zur digitalen Resilienz. Der Blickwinkel des AI Acts als KI-spezifisches Produktregulierungsrahmenwerk unterscheidet sich jedoch vom Blickwinkel des traditionellen sektoralen Finanzmarktaufsichtsrecht und ergänzt dieses um weitere regulatorische Dimensionen bzw. Ziele. Telos des aufsichtlichen Rechtsrahmens ist regelmäßig die

²⁸ ESMA, *Public Statement: On the use of Artificial Intelligence (AI) in the provision of retail investment services*, 30.05.2024, ESMA35-335435667-5924, abrufbar unter: https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdf (zuletzt abgerufen am 31.07.2026).

²⁹ Richtlinie 2014/65/EU über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (*Markets in Financial Instruments Directive II, MiFID II*), ABl. Nr. L 173 vom 12.06.2014 S. 349, idF der Richtlinie (EU) 2024/2811 zur Änderung der Richtlinie 2014/65/EU über Märkte für Finanzinstrumente, ABl. Nr. L 2024/2811 vom 14.11.2024.

³⁰ ESMA, *Public Statement: On the use of Artificial Intelligence (AI) in the provision of retail investment services*, ESMA35-335435667-5924, Rz. 6 ff.

³¹ ESMA, *Public Statement: On the use of Artificial Intelligence (AI) in the provision of retail investment services*, ESMA35-335435667-5924, Rz. 5; diese betreffen u.a. algorithmischen Bias/Verzerrungen, Datenqualitätsprobleme, die potentiell undurchsichtige Entscheidungsfindung von Mitarbeitern sowie Herausforderungen betreffend (Daten-)Sicherheit und Datenschutz.

³² Vgl. bspw. ESMA, *TRV Risk Analysis, AI adoption and trends in securities markets: EU evidence*, 20.02.2026, ESMA50-481369926-30599, abrufbar unter: www.esma.europa.eu/sites/default/files/2026-02/ESMA50-481369926-30599_TRV_Risk_Analysis_AI_adoption_and_trends_in_securities_markets.pdf (zuletzt abgerufen am 31.07.2026).

Sicherstellung der finanziellen Stabilität von Finanzmarktteilnehmern, die professionelle Interaktion mit Kunden und die Mitigierung von Informationsasymmetrie. Der Wesenskern des produktspezifischen KI-Regulierungsrahmens ist hingegen die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von menschenzentrierter und vertrauenswürdiger Künstlicher Intelligenz zu fördern und ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und der in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte sicherzustellen.

Hierdurch ergeben sich unterschiedliche regulatorische Perspektiven - Bestimmungen des AI Acts können im Ergebnis inhaltlich selbstständig neben sektoralen finanzmarktrechtlichen Bestimmungen stehen oder von diesen derogiert / in diese integriert werden.³³

4 KI-NUTZUNG IM KONTEXT PRODUKTSPEZIFISCHER REGULIERUNG DURCH DEN ARTIFICIAL INTELLIGENCE ACT

Der AI Act gehört zum Bereich der Produktregulierung und regelt Wirtschaftssektor-übergreifend, welche Anforderungen ein KI-System je nach Risikoklasse, bestimmungsgemäßem Verwendungszweck und Rolle in der KI-Wertschöpfungskette erfüllen muss, bevor es in Verkehr gebracht, in Betrieb genommen oder verwendet wird. Neben der rechtlichen **Konkretisierung durch delegierte Rechtsakte** (vgl. Art. 97 AI Act) und durch das AI Office der Europäischen Kommission erlassene Soft Law - Instrumente (**Leitlinien**, vgl. Art. 96 AI Act) erfolgt die technische Konkretisierung durch **harmonisierte Europäische Normen** (hEN), die derzeit auf Basis eines Normungsauftrags der Europäischen Kommission durch CEN und CENELEC ausgearbeitet werden.³⁴ Die Anwendung harmonisierter Normen ist im Regelfall freiwillig, deren Anwendung löst jedoch eine Konformitätsvermutung aus (Beweislastumkehr; vgl. Art. 40 ff bzw. ErwG. 121 AI Act). Von daher kommt den **harmonisierten Europäischen Normen** eine **hohe praktische Bedeutung** zu. Darüber hinaus geben Praxisleitfäden (vgl. Art. 56 AI Act) und Verhaltenskodizes (vgl. Art. 95 AI Act) weitere Guidance für Akteure der KI-Wertschöpfungskette.

³³ Vgl. Darstellung der EBA betreffend der Interaktion von Bestimmungen des Finanzmarktrechts mit dem AI Act in EBA, *AI Act: Implications for the EU banking and payments sector*, S. 3.

³⁴ Vgl. RTR (KI-Servicestelle), Begleitgesetzgebung, abrufbar unter <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/erg-leitlinien-und-dokumente.de.html> (zuletzt abgerufen am 31.07.2026), EK (Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU), Normen in Europa, abrufbar unter: europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_de.htm (zuletzt abgerufen am 31.07.2026) sowie DIN e.V., Die Rolle von europäischen Normen, abrufbar unter: www.din.de/de/forschung-und-innovation/themen/kuenstliche-intelligenz/ai-act/rolle-von-europaeischen-normen-beim-ai-act (zuletzt abgerufen am 31.07.2026).

Inhaltlich können die regulatorischen Anforderungen des AI Acts insb. aus den folgenden Perspektiven betrachtet werden, welche der weiteren Struktur dieser Publikation zugrunde gelegt wurden:

- **Risikoperspektive:** Risikobasierte Klassifizierung von KI-Systemen und daran anknüpfend abgestufte regulatorische Anforderungen für diese;
- **Akteur-Perspektive:** Unterschiedliche Anforderungen je nach Position des jeweiligen Akteurs in der KI-Wertschöpfungskette.

Weiters ist noch zwischen **KI-Modellen**³⁵, insb. KI-Modellen mit allgemeinem Verwendungszweck (*General Purpose AI, GPAI*) gemäß Art. 3 Z 63 AI Act, **und KI-Systemen** gemäß Art. 3 Z 1 AI Act zu unterscheiden (siehe Punkt 4.2).

Durch den Vorschlag der Europäischen Kommission betreffend eine **Digital-Omnibus-Verordnung zur KI**³⁶ wurden Änderungen im produktspezifischen Regulierungsrahmen des AI Acts vorgenommen.³⁷ Neben inhaltlichen Anpassungen³⁸ wurde insbesondere die Anwendbarkeit des Regelungsrahmens für folgende Themenbereiche verschoben:

- Hochrisiko-KI-Systeme des Anhangs III AI Act (von bisher 02.08.2026) auf 02.12.2027;
- Regulatorische Reallabore (von bisher 02.08.2026) auf 02.12.2027;
- Transparenzpflichten gemäß Art. 50 Abs. 2 AI Act, sofern das KI-System vor dem 02.08.2026 in Verkehr gebracht wurde, auf den 02.12.2026.

In diesem Zusammenhang ist darauf hinzuweisen, dass trotz der Verschiebung des produktspezifischen Regulierungsrahmens für KI im finanzmarktrechtlichen Kontext verwendete KI-Systeme auch vor der (vollständigen) Anwendbarkeit des AI Act den technologieneutralen Anforderungen des Finanzmarktrechts genügen müssen, wenn diese im Rahmen der Erbringung regulierter Finanzdienstleistungen eingesetzt werden.

³⁵ Vgl. Art. 51 ff AI Act hinsichtlich des Regelungsrahmens für KI-Modelle mit allgemeinem Verwendungszweck und der diesbezüglichen Zuständigkeit der EK.

³⁶ Vorschlag für eine Verordnung zur Änderung der Verordnungen (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (*Digital-Omnibus-Verordnung zur KI*), COM/2025/836 final. In diesem Kontext ist insb. auf den potentiellen Aufschub der Anwendbarkeit des Rechtsrahmens für Hochrisiko-KI-Systeme gemäß Art. 6 Abs. 2 iVm Anhang III AI Act hinzuweisen.

³⁷ Vgl. Europäisches Parlament, Pressemitteilung zur Digital Omnibus Trilog-Einigung, abrufbar unter: [AI Act: deal on simplification measures, ban on "nudifier" apps | News | European Parliament](#) (zuletzt abgerufen am 31.07.2026).

³⁸ Anm.: Die inhaltlichen Änderungen umfassen ua: Neue verbotene KI-Praktiken, Anpassungen am Rechtsrahmen für Hochrisiko-KI-Systeme gemäß Art. 2 Abs. 1 i m Anhang I AI Act, Erweiterung der Zuständigkeiten des AI Office (Marktüberwachungsbehörde betreffend KI-Systeme die auf KI-Modellen mit allgemeinem Verwendungszweck aufbauen) sowie Änderungen bei rechtlichen Anforderungen (Ausweitung der Erleichterungen für kleine und mittlere Unternehmen auf kleine Midcap-Unternehmen) und innovationsfördernden Maßnahmen.

4.1 EXKURS: NATIONALE ZUSTÄNDIGKEIT ZUM VOLLZUG DES AI ACTS

Die Mitgliedsstaaten haben im Rahmen der nationalen Begleit- und Durchführungsgesetzgebung die für den Vollzug des AI Acts zuständigen Behörden zu designieren. Art. 74 Abs. 6 AI Act sieht hierbei grundsätzlich vor, dass **die für unionsrechtlich regulierte Finanzinstitute zuständige nationale Aufsichtsbehörde** auch als **Marktüberwachungsbehörde gemäß AI Act** für von diesen Finanzinstituten eingesetzte Hochrisiko-KI-Systeme, die mit der **Erbringung von Finanzdienstleistungen in direktem Zusammenhang stehen**, designiert werden soll. Darüber hinaus wurde die FMA aufgrund ihrer Zuständigkeiten im kollektiven Verbraucherschutz als für den **Schutz der Grundrechte zuständige Behörde** gemäß Art. 77 AI Act der Europäischen Kommission notifiziert.³⁹

Die konkrete nationale AI Act - Aufsichtsarchitektur wird final erst nach Abschluss des legislativen Prozesses für das nationale Begleit- und Durchführungsgesetz feststehen. Die FMA geht derzeit davon aus, dass neben der im AI Act angelegten Marktüberwachungszuständigkeit für bestimmte Hochrisiko-KI-Systeme von bestehenden FMA-Aufsichtssubjekten auch die Vollzugszuständigkeit gemäß Art. 50 AI Act betreffend Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme, welche in direktem Zusammenhang mit der Erbringung von Finanzdienstleistungen stehen, übertragen wird.

4.2 DEFINITION: KI-SYSTEM

In Art. 3 Z 1 AI Act werden KI-Systeme legaldefiniert: *"ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können."* ErwG. 12 AI Act beinhaltet dahingehend zentrale Anhaltspunkte zur Interpretation der Legaldefinition für KI-Systeme. Die Europäische Kommission veröffentlichte darüber hinaus **Leitlinien zur Definition von KI-Systemen**⁴⁰ (folgend: *"GL on AI system definition"*) gemäß Art. 96 Abs. 1 Buchstabe f AI Act, welche die praktische Umsetzung der Bestimmung erleichtern und damit ebenso eine bessere Abgrenzung des Anwendungsbereichs des AI Acts ermöglichen sollen. Gemäß dieser Leitlinien beinhaltet die Legaldefinition **sieben definitorische Hauptelemente**:

³⁹ Bundeskanzleramt (Digital Austria), AI Act: Artikel 77 stärkt Grundrechte, abrufbar unter: www.digitalaustria.gv.at/themen/kuenstliche-intelligenz/behoerden-art77-ai-act.html (zuletzt abgerufen am 31.07.2026).

⁴⁰ EK, Leitlinien zur Definition eines Systems der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (folgend: *GL on AI system definition*), 29.07.2025, C(2025) 5053 final, abrufbar unter: digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (zuletzt abgerufen am 31.07.2026).

4.2.1 MASCHINENGESTÜTZTES SYSTEM

(1) **Maschinengestütztes System:** Der Begriff „*maschinengestützt*“ bezieht sich auf die Tatsache, dass KI-Systeme mithilfe von Maschinen entwickelt und auf Maschinen betrieben werden.⁴¹

4.2.2 AUTONOMIE

(2) **Autonomie:** „*mit verschiedenen Graden der Autonomie*“ bedeutet, dass KI-Systeme bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren können und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. Hierdurch werden Systeme ausgenommen, die ausschließlich für den Betrieb unter vollständigem, manuellem Zutun und Eingreifen des Menschen konzipiert sind.⁴²

4.2.3 ANPASSUNGSFÄHIGKEIT

(3) **Anpassungsfähigkeit:** „*das nach seiner Betriebsaufnahme anpassungsfähig sein kann*“ bezieht sich auf die Lernfähigkeit, durch die sich das Verhalten des KI-Systems während seiner Verwendung verändern kann. Das neue Verhalten des angepassten KI-Systems kann bei denselben Eingaben gegenüber dem vorherigen KI-System zu anderen Ausgaben führen.⁴³

4.2.4 EXPLIZITE / IMPLIZITE ZIELE VON KI-SYSTEMEN

(4) **Ziele des KI-Systems:** „*für explizite oder implizite Ziele ableitet*“ bedeutet, dass KI-Systeme so ausgelegt sind, dass sie mit einem oder mehreren expliziten oder impliziten Zielen betrieben werden können. Diese Ziele können sich unter Umständen von den Zweckbestimmungen (als nach außen gerichtetem Kontext, in welchem das KI-System eingesetzt werden soll) unterscheiden.⁴⁴

4.2.5 ABLEITEN

(5) **Ableiten:** Diese Fähigkeit bezieht sich auf den Prozess der Erzeugung von Ausgaben (bspw. Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen), die physische und digitale Umgebungen beeinflussen können sowie auf die Fähigkeit von KI-Systemen, Modelle und/oder Algorithmen aus Eingaben oder Daten abzuleiten.⁴⁵ Die Fähigkeit eines KI-Systems, abzuleiten, **geht über die einfache Datenverarbeitung hinaus**, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden. KI-Systeme sind daher von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abzugrenzen. Nicht umfasst sind Systeme, die

⁴¹ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 11 ff.

⁴² Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 14 ff mit Verweis auf ErwG. 12 AI Act.

⁴³ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 22 ff mit Verweis auf ErwG. 12 AI Act.

⁴⁴ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 24 ff mit Verweis auf ErwG. 12 AI Act.

⁴⁵ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 26 ff mit Verweis auf ErwG. 12 AI Act.

auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen.⁴⁶

4.2.5.1 Die Ableitung ermöglichende KI-Techniken

Die Leitlinien präzisieren die in ErwG. 12 AI Act erwähnten Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen ("KI-Techniken"), welches zentrales Abgrenzungsmerkmal der Legaldefinition in Art. 3 Z 1 AI Act ist. Diese KI-Techniken umfassen insb.:

- Ansätze für **maschinelles Lernen**,⁴⁷ wobei **aus Daten gelernt** wird, wie bestimmte Ziele erreicht werden können. Hierzu zählen überwachtes Lernen, unüberwachtes Lernen, selbstüberwachtes Lernen und bestärkendes Lernen sowie Deep Learning.
- **Logik- und wissensgestützte Konzepte**,⁴⁸ wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird. Anstatt aus Daten zu lernen, **lernen** diese KI-Systeme **aus Wissen, einschließlich Regeln, Fakten und Beziehungen, die von menschlichen Sachverständigen kodiert wurden**.⁴⁹

4.2.5.2 Systeme außerhalb des Anwendungsbereichs des AI Acts

Die Definition von KI-Systemen soll solche Systeme von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen. Die Definition von KI-Systemen soll sich nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen. Abzugrenzen sind insb. solche Systeme, die lediglich in begrenztem Umfang Muster analysieren bzw. ihre Ergebnisse autonom anpassen können. Die Leitlinien führen hierzu beispielhaft bestimmte Systemgruppen an:⁵⁰

- **Systeme zur Verbesserung der mathematischen Optimierung** oder zur Beschleunigung und Annäherung traditioneller, gängiger Optimierungsmethoden wie die für Finanzmarktteilnehmer besonders praktisch relevanten **lineare oder logistische Regressionsmethoden** fallen (grds.) **nicht in den Anwendungsbereich** der Definition eines KI-Systems. Obwohl solche Modelle ableiten können, gehen sie dennoch nicht über die grundlegende Datenverarbeitung hinaus. Ein Hinweis darauf, dass ein System nicht über die grundlegende Datenverarbeitung hinausgeht, könnte sein, dass es seit vielen Jahren in konsolidierter Weise genutzt wird.⁵¹

⁴⁶ Vgl. EK GL on AI system definition, C(2025) 5053 final, ErwG. 12 AI Act.

⁴⁷ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 32 ff mit Verweis auf ErwG. 12 AI Act.

⁴⁸ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 39 mit Verweis auf ErwG. 12 AI Act.

⁴⁹ Anm.: Als Beispiele werden in Rz. 39 der GL on AI system definition, C(2025) 5053 final, klassische Sprachverarbeitungsmodelle sowie Expertensysteme früher Generationen für die medizinische Diagnose angeführt, sowie Wissensrepräsentation, induktive (logische) Programmierung, Wissensdatenbanken, Inferenzmaschinen und deduktive Maschinen, (symbolisches) Argumentieren, Expertensysteme sowie Such- und Optimierungsmethoden.

⁵⁰ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 40 bis 51.

⁵¹ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 42 ff.

- **Einfache Datenverarbeitung**, d.h. das System folgt vorab festgelegten, expliziten Anweisungen oder Vorgängen (bspw. Filterfunktionen von Datenbankverwaltungssystemen, Tabellenkalkulationsanwendungen ohne KI-gestützte Funktionen oder Systeme für beschreibende Analysen, zum Testen von Hypothesen und zur Visualisierung von Daten). Diese Systeme arbeiten auf der Grundlage fester, vom Menschen programmierter Regeln, ohne KI-Techniken wie maschinelles Lernen oder logikgestützte Ableitungen einzusetzen, um damit Ausgaben zu erzeugen.⁵²
- **Auf klassische Heuristik gestützte Systeme**, d.h. Problemlösungstechniken, die auf erfahrungsgestützten Methoden beruhen und mit deren Hilfe effizient Näherungslösungen gefunden werden. Hierbei handelt es sich um regelgestützte Ansätze, Mustererkennung oder Strategien des systematischen Ausprobierens auf Basis vordefinierter Regeln oder Algorithmen, um Lösungen abzuleiten.⁵³
- **Einfache Vorhersagesysteme** sind alle maschinengestützten Systeme, deren Leistung durch eine grundlegende statistische Lernregel erreicht werden kann. Auch wenn diese technisch auf maschinellem Lernen beruhen, fallen sie aufgrund ihrer Leistung nicht in den Anwendungsbereich der Definition eines KI-Systems. Nicht erfasst sind demnach insb. einfache statistische Schätzmethoden (bspw. Finanzprognosen zukünftiger Aktienkurse durch einfache Mittelwert-Schätzfunktion).⁵⁴

Hervorzuheben ist, dass **keine generelle Ausnahme deterministischer Algorithmen** besteht - weder durch den AI Act noch durch die getroffenen Klarstellungen. Eine Ausnahme besteht nur dann, wenn das gegenständliche System ohne jede Form von **Inferenz** arbeitet. Ebenso enthält die Legaldefinition kein Erfordernis, dass die von einem KI-System generierten Ausgaben unvorhersehbar sein müssen. Dies wird durch die im Zusammenhang mit logik- und wissensbasierten Systemen angeführten Beispiele verdeutlicht. Auch vollständig vorhersagbare, regelbasierte Schlussfolgerungen können unter den KI-Begriff fallen, sofern eine Inferenzkomponente vorliegt.

⁵² Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 46 f.

⁵³ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 48.

⁵⁴ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 49 ff.

(6) **Ausgaben:** Unter "*Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden*", können insb. folgende vier zentrale Fallgruppen unterschieden werden:

- **Vorhersage**, d.h. eine Schätzung eines unbekannten Werts (Ausgabe) anhand bekannter Werte (Eingabe), die dem System zur Verfügung gestellt werden.⁵⁵
- **Inhalte**, d.h. Erzeugung neuer Materialien durch ein KI-System wie bspw. Text, Bilder, Videos, Musik und andere Ausgabeformen.⁵⁶
- **Empfehlungen**, d.h. Vorschläge für konkrete Entscheidungen, Maßnahmen, Produkte oder Dienstleistungen für Nutzer auf der Grundlage ihrer Vorlieben, Verhaltensweisen oder sonstigen Dateneingaben.⁵⁷
- **Entscheidungen**, d.h. Schlussfolgerungen oder Auswahlentscheidungen eines KI-Systems, welches als vollautomatischer Vorgang Entscheidung ausgibt und automatisiert Prozesse, die üblicherweise dem menschlichen Urteilsvermögen vorbehalten sind.⁵⁸

(7) **Interaktion** mit der Umgebung: "*Ausgaben [...] die physische oder virtuelle Umgebungen beeinflussen können*" bedeutet, dass KI-System sowohl auf materielle, physische Objekte (bspw. einen Roboterarm) und/oder auch auf virtuelle Umgebungen, einschließlich digitaler Räume, Datenströme und Software-Ökosysteme, Einfluss nehmen kann.⁵⁹

Reduziert man diese Definition auf ihre wesentlichen Bestandteile, handelt es sich bei einem KI-System um ein System, das aus erhaltenen Eingaben für vorgegebene oder implizite Ziele ableitet, wie Outputs erzeugt werden. **Zentrales Abgrenzungsmerkmal** ist damit die **Fähigkeit zur Ableitung (Inferenz)**; nicht jede bloß deterministische oder regelbasierte Software wird daher durch die Legaldefinition in Art. 3 Z 1 AI Act erfasst.

Beispiel: Kein automatischer Ausschluss deterministischer KI-Systeme

Systeme, deren Ausgaben vorhersagbar sind bzw. deren Output durch deterministische Regeln innerhalb des Modells oder nachgelagert überprüft bzw. angepasst wird (sog. "*Guardrails*") können trotzdem KI-Systeme iSd Art. 3 Z 1 AI Act sein. Aus Sicht des Rechtsanwenders ist hinsichtlich des Anwendungsbereichs des AI Acts für die Abgrenzung der Legaldefinition eines KI-Systems gemäß Art. 3 Z 1 AI Act zentral, ob dieses aus Eingaben mittels KI-Techniken wie

⁵⁵ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 54 f.

⁵⁶ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 56.

⁵⁷ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 57 f.

⁵⁸ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 58 f.

⁵⁹ Vgl. EK, GL on AI system definition, C(2025) 5053 final, Rz. 60.

maschinelles Lernen oder Logik- und wissensgestützter Konzepte autonom ableitet, wie Ausgaben erzeugt werden können.

Beispiel: Einordnung KI-Chatbot / rein beratende Systeme:

Ein KI-Chatbot auf der Website eines Unternehmens, der ausschließlich Kunden bei der Produktauswahl berät, beeinflusst nach dieser Definition den virtuellen Raum, auch wenn dieser bspw. nicht direkt einen Vertrag abschließt oder über einen Anspruch entscheiden kann. Auch die reine Beratung stellt eine Einflussnahme auf den virtuellen Raum dar. Nach der Qualifikation als KI-System gemäß Art. 3 Z 1 AI Act wäre in der Folge auch eine Prüfung der Eignung als Hochrisiko-KI-System gemäß Art. 6 Abs. 2 in Verbindung mit Anhang III Abs. 5 Buchstabe c AI Act erforderlich, falls die Verwendung des Chatbots bestimmungsgemäß der Risikobewertung und Preisbildung in Bezug auf natürliche Personen betreffend die Lebens- und Krankenversicherung dient.

Aufgrund der Weite der Definition des KI-Systems gemäß Art. 3 Z 1 AI Act und dem kontinuierlichen Voranschreiten der technologischen Entwicklung ist davon auszugehen, dass trotz der bestehenden *GL on AI system definition* der Europäischen Kommission die exakte Abgrenzung des sachlichen Anwendungsbereichs Rechtsanwender vor Herausforderungen stellen wird zumal letztlich eine autoritative Auslegung der unionsrechtlichen Bestimmung nur durch den Gerichtshof der Europäischen Union (EuGH) erfolgen kann.⁶⁰

4.3 RISIKOPERSPEKTIVE: KLASSIFIKATION VON KI-SYSTEMEN NACH RISIKOSTUFEN

Nach erfolgter Einstufung des Systems als KI-System iSd Art. 3 Z 1 AI Act ist zu prüfen ob und wenn ja welchen regulatorischen Anforderungen das spezifische KI-System im Rahmen des risikobasierten Regulierungsansatzes des AI Acts unterliegt. Die Einstufung erfolgt auf Basis des inhärenten Gefährdungspotentials betreffend die unionsrechtlich verankerten Werte der Union, Grundfreiheiten und Grundrechte in folgende Risikokategorien:⁶¹ **Verbotene KI-Praktiken** gemäß Art. 5 AI Act (inakzeptables Risiko), **Hochrisiko-KI-Systeme** gemäß Art. 6 ff AI Act (hohes Risiko) sowie **transparenzpflichtige KI-Systeme** gemäß Art. 50 AI Act (Transparenzpflichten / begrenztes

⁶⁰ In diesem Kontext ist auch auf die in der Wissenschaft thematisierte Einordnung anhand einer 3-Faktor-Methode hinzuweisen - vgl. bspw. Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605. Weitere Ansätze einer definitorischen Einordnung finden sich in den ISO-Standards ISO/IEC 22989:2022.

⁶¹ Vgl. ErwG. 6 ff AI Act.

Risiko).⁶² Risikostufen können auch parallel gelten - im Konkreten unterliegen daher auch Hochrisiko-KI-Systeme, welche in den Anwendungsbereich des Art. 50 AI Act fallen, den (allgemeinen) Transparenzpflichten.

Ein großer Teil der Systeme liegt unter diesen Risikoschwellen. Dies führt dazu, dass im Ergebnis trotz der Einstufung als KI-System iSd Art. 3 Z 1 AI Act ein großer Teil der KI-Systeme keinen spezifischen regulatorischen Anforderungen gemäß AI Act unterliegt, da von diesen nur ein minimales Risiko ausgeht (bspw. KI-gestützte Spamfilter).⁶³

4.3.1 VERBOTENE KI-PRAKTIKEN (INAKZEPTABLES RISIKO)

Der Art. 5 AI Act listet bestimmte verbotene KI-Praktiken auf, welche aufgrund des inhärenten inakzeptablen Risikos für Grundwerte, -freiheiten und -rechte der Europäischen Union absolut verboten sind. Gemäß Art. 96 Abs. 1 Buchstabe b AI Act erließ die Europäische Kommission **Leitlinien zur praktischen Umsetzung der nach Art. 5 AI Act verbotenen KI-Praktiken** (folgend: "*GL on prohibited AI practices*").⁶⁴ Die verbotenen KI-Praktiken umfassen die folgenden Gruppen von KI-Systemen:

- Schädliche Manipulation, Täuschung und Ausbeutung (Art. 5 Abs. 1 Buchstabe a und b AI Act);⁶⁵
- Soziale Bewertung ("*Social Scoring*"; Art. 5 Abs. 1 Buchstabe c AI Act);⁶⁶
- Individuelle Risikobewertung und Vorhersage von Straftaten (sog. "*Predictive Policing*" über Profiling; Art. 5 Abs. 1 Buchstabe d AI Act);⁶⁷
- Ungezieltes Auslesen von Gesichtsbildern (Art. 5 Abs. 1 Buchstabe d AI Act);⁶⁸
- Emotionserkennung (Art. 5 Abs. 1 Buchstabe f AI Act);⁶⁹
- Biometrische Kategorisierung betreffend bestimmte sensible Merkmale (Art. 5 Abs. 1 Buchstabe g AI Act);⁷⁰
- Biometrische Echtzeit-Fernidentifizierungssysteme zu Strafverfolgungszwecken bzw. im öffentlichen Raum (Art. 5 Abs. 1 Buchstabe h und Abs. 2 AI Act).⁷¹

⁶² In diesem Kontext ist anzumerken, dass Hochrisiko-KI-Systeme gemäß Art. 6 ff AI Act bei Erfüllung der Voraussetzungen des Art. 50 AI Act zusätzlich den jeweiligen Transparenzpflichten unterliegen.

⁶³ Vgl. RTR (KI-Servicestelle), Risikostufen von KI-Systemen, abrufbar unter www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.de.html (zuletzt abgerufen am 31.07.2026).

⁶⁴ EK, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (folgend: *GL on prohibited AI practices*), 29.07.2025, C(2025) 5052 final, abrufbar unter: digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (zuletzt abgerufen am 31.07.2026).

⁶⁵ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 58 ff.

⁶⁶ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 146 ff.

⁶⁷ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 184 ff.

⁶⁸ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 222 ff.

⁶⁹ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 239 ff.

⁷⁰ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 271 ff.

⁷¹ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 289 ff.

- Darüber hinaus wurden durch den Vorschlag der Europäischen Kommission betreffend eine **Digital-Omnibus-Verordnung zur KI**⁷² bestimmte KI-Praktiken mit Bezug zu sexualisiertem Inhalt verboten.

Bezugnehmend auf das Tätigkeitsprofil von Finanzmarktteilnehmern können insb. die verbotenen KI-Praktiken betreffend Schädliche Manipulation, Täuschung und Ausbeutung sowie sozialer Bewertung einschlägig sein.

4.3.2 HOCHRISIKO-KI-SYSTEME (HOHES RISIKO)

Art. 6 Abs. 2 iVm Anhang III⁷³ AI Act listet KI-Systeme auf, welche aufgrund des inhärent hohen Risikos für Grundwerte, -freiheiten und -rechte der Europäischen Union, nur unter Einhaltung hoher regulatorischer Standards als Hochrisiko-KI-System in Verkehr gebracht oder in Betrieb genommen werden dürfen. Zusätzlich werden durch Art. 6 Abs. 1 iVm Anhang I AI Act bestimmte KI-Systeme die selbst europäisch regulierte Produkte sind oder ein Sicherheitsbauteil für diese darstellen, zu Hochrisiko-KI-Systemen erklärt.

4.3.2.1 Hochrisiko-KI-Systeme mit unmittelbarem Bezug zur Erbringung regulierter Finanzdienstleistungen

Im Kontext der Erbringung regulierter Finanzdienstleistungen sind für Finanzmarktteilnehmer insb. die folgenden gemäß Art. 6 Abs. 2 iVm Anhang III Abs. 5 AI Act in der Rubrik "*Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen*" relevant:

- KI-Systeme, die bestimmungsgemäß für die **Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen** verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden (Art. 6 Abs. 2 iVm Anhang III Abs. 5 Buchstabe b) sowie
- KI-Systeme, die bestimmungsgemäß für die **Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen** verwendet werden sollen (Art. 6 Abs. 2 iVm Anhang III Abs. 5 Buchstabe c).

⁷² Vorschlag für eine Verordnung zur Änderung der Verordnungen (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), COM/2025/836 final. In diesem Kontext ist insb. auf den potentiellen Aufschub der Anwendbarkeit des Rechtsrahmens für Hochrisiko-KI-Systeme gemäß Art. 6 Abs. 2 iVm Anhang III AI Act hinzuweisen.

⁷³ Anm.: Hierbei handelt es sich um sog. "Stand-alone" Hochrisiko-KI-Systeme.

Beispiel: Hochrisiko-KI-Systeme außerhalb des Banken- und Versicherungssektors

Die Rubrik "*Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen*" schränkt den Anwendungsbereich der gelisteten Hochrisiko-KI-Systeme nicht auf bestimmte Wirtschaftssektoren ein. Im Kontext dieser Bestimmung ist daher nach aktuellem Stand davon auszugehen, dass klassische Finanzdienstleistungen als grundlegende private Leistungen zu qualifizieren sind. Wird der Zugang zu Finanzdienstleistungen durch ein KI-System zur Bonitätsbewertungen (und allenfalls an dieser anknüpfende Gebühren- bzw. Risikoaufschläge) gesteuert, ist eine Qualifikation als Hochrisiko-KI-System gemäß Art. 6 Abs. 2 iVm Anhang III Abs. 5 Buchstabe b AI Act daher grundsätzlich denkbar.⁷⁴

Gemäß Art. 6 Abs. 3 AI Act können in Anhang III genannte KI-Systeme **als nicht hocharisikant eingestuft werden** (sog. "Filter"), wenn diese kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst. Dies ist der Fall, wenn das KI-System dazu bestimmt ist

- eine eng gefasste Verfahrensaufgabe durchzuführen;
- das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern;
- Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen oder
- eine vorbereitende Aufgabe für eine Bewertung durchzuführen, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist.
- Ein KI-System des Anhangs III, welches Profiling natürlicher Personen vornimmt, ist von der Anwendung der Filterregelung ausgeschlossen.

In diesem Kontext ist darauf hinzuweisen, dass weitere **Hochrisiko-KI-Systeme des Anhangs III** für Finanzmarktteilnehmer von Relevanz sind, **die nicht unmittelbar mit der Erbringung regulierter Finanzdienstleistungen in direktem Zusammenhang stehen**. Dies betrifft insb. Hochrisiko-KI-Systeme, welche bestimmungsgemäß im Bereich "*Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit*" gemäß Art. 6 Abs. 2 iVm Anhang III Abs. 4 AI Act im Rahmen von

⁷⁴ Anm.: Im Bereich des Derivatehandels unter dem WAG 2018, dem Börsegesetz 2018 (BörseG 2018), BGBl. I Nr. 107/2017 idF BGBl. I Nr. 6/2026 sowie der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (MiCAR), ABl. Nr. L 150 vom 09.06.2023 S. 40, idF der Berichtigung ABl. Nr. L 2024/90658 vom 30.10.2024, besteht bei KI-basierten Positions- bzw. Risikomanagementsystemen im gehebelten bzw. kreditfinanzierten Handel das grundsätzliche Potenzial, dass entsprechende Systeme als Hochrisiko-KI-Systeme einzustufen sind.

Bewerbungsverfahren, Personalentwicklung, interner Leistungsbewertung oder Vergütungsentscheidungen eingesetzt werden.

4.3.3 GRENZE ZWISCHEN VERBOTENEN KI-PRAKTIKEN UND HOCHRISIKO-KI-SYSTEMEN

Die Abgrenzung zwischen Hochrisiko-KI-System und verbotenen Praktiken ist nicht strikt kategorial. Der Kontext, in welchem KI-Systeme eingesetzt werden, bestimmt maßgeblich, ob es sich um ein erlaubtes Hochrisiko-KI-System oder eine verbotene KI-Praktik handelt. Dies ist insb. für die mit der Erbringung regulierter Finanzdienstleistungen in Zusammenhang stehenden Hochrisiko-KI-Systeme zur Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen sowie Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen von Relevanz. Ob es sich konkret um einen (erlaubten) Betrieb eines Hochrisiko-KI-Systems handelt oder eine verbotene KI-Praktik (bspw. sog. "Social Scoring" iSd Art. 5 Abs. 1 Buchstabe c AI Act) ist jeweils anhand der Tatbestände des Art. 5 AI Act im Einzelfall zu prüfen. Zum besseren Verständnis folgt eine Darstellung der Grenzen anhand von illustrativen Beispielen:

Beispiel: Social Scoring⁷⁵

Art. 5 Abs. 1 Buchstabe c AI Act verbietet "Social Scoring", sofern folgende drei Bedingungen kumulativ erfüllt werden:⁷⁶

I. Die Praxis muss das „Inverkehrbringen“, die „Inbetriebnahme“ oder die „Verwendung“ eines KI-Systems darstellen.

II. Das KI-System ist für **soziale Bewertung** bestimmt, d.h. Bewertung oder Einstufung auf der Grundlage des sozialen Verhaltens bzw. persönlicher Eigenschaften oder Persönlichkeitsmerkmale über einen bestimmten Zeitraum.

III. Die soziale Bewertung muss zu einer **Schlechterstellung oder Benachteiligung** in nicht miteinander zusammenhängenden sozialen Kontexten und/oder im Hinblick auf das soziale Verhalten oder dessen Tragweite zu einer ungerechtfertigten oder unverhältnismäßigen Behandlung führen.

Das Verbot des Art. 5 Abs. 1 Buchstabe c AI Act **gilt** nicht nur für staatliche Akteure sondern **ebenso für private und juristische Personen**. Wird ein KI-System von einem Institut zur Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen oder Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen

⁷⁵ Vgl. EK, GL on prohibited AI practices, C(2025) 5052 final, Rz. 37.

⁷⁶ Anm.: Darstellung gemäß des in Rz. 149 ff der EK, GL on prohibited AI practices, C(2025) 5052 final, festgelegten Prüfschemas.

eingesetzt, welches die Bedingungen des Art. 5 Abs. 1 Buchstabe c AI Act erfüllt, ist das Inverkehrbringen, die Inbetriebnahme und die Verwendung in der Union verboten.

Beispiel: Verbotene KI-Praktik - unzulässige Verwendung personenbezogener Finanzdaten durch ein Versicherungsunternehmen⁷⁷

Eine Versicherungsgesellschaft holt bei einer Bank Auskünfte über Ausgaben und sonstige Finanzinformationen ein, die in keinem Zusammenhang mit der Feststellung der Eignung der Bewerber für eine Lebensversicherung stehen und zur Festlegung der Höhe, der für eine solche Versicherung zu zahlenden Prämie herangezogen werden. Ein KI-System analysiert diese Informationen und empfiehlt auf dieser Grundlage, einen Vertrag abzulehnen oder für eine bestimmte Einzelperson oder Kundengruppe höhere Lebensversicherungsprämien festzusetzen.

Die **Abgrenzung** von verbotenen KI-Praktiken und erlaubten Hochrisiko-KI-Systemen erfordert regelmäßig den **Rückgriff auf das anwendbare sektorale Aufsichtsrecht** - dies ergibt sich im Zusammenhang mit "Social Scoring" insb. aus ErwG. 31: "[...] Dieses Verbot sollte nicht die rechtmäßigen Praktiken zur Bewertung natürlicher Personen berühren, die im Einklang mit dem Unionsrecht und dem nationalen Recht zu einem bestimmten Zweck durchgeführt werden". Was eine **rechtmäßige Praktik im Einklang mit dem Unionsrecht⁷⁸ und nationalem Recht** im Zusammenhang mit der Erbringung von regulierten Finanzdienstleistungen ist, hat **materiell** insb. anhand des **Finanzmarktrechts und an den (finanzmarktrechtlichen) Verbraucherschutzbestimmungen gemessen** zu werden. Rz. 177 der *GL on prohibited AI practices* führt dazu konkret wie folgt aus: "Werden sektorspezifische Rechtsvorschriften der Union eingehalten, beispielsweise im Bereich der Bonitätsbewertung, der Bekämpfung von Geldwäsche usw., in denen festgelegt ist, welche Art von Daten für den spezifischen legitimen Zweck der Bewertung als relevant und erforderlich verwendet werden können, und mit denen sichergestellt wird, dass die Behandlung gerechtfertigt ist und in einem angemessenen Verhältnis zum sozialen Verhalten steht, kann somit sichergestellt werden, dass die betreffende KI-Praxis nicht in den Anwendungsbereich des Verbots nach Artikel 5 Absatz 1 Buchstabe c der KI-Verordnung fällt."

⁷⁷ Anm.: Bsp. gemäß Rz. 170 der EK, *GL on prohibited AI practices*, C(2025) 5052 final.

⁷⁸ Anm.: In diesem Zusammenhang ist ebenso der datenschutzrechtliche Rahmen insb. betreffend Profiling von Relevanz, vgl. Art. 4 Nr. 4 iVm Art. 22 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S 1, idF der Berichtigung ABl. Nr. L 74 vom 04.03.2021 S 35.

Beispiel: Keine verbotene KI-Praktik - Systeme zur finanziellen Bonitätsbewertung von Kreditgebern oder Wirtschaftsauskunfteien unter Einhaltung sektoraler Vorgaben⁷⁹

Nicht in den Anwendungsbereich von Art. 5 Abs. 1 Buchstabe c AI Act fallen Systeme zur finanziellen Bonitätsbewertung⁸⁰, die von Kreditgebern oder Wirtschaftsauskunfteien zur Bewertung der finanziellen Kreditwürdigkeit oder ausstehender Verbindlichkeiten eines Kunden genutzt werden, um eine Einstufung der Bonität oder Feststellung seiner Kreditwürdigkeit vorzunehmen, wobei sie sich auf die Einnahmen und Ausgaben des Kunden und andere finanzielle und wirtschaftliche Umstände stützen, sofern diese für den rechtmäßigen Zweck der Bonitätsbewertung relevant sind und im Einklang mit Verbraucherschutzgesetzen stehen, in denen die Art der Daten und die erforderlichen Schutzvorkehrungen festgelegt sind, um die faire Behandlung von Verbrauchern bei Kreditwürdigkeitsprüfungen zu gewährleisten. Als **Prüfmaßstab** ist gemäß FN 126 der *GL on prohibited AI practices* hierfür neben der Richtlinie (EU) 2023/2225 über Verbraucherkreditverträge (*Consumer Credit Directive, CCD*) insb. **auch das einschlägige europäische Soft Law**, konkret die EBA-Leitlinien für die Kreditvergabe und Überwachung,⁸¹ heranzuziehen.

Beispiel: Keine verbotene KI-Praktik - telematikgestützte Versicherungstarife unter Einhaltung sektoraler Vorgaben⁸²

Über Telematikgeräte erhobene Informationen, die zeigen, dass ein Fahrer zu schnell fährt oder keine sichere Fahrweise pflegt, können von einem Versicherungsunternehmen, welches telematikgestützte Versicherungstarife für das hochriskante Fahrverhalten eines Versicherungsnehmers anbietet, verwendet werden. Diese Informationen können zu einer Erhöhung der Versicherungsprämien für den betreffenden Versicherungsnehmer genutzt und mit der durch dieses Fahrverhalten erhöhten Unfallgefahr begründet werden, sofern die Erhöhung der Versicherungsprämie in einem angemessenen Verhältnis zum risikobehafteten Verhalten des Fahrers steht. Aus diesem Grund liegt eine rechtmäßige Bewertungspraktiken, die im Einklang mit Unionsrecht und nationalem Recht steht vor, welche somit nicht in den Anwendungsbereich von Art. 5 Abs. 1 Buchstabe c AI Act fällt.

⁷⁹ Anm.: Bsp. gemäß Rz. 177 der EK, *GL on prohibited AI practices*, C(2025) 5052 final.

⁸⁰ Anm.: Aus datenschutzrechtlicher Sicht ist iZm Bonitätsbewertungen insb. auf das Urteil des Europäischen Gerichtshofs vom 27. Februar 2025, C-203/22 (*Dun & Bradstreet Austria GmbH*) hinzuweisen. Siehe hierzu österreichische Datenschutzbehörde (DSB), Mitteilung zum besonderen Auskunftsanspruch im Rahmen von Bonitätssoring, abrufbar unter: <https://dsb.gv.at/aktuelles/rundschreiben-der-datenschutzbehoerde-zum-recht-auf-auskunft-im-zusammenhang-mit-%E2%80%9Ebonitaetssoring%E2%80%9C> (zuletzt abgerufen am 31.07.2026).

⁸¹ EBA, Leitlinien für die Kreditvergabe und Überwachung, EBA/GL/2020/06.

⁸² Anm.: Bsp. gemäß Rz. 177 der EK, *GL on prohibited AI practices*, C(2025) 5052 final.

Auch hinsichtlich der durch Art. 5 Abs. 1 Buchstabe a und b AI Act verbotenen KI-Praktiken, d.h. **KI-Systeme die menschliches Verhalten manipulieren oder Schwächen von Menschen** (insb. aufgrund der sozialen oder wirtschaftlichen Lage, des Alters oder einer Behinderung) **ausnützen**, hat die Abgrenzung im Kontext regulierter Finanzdienstleistungen anhand des einschlägigen finanzmarktrechtlichen Rechtsrahmens und des in diesem Zusammenhang erlassenen Soft Law zu erfolgen. Rz. 143 der *GL on prohibited AI practices* führt dazu konkret wie folgt aus: *"Das in der KI-Verordnung enthaltene Verbot schädlicher ausbeuterischer und täuschender KI-Praktiken ergänzt zudem andere geltende Rechtsvorschriften der Union, in denen allgemeine Transparenzvorschriften für Werbung, Verbraucherschutz und das ordnungsgemäße Verhalten von Wirtschaftsbeteiligten festgelegt sind (z.B. werden in der MIFID-Richtlinie 2014/65/EU, der Richtlinie (EU) 2016/97 über Versicherungsvertrieb, der Richtlinie (EU) 2023/2225 über Verbraucherkreditverträge, der Richtlinie (EU) 2002/65 über den Fernabsatz, der Richtlinie 2006/114/EG über irreführende und vergleichende Werbung und der Richtlinie (EU) 2011/83 über die Rechte der Verbraucher allgemeine Verbraucherschutzstandards festgelegt). In diesem Zusammenhang hat die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) bereits eine aufsichtliche Erklärung zu einigen unlauteren ausbeuterischen Praktiken im Zusammenhang mit differenzierten Preisen abgegeben, die auch in den Anwendungsbereich der KI-Verordnung fallen könnten, wenn sie durch KI-Systeme ermöglicht werden."* Für die konkrete AI Act konforme Ausgestaltung eines zulässigen (idR Hochrisiko-)KI-Systems eines Finanzmarktteilnehmers, welches jedoch potentiell als schädlich ausbeuterisch oder täuschende KI-Praktiken qualifiziert werden könnte, ist daher insb. das sektorale Aufsichtsrecht (bspw. vertriebsbezogene Vorschriften) samt einschlägigem Soft Law maßgeblich.

Beispiel: Verbotene KI-Praktik - "Price Walking" iZm Nicht-Lebensversicherungen betreffend ältere Versicherungsnehmer

Werden Preisstrategien durch ein KI-System so gestaltet, dass bei der Verlängerung von Nicht-Lebensversicherungen wiederholt die zu zahlende Prämie aufgrund von Faktoren, die nicht mit dem versicherungstechnischen Risiko oder den Dienstleistungskosten zusammenhängen, erhöht wird, bspw. Attribute welche ältere Versicherungsnehmer umschreiben, kann dies eine verbotene Ausnutzung der Vulnerabilität oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen darstellen, welche zu einem erheblichen Schaden führt. Hierdurch wird der Tatbestand der Verbotenen KI-Praktik gemäß Art. 5 Abs. 1 Buchstabe b AI Act erfüllt.

Die Praxis ist weiters auch nicht durch sektorales Finanzmarktrecht rechtfertigbar. Im konkreten Fall handelt sich um eine **differenzierte Preisgestaltungspraktik**⁸³, welche zu einem diskriminierenden Verhalten gegenüber älteren Versicherungsnehmern führt und auch gemäß

⁸³ Vgl. EIOPA, *Supervisory statement on differential pricing practices in non-life insurance lines of business*, [EIOPA-BoS-23/076](#), Rz. 2.12.

dem *EIOPA Supervisory Statement on differential pricing practices in non-life insurance lines of business*⁸⁴ als nicht mit Art. 17 IDD vereinbar eingestuft wird.

Die in Art. 17 IDD stipulierte Anforderung, dass Versicherungsvertreiber bei ihrer Versicherungsvertriebstätigkeit gegenüber ihren Kunden stets **ehrlich, redlich und professionell in deren bestmöglichem Interesse** zu handeln haben findet sich auch in anderen sektoralen Rechtsakten. Die **Einordnung von KI-Systemen zur Preisdifferenzierung**, bspw. im Bereich KI-gesteuerter Gebühren-Modelle, **als verbotene KI-Praktik** ist daher regelmäßig insb. auch **an den sektoralen finanzmarktrechtlichen Anforderungen**^{85 86} **zu messen**. Beispielsweise haben Anbieter von Kryptowerte-Dienstleistungen gemäß Art. 66 der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (*Markets in Crypto Assets Regulation, MiCAR*)⁸⁷ ehrlich, redlich und professionell im besten Interesse ihrer (potenziellen) Kunden zu Handeln. Zudem haben sie abhängig vom Geschäftsmodell gemäß Art. 77 MiCAR zum Tausch von Kryptowerten gegen Geldbeträge bzw. andere Kryptowerte alternativ zu einem festen Preis die Methode zur Bestimmung des Preises eindeutig und verständlich sowie nachvollziehbar offenzulegen. Die Ausgestaltung und der bestimmungsgemäße Einsatz von KI-Systemen durch diese Finanzmarktteilnehmer ist daher insb. auch an den einschlägigen sektoralen finanzmarktrechtlichen Anforderungen zu messen.

4.3.4 TRANSPARENZPFLICHTEN (BEGRENZTES RISIKO / TRANSPARENZRISIKO)

Jene KI-Systeme, die bestimmungsgemäß mit natürlichen Personen interagieren oder Inhalte erzeugen sollen, können unabhängig davon ob sie als hochriskant eingestuft werden ein besonderes Risiko in Bezug auf Identitätsbetrug oder Täuschung bergen.⁸⁸ Zur Adressierung dieses Transparenzrisikos sieht Art. 50 AI Act Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme vor:⁸⁹

- **KI-Systeme, welche bestimmungsgemäß mit natürlichen Personen direkt interagieren** (bspw. KI-Chatbots) - Anforderung der Offenlegung, dass mit einem KI-System interagiert wird, sofern dies nicht aufgrund der Umstände und des Kontextes der Nutzung offensichtlich ist.
- **KI-Systeme, die bestimmungsgemäß synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen oder manipulieren (inkl. Deepfakes)** - Anforderung, dass die Ausgaben des KI-

⁸⁴ Vgl. EIOPA, *Supervisory statement on differential pricing practices in non-life insurance lines of business*, *EIOPA-BoS-23/076*, Rz. 3.8.

⁸⁵ Vgl. EK, *GL on prohibited AI practices*, C(2025) 5052 final, Rz. 143.

⁸⁶ Anm.: Andere Beispiele wären etwa Gleichbehandlungsgrundsätze, Verbote unsachlicher Differenzierung, Produktfairness-Regeln oder Verbraucherschutzrechtlichen Transparenzpflichten.

⁸⁷ Verordnung (EU) 2023/1114 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (*Markets in Crypto Assets Regulation, MiCAR*), ABl. Nr. L 150 vom 09.06.2023 S. 40, in der Fassung der Berichtigung ABl. Nr. L 2024/90658 vom 30.10.2024.

⁸⁸ Vgl. ErwG. 132 AI Act.

⁸⁹ Vgl. RTR (KI-Servicestelle), *Risikostufen von KI-Systemen*, abrufbar unter: www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.de.html (zuletzt abgerufen am 31.07.2026).

Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Diese Transparenzpflicht gilt für Anbieter von KI-Systemen.

- **KI-Systeme die bestimmungsgemäß zur biometrische Kategorisierung- oder Emotionserkennung eingesetzt werden** - Anforderung der Offenlegung gegenüber betroffenen natürlichen Personen über den Betrieb des Systems und die Verarbeitung personenbezogener Daten.

Die Transparenzpflichten gemäß **Art. 50 AI Act** sind bei Erfüllung der Tatbestandsvoraussetzungen **auch von Hochrisiko-KI-Systemen einzuhalten**. Zusätzlich bestehen für Hochrisiko-KI-Systeme erweiterte Transparenzpflichten; hervorzuheben ist die **Information der direkt oder indirekt⁹⁰ von einer Entscheidung Betroffenen gemäß Art. 26 Abs. 11 AI Act**. Darüber hinaus können KI-Systeme, die in den Anwendungsbereich des Art. 50 AI Act fallen, auch **verbotene KI-Praktiken** darstellen - bspw. Deepfakes zur Manipulation menschlichen Verhaltens.

Zusammenspiel der Transparenzpflichten gemäß AI Act und sektorialem Finanzmarktrecht

Der AI Act enthält Transparenzverpflichtungen, diese ergänzen die Transparenzverpflichtungen die das sektorale Finanzmarktrecht (für bspw. den Vertrieb von Finanzprodukten) vorsieht. Ein Chatbot oder Robo-Advice-Interface muss gegenüber Nutzern grundsätzlich offenlegen, dass diese mit einem KI-System interagieren, sofern dies nicht aus den Umständen ohnehin offensichtlich ist. Diese Transparenzpflicht tritt neben bestehende sektorale Informations- und Wohlverhaltenspflichten.

4.4 AKTEUR-PERSPEKTIVE

4.4.1 IM ÜBERBLICK: ANFORDERUNGEN AN DEN BETRIEB VON HOCHRISIKO-KI-SYSTEMEN

Art. 6 ff (Kapitel III) AI Act legt die regulatorischen Anforderungen für in Verkehr gebrachte oder in Betrieb genommene Hochrisiko-KI-Systeme fest. Hierbei differenzieren die Anforderungen, je nach Akteur der KI-Wertschöpfungskette. Zu unterscheiden sind insb.:

- **Anbieter** gemäß Art. 3 Z 3 AI Act: *"eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich"*,⁹¹ sowie

⁹⁰ Anm.: Eine Entscheidung, die durch ein Hochrisiko-KI-System unterstützt wurde.

⁹¹ Anm.: Umfasst sind demnach insbesondere auch intern entwickelte und intern verwendete KI-Systeme.

- **Betreiber** gemäß Art. 3 Z 4 AI Act: *"eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System **in eigener Verantwortung verwendet**, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet"*.

Zwar bestehen für jeden Akteur auch gemeinsame Verpflichtungen, wie die Sicherstellung adäquater KI-Kompetenz beim Personal gemäß Art. 4 AI Act, grundsätzlich sind die Vorgaben jedoch je nach Akteur unterschiedlich ausgestaltet. In diesem Kontext ist darauf hinzuweisen, dass Akteure der KI-Wertschöpfungskette (insb. Betreiber) bei Verwirklichung der in Art. 25 AI Act vorgesehenen Tatbestände den Anbieterpflichten unterliegen.⁹²

4.4.2 ÜBERSICHT SPEZIFISCHER ANBIETERPFLICHTEN⁹³

Die Verpflichtungen von Anbietern, die sich u.a. aus Art. 16 AI Act ergeben, sind insbesondere:⁹⁴

- Ausreichendes Risiko- und Qualitätsmanagement (Art. 9 und 17 AI Act);
- Anforderungen an das KI-System selbst, z.B. Datenqualität (Art. 10 AI Act), menschliche Aufsicht (Art. 14 AI Act) sowie Genauigkeit, Robustheit und Cyber-Sicherheit (Art. 15 AI Act), inkl. Sicherstellung der Barrierefreiheitsanforderungen (Art. 16 Buchstabe l AI Act);
- Aufzeichnungs- und Protokollierungs- (Art. 11 und 12 AI Act), Aufbewahrungs- (Art. 18 und 19 AI Act) sowie Melde- und Kooperationspflichten gegenüber Behörden (Art. 16 Buchstabe k, 20, 21 und 73 AI Act sowie die Verordnung (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten⁹⁵) bzw. Post-Market Monitoring (Art. 72 AI Act);
- Transparenz-, Informations- und Kennzeichnungspflichten (Art. 13 und 16 Buchstabe b AI Act) sowie ggf. die Ernennung eines Bevollmächtigten bei einem Drittstaatsbezug (Art. 22 AI Act);
- Korrekturmaßnahmen (Art. 20 AI Act) sowie Konformitätsbewertung und -erklärung (Art. 43, 47 und 48 AI Act);
- Registrierungs- und Mitteilungspflichten in einer EU-Datenbank (Art. 49 AI Act).

⁹² Anm.: Dies ist gemäß Art. 25 Abs. 1 AI Act insbesondere dann der Fall, wenn wesentliche Veränderungen an einem bestehenden Hochrisiko-KI-System vorgenommen werden bzw. wenn ein gemäß der Zweckbestimmung als Nicht-Hochrisiko-KI-System eingestuftes System durch einen Betreiber im Hochrisiko-KI-Bereich eingesetzt wird.

⁹³ Vgl. RTR (KI-Servicestelle), Anbieterverpflichtungen, abrufbar unter: www.rtr.at/rtr/service/ki-servicestelle/ai-act/Anbieterverpflichtungen.de.html (zuletzt abgerufen am 31.07.2026).

⁹⁴ Für wesentliche Anforderungen betreffend Hochrisiko-KI-Systeme siehe insbesondere Kapitel III Abschnitt 2 AI Act.

⁹⁵ Verordnung (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011, ABl. Nr. L 169 vom 25.06.2019 S 1, idF der Verordnung (EU) 2024/1252 zur Schaffung eines Rahmens zur Gewährleistung einer sicheren und nachhaltigen Versorgung mit kritischen Rohstoffen und zur Änderung der Verordnungen (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1724 und (EU) 2019/1020, ABl. Nr. L 2024/1252 vom 03.05.2024.

4.4.3 ÜBERSICHT SPEZIFISCHER BETREIBERPFLICHTEN⁹⁶

Die *wesentlichsten Verpflichtungen* von Betreibern, die sich insb. aus Art. 26 AI Act ergeben, sind u.a.:

- Verwendung des Hochrisiko-KI-Systems laut Betriebsanleitung (Art. 26 Abs. 1, 3 und 4 AI Act);
- Menschliche Aufsicht (Art. 26 Abs. 2 iVm Art. 114 Abs. 3 Buchstabe b AI Act);
- Transparenz- (Art. 26 Abs. 11 AI Act), Überwachungs- sowie Meldepflichten von schwerwiegenden Vorfällen (Art. 26 Abs. 5 und 73 AI Act);
- Aufbewahrungspflicht von automatisch erzeugten Protokollen (Art. 26 Abs. 6 AI Act);
- Kooperationspflicht gegenüber Behörden (Art. 26 Abs. 12 AI Act);
- Recht auf Erläuterung der Entscheidungsfindung im Einzelfall (Art. 86 Abs. 1 AI Act);
- Besondere Pflichten für bestimmte Betreiber (Art. 26 Abs. 7, 8, 10 sowie Art. 27 AI Act) sowie ggf. Durchführungspflicht einer Datenschutz-Folgenabschätzung (Art. 26 Abs. 9 AI Act).

4.4.4 GRUNDRECHTE-FOLGENABSCHÄTZUNG FÜR HOCHRISIKO-KI-SYSTEME

Betreiber von u.a. Hochrisiko-KI-Systemen gemäß Anhang III Abs. 5 Buchstabe b (Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen) und c (Risikobewertung und Preisbildung in der Lebens- und Krankenversicherung betreffend natürliche Personen) AI Act führen entsprechend Art. 27 AI Act **vor Inbetriebnahme** eine Abschätzung der Auswirkungen durch, die die Verwendung eines solchen Systems auf die Grundrechte haben kann (**Fundamental Rights Impact Assessment, FRIA**). Das AI Office der Europäischen Kommission arbeitet hierfür gemäß Art. 27 Abs. 5 AI Act ein Muster für einen entsprechenden Fragebogen (FRIA-Template) aus, um in diesem Bereich Vergleichbarkeit zu gewährleisten. Das durchgeführte FRIA ist gemäß Art. 27 Abs. 3 AI Act **vom Betreiber der Marktüberwachungsbehörde mitzuteilen**.

Soweit im sektoralen Aufsichtsrecht oder in internen Governance-Rahmen weitere Impact Assessments vorgesehen sind, sind deren Zweck und Prüfungsmaßstab von der Grundrechts-Folgenabschätzung gemäß Art. 27 AI Act sauber zu trennen und ersetzen diese nicht.⁹⁷

4.4.5 STRAFBESTIMMUNG

Art. 99 ff AI Act legt das Sanktionsregime bei Verletzung des produktspezifischen regulatorischen Rahmens für Künstliche Intelligenz fest - Mitgliedsstaaten haben hierzu die entsprechenden Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen zu erlassen. In diesem

⁹⁶ Vgl. RTR (KI-Servicestelle), *Betreiberpflichtungen*, abrufbar unter: www.rtr.at/rtr/service/ki-servicestelle/ai-act/Betreiberpflichtungen.de.html <https://www.rtr.at/rtr/service/ki-servicestelle/ai-a> (zuletzt abgerufen am 31.07.2026).

⁹⁷ Vgl. hierzu auch EIOPA, *Opinion on AI Governance and Risk Management*, [EIOPA-BoS-25-360](#), Rz 3.1 ff sowie Annex I.

Zusammenhang sind für Finanzmarktteilnehmer **insb. die folgenden Sanktionsbestimmungen hervorzuheben:**

- **Verstoß gegen verbotene KI-Praktiken** (Art. 5 AI Act):
Geldbußen bis zu **35 Mio. EUR** oder - im Falle von Unternehmen - von bis zu **7%** des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher Betrag höher ist).
- **Verstöße gegen u.a. Anbieter-** (Art. 16 AI Act) oder **Betreiberpflichten** (Art. 26 AI Act) sowie **Transparenzpflichten** für Anbieter und Betreiber (Art. 50 AI Act):
Geldbußen bis zu **15 Mio. EUR** oder - im Falle von Unternehmen - von bis zu **3%** des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher Betrag höher ist).
- **Vorlage falscher, unvollständiger oder irreführender Informationen bei Auskunftersuchen zuständiger nationaler Behörden** oder notifizierender Stellen:
Geldbußen bis zu **7,5 Mio. EUR** oder - im Falle von Unternehmen - von bis zu **1%** des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher Betrag höher ist).

Darüber hinaus werden Marktüberwachungsbehörden durch die Verordnung (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten insb. Befugnisse zur Setzung von nichtmonetären Korrekturmaßnahmen eingeräumt.

In diesem Kontext ist darauf hinzuweisen, dass hinsichtlich der Aufsichtssubjekte der FMA bei Verstößen der produktspezifischen Vorschriften des AI Acts **potentiell zusätzlich ein Verstoß (verwaltungsstrafrechtlich-)sanktionierter Bestimmungen des Finanzmarktaufsichtsrechts** vorliegen kann, wenn die Nutzung von Künstlicher Intelligenz in Zusammenhang mit der Erbringung regulierter Finanzdienstleistungen steht.