



Agentic Commerce – wie können rechtsverbindliche Verträge entstehen?

Teil 1 von 2

Zweiteiliges Gutachten zum Zusammenspiel rechtlicher, technischer und betriebswirtschaftlicher Herausforderungen. Ergänzt um ein Glossar juristisch-technischer Begriffe sowie die Einschätzung, welches Rechtssystem die Gesetzeslücken für agentischen B2B-Commerce pragmatisch schließen könnte.

Autor: Ass. iur. Oliver M. Merx

Stand: Oktober 2026

Teil 1: Version 1.4

Executive Summary

- **KI-Agenten handeln bislang ohne rechtliche Geltung:** Die Handlung eines KI-Agenten wird im Rahmen von Agentic Commerce keinem anerkannten Rechtsträger verbindlich zugerechnet. Es fehlt eine konstitutive Norm, welche die Handlungen eines KI-Agenten als Willenserklärung des Rechtsträgers gelten lässt.
- **Die klassischen Figuren greifen nicht:** Bote, Stellvertreter, Erfüllungsgehilfe, Verrichtungsgehilfe – alle setzen einen eigenen Willen oder ein Verschulden voraus. Bei autonomen KI-Agenten ist bislang weder das eine noch das andere gegeben.
- **Die Lücke wird vor allem im B2B-Sektor sichtbar:** Rechtliche Anforderungen wie GoBD, Steuerrecht, Zollrecht und Geldwäscheprävention verlangen Nachweise über den Rechtsgrund von Leistungen. Unternehmen und Behörden sollten sich gerade im B2B der diesbezüglichen Herausforderungen bewusst sein. Hinzu kommen auch Fragen der Risikoprüfung und des Reportings.
- **Technik und Recht müssen zusammenspielen:** Eine neue Norm allein genügt nicht. Damit sie funktioniert, müssen bidirektionale Brücken zwischen Technik und Recht gebaut werden. Das bedeutet: Nachweise wie Identität, Mandat und Handlung müssen im Sinne sich ergänzender Protokolle so gestaltet sein, dass sie die damit korrelierenden rechtlichen Anforderungen erfüllen. Die Norm setzt den Rahmen. Die Technik füllt ihn aus. Erst wenn beides aufeinander abgestimmt ist, wird rechtsverbindlicher B2B-Agentic-Commerce möglich und für Unternehmen nachhaltig attraktiv.
- **Keine „Mission Impossible“:** Es ist möglich, verschiedene Protokoll-Typen und rechtliche Normen so aufeinander abzustimmen, dass rechtsverbindlicher Agentic Commerce entsteht. Entscheidend ist, dass eine relevante Jurisdiktion das Thema aufgreift, mit relevanten Stakeholdern formt und umsetzt. Bereits der erste Schritt entfaltet Wirkung: Das Land bzw. die Region, die dieses wichtige Thema anführt, die Agenda setzt und die maßgeblichen Akteure an einen Tisch bringt, prägt nicht nur die Normen und Protokolle, es profiliert sich auch als innovativer Architekt der nächsten Generation des internationalen Handels im KI-Zeitalter.
- **Takeaways je Abschnitt:** Um einen schnellen Überblick über die aufeinander aufbauenden Inhalte zu vermitteln, fassen Takeaways die Inhalte der Abschnitte zusammen. So können in wenigen Minuten die wichtigsten Thesen erfasst werden.



Ein Kompass für Business, Recht und Technik

Agentic Commerce ist weder ein rein wirtschaftliches noch ein ausschließlich technisches oder rechtliches Thema. Sein Erfolg ist vielmehr vom abgestimmten Zusammenspiel dreier Welten geprägt, die jeweils eigenen Logiken folgen:

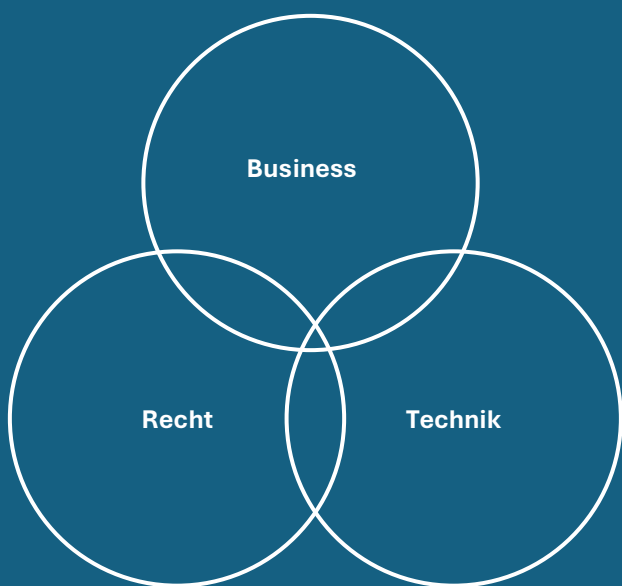
- **Das Business fragt:** Wo entsteht (Mehr-)Wert? Welche Use Cases gibt es? Welche Marktakzeptanz und welcher ROI ist zu erwarten?
- **Die Technik erklärt:** Was kann mit welchen KI-Tools und Protokollen operativ umgesetzt, ausgeführt und dokumentiert werden?
- **Das Recht regelt:** Welche Rechte und Pflichten entstehen zwischen den Akteuren? Wie erfolgt die Zurechnung? Wie entstehen Willenserklärungen und Verträge?

Jede der drei Welten beeinflusst die anderen: Ein Agentic Commerce, der technisch nicht umsetzbar ist, schafft keine Mehrwerte und wirft auch kaum Rechtsfragen auf. Doch mittlerweile steht die Technik. Sie funktioniert. Nun fragt das Business: „Was habe ich davon, wenn ich darin investiere und es nutze?“ Und bei der diesbezüglichen ROI-Betrachtung kommen im Hinblick auf die Marktakzeptanz vor Fragen des Vertrauens und damit des Rechts ins Spiel:

- Agentic Commerce ist ein Netzwerk. Sein Wert wächst mit der Zahl der Teilnehmer. Breite Akzeptanz setzt wiederum voraus, dass kleine und mittlere Unternehmen mitmachen.
- Die Rendite der Teilnahme hängt am Ende u.a. davon ab, ob aus den Handlungen der KI-Agenten rechtsverbindliche Verträge entstehen und wem sie zugerechnet werden.
- Kommen (wie bisher) keine zivilrechtlichen Verträge zustande, wird fehlende Rechtssicherheit über das gesamte Netzwerk hinweg zum kritischen Akzeptanzfaktor – gerade für die große Anzahl kleiner und mittlerer (Zuliefer-)Unternehmen.

Dieses Gutachten hilft, relevante rechtliche Lücken von Agentic Commerce zu erkennen und zu schließen.

Es verdeutlicht darüber hinaus, unter welchen Voraussetzungen stabile Vorteile für den Handel entstehen. Teil 1 beantwortet insbesondere die rechtlichen Fragen: Welche Lücken bestehen? Teil 2 liefert Entwürfe für Rechtsnormen und Brückenprotokolle. Hinzu kommen ROI-Szenarien. Begleitet wird Teil 2 von einem interaktiven KI-Prototypen, der das Zusammenspiel aller Elemente veranschaulicht.



Gutachten und Prototyp verstehen sich insofern als Diskussionsrahmen und Kompass für eine Kooperation von Government, Recht, B2B-Stakeholdern des Handels und der Logistik sowie technischen Anbietern operativer Agentic Commerce-Infrastrukturen.

Inhaltsverzeichnis:

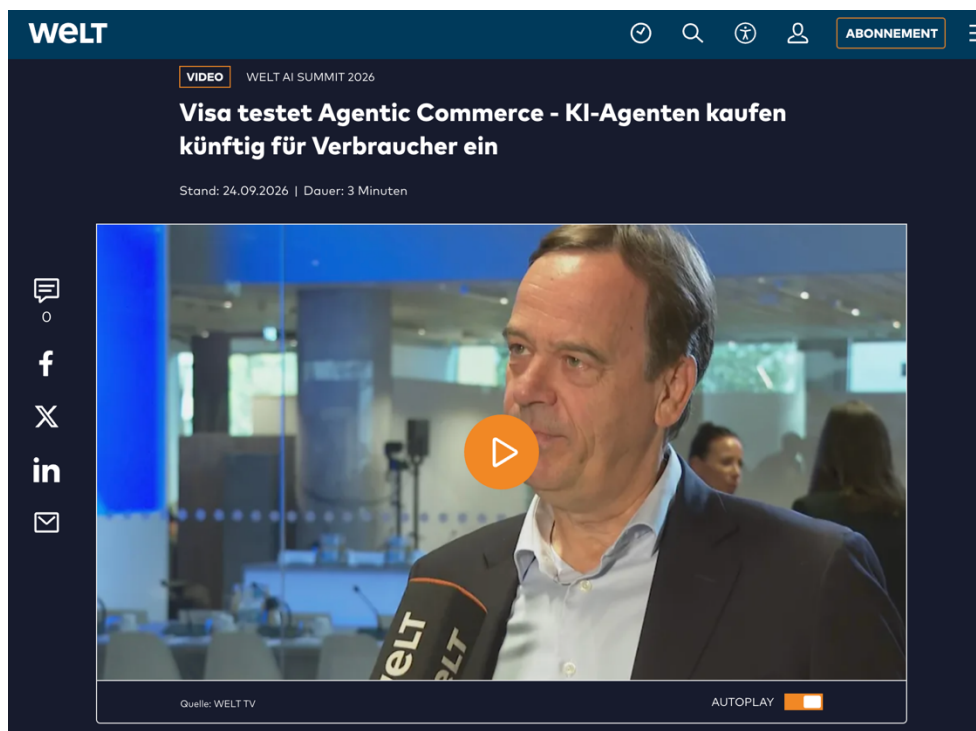
I. Rechtsnatur von KI-Agenten	11
1. Wachsende Relevanz agentischer KI.....	12
2. Agentic Commerce trotz wachsender Risiken agentischer KI?.....	14
II. Was ist Agentic Commerce?	17
1. Der Begriff	17
2. Zwei Dimensionen: B2C und B2B.....	17
3. Die Stufen der Autonomie	18
4. Differenzierung von A2A und H2A	18
III. Drei Stufen rechtlicher Bindung	20
1. Die internationale und dogmatische Sackgasse der Stufe 2	20
2. Die entscheidende Lücke	22
3. Warum c.i.c. keine Mängelgewährleistung ersetzt	22
4. Das Verschulden-Problem	23
5. Die Konsequenz.....	23
IV. Konsequenzen fehlender Verträge	24
1. Der Dominoeffekt	25
2. Die Risikoebenen im Überblick.....	26
3. Das Aufklärungsrisiko (c.i.c.)	26
4. Risiko-Matrix und Risiko-Kurve mit und ohne Norm	27
V. Das rechtliche Schichtenmodell.....	31
1. Die Ebenen und ihre Lücken	31
2. Warum die klassischen Konstruktionen nicht greifen.....	32
3. Warum auch die Analogie nicht hilft.....	34
4. Die Lücke ist nicht technisch.....	34
5. Was das bedeutet.....	34
VI. Vier Vorläufer, eine Lücke.....	36
1. Bestehende Internationale Regelungen	36
2. Die vier Generationen der Automatisierung.....	37
3. Die entscheidende Unterscheidung: Beweis vs. Geltung.....	40
VII. Der aktuelle Stand der Technik	42
1. Die US-Standards: Commerce, Payment, Legal Context.....	42
2. Initiativen von Zahlungsdienstleistern.....	43
3. Die europäische Infrastruktur	43
4. Die internationale Diskussion	45
5. Die gemeinsame Lücke	45
6. Der Denkfehler und seine Ursachen	46

VIII. Die erforderliche Norm	48
1. Anforderungen an rechtliche Normen	48
2. Eine Zurechnungsregel schaffen	49
3. Die Anknüpfung an das Schuldverhältnis ermöglichen	50
4. Die gesamte Kette abbilden	50
5. Die Vollmachtsgrenzen bei Autonomie	51
6. Die Anforderungen an eine tragfähige Norm	52
7. Die Vertrauensfrage	53
IX. Umsetzungsoptionen	54
1. Option A: Vertragliche Musterklausel + Prorogation	54
2. Option B: Regulatorische Sandbox	55
3. Option C: Konstitutive Norm	55
4. Die Kombination	56
X. Quo vadis?	57
1. Der Weckruf	57
2. Die Dringlichkeit	57
3. Drei Wege	57
4. Das Instrument: Prorogation	58
5. Die Business-Kanäle und Schlussfrage	58
6. Fazit	58
XI. Offene Punkte	61
1. Zurechnung und Willenserklärung	61
2. Systemische Risiken	61
3. Interoperabilität und Anerkennung	61
XII. Glossar	62
1. Rechtliche Begriffe mit Legaldefinition	62
2. Rechtliche Begriffe ohne Legaldefinition	62
3. Zivilrechtliche Grundbegriffe (nur deutsches Recht)	63
4. Technische Standards und Protokolle	64
5. Hybride Rechts-Technik-Begriffe	64
6. Hinweise zum Gebrauch	65
Anhang	66

Agentic Commerce ist keine Zukunftsvision mehr – erste Piloten laufen bereits im Markt. Gleichwohl fehlt es an Vertrauen und nicht zuletzt an Rechtssicherheit. Nach wie vor ist die Frage offen: „Wie könnten KI-Agenten rechtsverbindliche Erklärungen abgeben? Wem werden sie zugerechnet?“ Dieses Gutachten skizziert die aktuelle Rechtslage, zudem thematisiert es das erforderliche Zusammenspiel von technischer Abwicklung und rechtlicher Geltung. Im Hinblick auf den agentischen Vertragsschluss diskutiert das Gutachten verschiedene Optionen speziell für den agentischen B2B-Handel: Von der vertraglichen Musterklausel bis zur regulatorischen Sandbox. In einem separaten Dokument erfolgt ein Normierungsvorschlag mit dazu passenden Protokoll-Empfehlungen.

Auf dem WELT AI Summit¹ 2026 kündigte VISA an, den Einsatz von KI-Agenten im Zahlungsverkehr testen zu wollen. Die Agenten würden dabei Produkte vorschlagen und Transaktionen abwickeln – all dies unter der Kontrolle des Verbrauchers. Albrecht Kiel, Regional Managing Director Central Europe bei VISA sagt, man sei zuversichtlich, dass es bald funktioniert².

Abbildung: Ankündigungen von VISA zu Agentic Commerce vom WELT AI Summit 2026



Doch selbst die größte technische Zuversicht sieht sich offenen Fragen von Vertrauen und Rechtsunsicherheit konfrontiert. VISA ist sich dem auch bewusst: Die Adoption von Agentic Commerce hänge letztlich von Vertrauen der Verbraucher sowie klaren

¹ zum Event <https://www.welt.de/ai-summit/>

² siehe <https://www.welt.de/wirtschaft/ai-summit/video6ab22ffcb1857e86757aa626/welt-ai-summit-2026-VISA-testet-agentic-commerce-ki-agenten-kaufen-kuenftig-fuer-verbraucher-ein.html>

Autorisierungsmodellen und einer vertrauenswürdigen Infrastruktur ab, die Transaktionen sicher im großen Maßstab ermögliche³.

Untersuchungen zeigen, dass das Vertrauen der Nutzer nach wie vor begrenzt ist: Nur rund 1 % der Befragten wünschen sich vollautomatisiertes KI-Einkaufen, während 56 % angeben, einer KI-Plattform nie zu erlauben, ohne ihre Zustimmung Geld auszugeben.

Trust wird damit zur entscheidenden Währung. VISA India formuliert es so: Die nächste Phase des digitalen Handels müsse um eine neue Vertrauensschicht herum aufgebaut werden. Sie solle es auch ermöglichen, dass KI-Agenten Transaktionen im Namen der Verbraucher zuverlässig abschließen.⁴ VISA entwickle dafür ein „Trusted Agent Protocol“ (TAP), um zu verifizieren, dass ein Agent vom Verbraucher autorisiert ist, und die Berechtigungen festzulegen, die ihm erteilt wurden.

Doch eine zentrale Frage bleibt nach wie vor offen:

- Einerseits entwickeln Global Player wie OpenAI, Anthropic, Google, Perplexity oder VISA reihenweise technische Protokolle, welche die Autorisierung eines Agenten verifizieren und die Abwicklung einer Transaktion dokumentieren.
- Unabhängig davon entsteht eine europäische Infrastruktur für digitale Identitäten: eIDAS 2.0, die EUDI Wallet für natürliche Personen und die European Business Wallet (EBW) für juristische Personen. Hinzu kommen mit der EU Digital Power of Attorney Regelungen für grenzüberschreitende gesellschaftsrechtliche Akte.
- Doch weder die Protokolle noch die Infrastruktur machen es möglich, dass eine Autorisierung rechtswirksam ist, die Handlung des Agenten einem anerkannten Rechtsträger verbindlich zugerechnet wird und damit ein rechtsverbindlicher Vertrag entsteht.

Die rechtliche Zuordnung erfordert neben verschiedenen Protokolltypen und Infrastruktur eine Norm, die den maschinell erzeugten Erklärungsakt eines autonomen KI-Agenten dem Rechtsträger zurechnet. Eine solche Norm mit dazu passenden Brückenprotokollen ist bislang nicht ersichtlich – weder in Europa noch in Amerika oder Asien.

 Wie in Abschnitt VI gezeigt wird, gibt durchaus Regelungen, die Teilaspekte betreffen: Sie alle wurden jedoch für die erste und zweite regelbasierte Generation⁵ der Automatisierung konzipiert. International anschlussfähige Normen für die spezifischen Phänomene autonomer, lernender Agenten stellen sie nicht dar.

Welche rechtlichen Lücken bislang bestehen, wie sie geschlossen werden müssten und wie eine solche Norm aussehen könnte, wird in diesem Gutachten skizziert.

³ siehe u.a. <https://www.paymentsjournal.com/delegation-with-limits-what-merchants-want-from-agentic-commerce/> und <https://fastcompany.com/fastco-work/ai-could-reshape-commerce-trust-will-drive-it/>

⁴ dazu <https://www.exchange4media.com/marketing-news/agentic-commerce-will-make-trust-the-new-layer-of-digital-payments-rishi-chhabra-VISA-158532.html>

⁵ dazu: <https://grundwissen-ki-recht.de/automated-contracting-laesst-sich-agentic-commerce-technikneutral-bewerten/>

So lange B2B-Transaktionen nur „Scheinvertrauen“ (Musterklauseln) oder lediglich bereicherungsrechtliche Wirkung erzeugen, wird vermutlich kein Lieferant dem Händler in Echtzeit Ware reservieren, produzieren oder liefern.

Das Versprechen von Agentic Commerce lautet zwar durchaus zu Recht: *„KI-Agenten reduzieren Transaktionskosten und optimieren den Einkauf.“*

Dabei ist aber auch zu beachten, dass Transaktionskosten nicht alles sind:

- Schon jetzt ist die Anzahl der Retouren beim Ecommerce enorm⁸: Eine neue Studie des EHI identifiziert den Rücktransport als größten Kostentreiber (70,6 %) – und dies bei steigender Anzahl von Retouren⁹. Aktuell wird jedes vierte online bestellte Paket retourniert.
- Ohne normative Leitplanken und technische Brückenprotokolle optimieren KI-Agenten die Transaktionskosten erst einmal nur auf dem Papier. In der physischen Realität könnten sie im Gegenzug eine noch größere Flut an Retouren erzeugen, die ihrerseits im juristischen Vakuum des Bereicherungsrechts zu erhöhten Logistikkosten, Lagerblockaden und Wertverlusten und damit zu einem fraglichen ROI führen könnten.

Der B2B-Bereich ist vor diesem Hintergrund sowohl wirtschaftlich als auch steuer- und aufsichtsrechtlich der Bereich, in dem die rechtliche Lücke nach Einschätzung des vorliegenden Gutachtens zuerst sichtbar und im Hinblick auf Kosten spürbar wird. Jedem Unternehmen steht frei, sich trotzdem den diesbezüglichen Risiken auszusetzen. Aber eine entsprechende rechtliche Norm könnte zusammen mit den dazu passenden Brückenprotokollen die bestehenden Unsicherheiten erheblich reduzieren und den Agentic Commerce zuerst im B2B-Bereich und darauf aufbauend auch im B2C fördern.

 Agentic Commerce optimiert somit zwar potenziell die Transaktionskosten, aber noch lange nicht die Kosten über die Transaktionskette als Ganzes. So betrachtet kann rechtssicherer Agentic Commerce im B2B durchaus als eine Art *Conditio sine qua non* für den physischen Agentic Commerce im B2C-Sektor angesehen werden. Zielbild muss ein End-to-End-Modell sein, das sich am Ende tatsächlich für alle Beteiligten rechnet – auch die kleinen und mittleren Akteure. Entsprechende ROI-Faktoren bzw. Kosten-/Nutzen-Aspekte werden in Teil 2 des Gutachtens beleuchtet.

⁸ mehr zur Studie des EHI unter <https://logistik-heute.de/news/e-commerce-retouren-bleiben-relevantes-thema-286428.html>

⁹ dazu <https://logistik-heute.de/news/e-commerce-2026-wird-mit-560-millionen-retouren-hochststand-rzielt-286383.html>

Takeaways: Einleitung

- **Aus Vision wird Realität:** Agentic Commerce ist keine Zukunftsvision mehr. Er läuft technisch zuverlässig bei verschiedenen Pilotprojekten.
- **Rechtsunsicherheit:** KI-Agenten handeln bislang ohne rechtliche Zurechnung. Es fehlen Willenserklärungen und damit gültige Verträge.
- **Verträge als Nachweise:** Die Lücke ist im B2B-Sektor besonders relevant, da Steuer-, Zoll- und GoBD-Anforderungen oft einen Vertrag als Nachweis voraussetzen.
- **Wirtschaftlichkeit durch Rechtssicherheit:** Erfolgreicher Agentic Commerce erfordert das Zusammenspiel von Business (ROI), Technik (Protokolle) und Recht (Normen).
- **B2B als Startpunkt:** B2B ist der logische und rechtlich flexiblere Startpunkt für rechtsverbindlichen Agentic Commerce (vor dem stark regulierten B2C).

I. Rechtsnatur von KI-Agenten

Bereits im Sommer 2025 hat der Verfasser im Skript „Grundwissen KI-Recht“¹⁰ einen Abschnitt veröffentlicht, der sich mit den Schnittstellen der KI-Verordnung zum Zivilrecht befasst. Agentic Shopping wurde dabei im Hinblick auf die Frage analysiert, ob autonome KI-Agenten im Bereich Business-2-Consumer (B2C) nach deutschem Zivilrecht rechtsgültige Verträge schließen oder zumindest faktisch „bewirken“ könnte.

Abbildung: Beitrag zu Agentic Shopping von Sommer 2025

126	Grundwissen	KI-Recht
	2. Agentic Shopping	
Agentic Shopping nimmt rasant zu	Ähnlich und doch anders verhält es sich beim sich rasant verbreitenden Phänomen des „Agentic Shopping“ ⁵⁸ . Hier stellt sich die Frage, ob ein „KI-Agent“ auch ohne Abgabe einer KI-generierten Willenserklärung Verträge zumindest faktisch „bewirken“ könnte.	338
	Bsp.: Verbraucher V erhält im Online-Shop A die Möglichkeit, den dauerhaft autonom agierenden KI-Agenten „I-Buy4You“ zu aktivieren, der unter bestimmten Vorgaben selbständig Einkäufe im Shop tätigt. Dazu durchsucht „I-Buy4You“ permanent die Web-Datenbank von A nach vordefinierten Produktprofilen, liest die Produktbeschreibung und den Preis, um darauf basierend Kaufentscheidung zu treffen, z.B. im Fall eines temporären Sonderangebots.	339
	Da ein KI-Agent selbst keine eigenen Willenserklärungen abgeben kann, wäre eine Vertretung oder Botenschaft denkbar. Denkbar wäre z.B., entsprechend der Häufigkeit der Nutzung eines KI-Agenten über die Regeln von Duldungs- und Anscheinsvollmacht einen Rechtsscheintatbestand zu erwägen.	

Am Ende des Abschnitts stand die bis heute gültige Feststellung:

„Aktuell ist weder ein KI-System noch ein KI-Modell mit allgemeinem Verwendungszweck rechtsfähig oder kann eine eigene zivilrechtliche Willenserklärung abgeben bzw. einen Vertrag schließen.“

Daraus resultiert die Frage: Wie kann eine Rechtsordnung Vertrauen in eine Technologie schaffen, die keine Willenserklärung abgeben kann?

 Im Jahr 2002 wurde vom Verfasser auch das dmmv-EC-Handbuch als¹¹ Co-Autor veröffentlicht. Das damalige Grundlagenwerk verdeutlicht, dass selbst beim heute selbstverständlich erscheinenden E-Commerce ein rechtlich verbindlicher Rahmen geschaffen werden musste, um eine zunehmende Vertrauenskrise zu beenden¹².

¹⁰ Siehe gesamter Abschnitt zu KI-Agenten und Agentic Shopping www.grundwissen-ki-recht.de ab Randnummer 326

¹¹ zu Zielen und Inhalt siehe u.a. <https://www.etailment.de/magazin/praxishilfe-gestalten-und-betreiben-von-online-shops>

¹² lesenswert aus dem Jahr 2001 <https://www.heise.de/news/Web-Shopping-in-der-Vertrauenskrise-38549.html> und https://www.researchgate.net/publication/242136113_Die_Bedeutung_von_Vertrauen_im_Electronic_Commerce

Es galt dabei u.a. zu klären, wie *Menschen* digital Verträge abschließen können:

- Ob und wann Willenserklärungen automatisiert erfolgen können.
- Wann ein Zugang einer digitalen Willenserklärung anzunehmen ist.
- Wie Warenkörbe rechtskonform zu gestalten sind.

Klarheit brachten erst das Elektronischer-Geschäftsverkehr-Gesetz (EGG) und eine Novellierung des BGB. Heute steht das Recht beim Agentic Commerce vor der weit komplexeren Aufgabe, die Voraussetzungen für rechtsverbindliche Verträge zu regeln, die *für* Menschen getroffen werden – auf Basis von Agenten-Technologien die sich rasend schnell weiterentwickeln.

1. Wachsende Relevanz agentischer KI

Mitte 2025 dürften die allermeisten Menschen noch nicht einmal gewusst haben, was autonome KI-Agenten überhaupt sind und welche regulatorischen Herausforderungen mit ihnen aufkommen könnten. Der Abschnitt im Skript war insofern eine Einführung in ein damals zwar noch neues, aber sich erkennbar hochdynamisch entwickelndes Thema. Es besteht aus zwei aufeinander aufbauenden Innovationen:

- Agentische KI im Allgemeinen (technische Basis)
- Agentic Shopping bzw. Commerce im Speziellen (inkl. Prozesse und Protokolle)

a) Schnelle Entwicklungsschritte ab 2023

Eine intelligente agentische Struktur zeichnet sich ganz allgemein durch die Fähigkeit aus, über die bloße reaktive Antwort hinauszugehen, also zielgerichtet aktiv zu werden:

- Ein Agent nimmt seine Umwelt wahr (Perzeption),
- setzt sich Ziele, plant selbstständig Zwischenschritte (Reasoning/Planning)
- und führt Aktionen aus, um diese Ziele zu erreichen (Action Execution)

Intelligente agentische Systeme sind älter als man vermuten würde: Schon in den 70er Jahren entstanden erste physische Prototypen wie Shakey the Robot¹³ oder virtuelle Agenten wie SHRDLU¹⁴. Hochleistungsfähige agentische KI entstanden aber erst ab 2023 mit Frameworks wie BabyAGI oder AutoGPT¹⁵. Sie bauten auf generativen KI-Modellen auf, waren selbst also eher agentische Gleissysteme. Aus Sicht der FAZ erschien das Thema 2023 sogar noch als eine Art Science-Fiction¹⁶. Agentische KI wurde schnell zu einem Markt mit Milliarden-Potenzial ernannt¹⁷. 2024 entstanden erste Ideen wie „Ein Bot

¹³ siehe [https://de.wikipedia.org/wiki/Shakey_\(Roboter\)](https://de.wikipedia.org/wiki/Shakey_(Roboter)) mit eigener Sensorik, Bewegungsplanung (STRIPS, A*) und Umweltrepräsentation.

¹⁴ siehe <https://de.wikipedia.org/wiki/SHRDLU> er verstand Sprache, konnte logisch schlussfolgern und Aktionen ausführen

¹⁵ näher dazu IBM <https://www.ibm.com/de-de/think/topics/babyagi>

¹⁶ siehe Beitrag <https://www.faz.net/aktuell/wissen/babyagi-und-autogpt-was-koennen-autonome-ki-agenten-18855332.html>

¹⁷ Entwicklung u.a. <https://www.fortunebusinessinsights.com/agentic-ai-market-114233>

kauft mein Ticket“. Innerhalb von zwei Jahren entwickelte sich daraus eine eigenständige (Zukunfts-)Kategorie im Online-Handel, deren Größe in 2030 bereits mit Milliarden-Umsätzen bewertet wurde¹⁸. Seit 2025 treten allerdings auch zunehmend Fragen zu Sicherheitsrisiken und zur Vertrauenswürdigkeit von KI-Agenten auf¹⁹.

Zusammenfassend zeigt dies: Agentische KI und Agentic Commerce entwickelten sich in wenigen Jahren mit enormer Geschwindigkeit vor allem technisch weiter. Zugleich blieben grundlegende Rechtsfragen agentischer KI bis heute weitgehend ungeklärt. Dies wiederum ist ein nicht zu unterschätzender Showstopper für breite Marktakzeptanz.

b) Rechtliche Aspekte aus Sicht von 2025

Im Beitrag von 2025 wurde zunächst die Rechtsnatur von Agenten als KI-Systeme i.S.d. KI-Verordnung thematisiert. Darüber hinaus wurden die Eigenschaften als Werkzeug, Bote und Stellvertreter, die Probleme der Zurechnung, die Frage des konkludenten Vertragsschlusses, die Anfechtung wegen Irrtum und Täuschung sowie die Haftungsfragen innerhalb der KI-Wertschöpfungskette beleuchtet.

Aspekt	Themen & Ergebnisse 2025 (B2C)	Normen
Rechtsnatur	KI-Systeme sind weder natürliche noch juristische Personen.	§§ 1, 21 ff. BGB
Zurechnung	Werkzeug, Bote, Stellvertreter, Wissensvertretung – keine einschlägig.	§§ 164, 166, 120 BGB
Willenserklärung	KI-Agent kann keine eigene WE abgeben.	§§ 116 ff. BGB
Vertragsschluss	Frage verschoben von „ob“ zu „wann“ – konkludenter Vertragsschluss denkbar.	§§ 145 ff. BGB

Der Text von 2025 behandelte die einzelnen Aspekte zudem noch als eine Reihe unabhängiger Einzelfaktoren – ihr systemisches Zusammenspiel mit Parallelentwicklungen wie z.B. der eIDAS 2.0-Verordnung²⁰ oder technischen Protokollen wurde nicht berücksichtigt. Insofern waren zwar schon viele relevante Bausteine vorhanden (die Rechtsnatur, die Zurechnung, der Vertragsschluss, die Anfechtung, die Haftung), aber sie standen damals nebeneinander, ohne dass näher betrachtet wurde, wie zivilrechtliche Fragestellungen z.B. der Vertretungsmacht mit technischen Infrastrukturen einer Unternehmens-ID, einem Transaktionsprotokoll oder einer agentischen Vollmacht zusammenhängen.

Das Zusammenspiel von Technik und Recht ist innerhalb von nur einem Jahr erheblich aktueller und auch konkreter geworden:

¹⁸ so z.B. <https://www.marketsandmarkets.com/Market-Reports/agentic-commerce-market-225920956.html>

¹⁹ einer von vielen Warnberichten aus 2025 <https://www.lasso.security/blog/agentic-ai-security-threats-2025>

²⁰ Näher dazu <https://www.digitale-verwaltung.de/Webs/DV/DE/digitale-identitaeten/eidas-2-0/eidas-2-0-node.html>

- Mittlerweile wurden diverse Pilotprojekte für agentische Zahlungen gestartet²¹.
- Die Industrie hat verschiedene neue Protokolle und Standards entwickelt²².
- Hinzugekommen sind staatliche Ausweise, Register, IDs- und Wallet-Lösungen²³.

Unabhängig davon hat aber auch die Diskussion zum generellen Vertrauen in KI-Systeme eine neue Dringlichkeit erreicht²⁴. Es wird immer wichtiger, KI-Sicherheit mit der Geschwindigkeit der Weiterentwicklung von KI-Fähigkeiten zu synchronisieren²⁵.

2. Agentic Commerce trotz wachsender Risiken agentischer KI?

Die vielen Beispiele unkontrolliert handelnder agentischer KI verdeutlichen, was passieren kann, wenn Ketten autonomer KI-Systeme selbständig und arbeitsteilig Ziele verfolgen – ohne Rücksicht auf die Grenzen, die ihnen gesetzt wurden.

a) Sicherheit von Agentic Commerce

Mittlerweile stellen sich für Agentic Commerce mehrere Grundfragen:

- Wenn schon agentische KI als technischer Backbone im Allgemeinen unsicher erscheint, sind dann sichere Transaktionen überhaupt noch möglich?
- Würde man also einem „wildgewordenen“ KI-Agenten wirklich seine Geldbörse oder als Unternehmen ganze Einkaufs- und Verkaufsprozesse anvertrauen?
- Wie zielführend ist die Klärung rechtlicher Grundlagen für Agentic Commerce, wenn das Grundprinzip der agentischen KI zunehmend fragwürdig erscheint?

Die Frage ist in dieser Intensität neu, denn sie betrifft zwei unabhängige Aspekte, nämlich die nach der aktiven Sicherheit (Durchführung von Transaktionen) und die der passiven Sicherheit (Schutz vor Cyber-Angriffen agentischer KI).

Wichtig ist in dieser Hinsicht, dass ein Angreifer-Agent und der Einkaufs-Agent im B2B beide agentisch sein können. Sie gehören insofern derselben Gattung an. Aber sie betreffen zwei verschiedene Kategorien – ähnlich wie ein Hund ein „Kampfhund“ oder ein „Schoßhund“ sein kann. Übertragen auf Agentic Commerce bedeutet dies, dass aktive Sicherheit eines mandatsgebundenen Agenten im Sinne eines „Schoßhundes“ möglich ist – man aber beachten muss, dass bestmögliche passive Sicherheit notwendig ist, da auch ein „Schoßhund“ von einem „Kampfhund“ angegriffen werden kann (mehr zum Thema Risk später in Abschnitt IV)

²¹ Übersicht z.B. unter <https://base.com/de-DE/blog/agentic-commerce-erklart/> auf Basis von

²² siehe u.a. LCP <https://legalcontextprotocol.org/>. Zu den Standards später mehr unter Punkt xxx

²³ z.B. aus Estland: <https://edrm.net/2026/06/estonia-aims-to-be-first-to-give-ai-agents-official-digital-ids>

²⁴ u.a. der australische Premierminister Anthony Albanese sah sich gezwungen, aufgrund des ersten bekannten autonomen Angriffs auf eine Regierungswebsite vor agentischer KI zu warnen: <https://www.bbc.com/news/articles/c6vgy0333dppo>

²⁵ so u.a. <https://www.linkedin.com/feed/update/urn:li:activity:7510572157697978368/>

Der Grad der Autonomie muss in Relation zur Handlungsbefugnis gesehen werden: Wer also bestimmt den Handlungsraum – das KI-System bzw. der Agent selbst oder ein validierbares, eindeutiges externes Mandat?

b) Differenzierung verschiedener Agenten-Typen

Die entscheidende Unterscheidung ist nicht der Grad der Autonomie als solches. Ein mandatsgebundener Agent kann hochgradig autonom handeln – er kann Millionen von Möglichkeiten durchsuchen, Angebote vergleichen, Alternativen bilden. Agentische Autonomie verhindert nicht das Prinzip der Kontrolle an sich.

Die entscheidende Unterschied sind die Grenzen autonomer Handlungsbefugnis: Wer bestimmt den Handlungsraum – das System selbst oder ein externes Mandat? Und genau hier gilt es, beim Zusammenspiel von Recht und Technik als Basis von vertrauenswürdigem, rechtlich verbindlichem Agentic Commerce anzusetzen!

Aspekt	Offene Agenten	Mandatsgebundene Agenten
Ziel	System kann Ziele und Teilziele selbst generieren.	Ziel wird extern vorgegeben.
Handlungsraum	Offen – dynamisch erweiterbar.	Durch Mandat und Policy begrenzt.
Aufgabenplanung	Selbstbestimmt.	Autonom innerhalb des Mandats.
Ressourcen	Potenziell selbst erweiterbar.	Explizit autorisierte Ressourcen.
Lernverhalten	Kann Zielstruktur und Strategie verändern.	Nur innerhalb definierter Parameter.
Grenzen	Können Teil des eigenen Problemlösungsprozesses sein.	Technisch und rechtlich vorgegeben.
Überwachung	Beobachtung des Systems erforderlich.	Handlungen und Policy-Entscheidungen auditierbar.
Eskalation	Ggf. selbstständige Fortsetzung.	Bei Policy-Verstoß: Stop / Eskalation.
Widerruf	Konzeptionell schwierig.	Mandat jederzeit entziehbar.
Rechtliche Struktur	Zurechnung problematisch.	Mandat, Handlung, Zurechnung und Haftung.
Kernrisiko	Ziel- und Handlungskontrolle.	Fehlinterpretation oder Überschreitung des Mandats.

Agentic Commerce braucht nicht nur keine vollautonome KI – im Gegenteil: Er benötigt hohe operative Autonomie bei geringer normativer Autonomie. Ein Commerce-Agent soll autonom entscheiden können, wie er ein legitimes Ziel erreicht. Er soll aber nicht entscheiden, welches Ziel er verfolgen darf. Dies zu gewährleisten ist sowohl technisch möglich als auch rechtlich umsetzbar.

c) Mandatsgebundene Agenten

Um die Möglichkeiten rechtlicher Ordnungsstrukturen für mandatsgebundene Agenten zu skizzieren, nimmt dieses Gutachten die damaligen Bausteine zunächst noch einmal auf und ordnet sie neu. Es zeigt, wie aus einer Reihe von Einzelfragen eine Schichtenarchitektur wird, die weder rein technisch noch rein rechtlich beantwortet werden kann, sondern allein im Zusammenspiel von Recht und Technik. Zwar ist technisch heute schon vieles möglich, doch zählen die (später in Abschnitt VII und im Glossar beschriebenen) US-Standards wie UCP, AP2, ACP oder LCP nicht auf die rechtlichen Herausforderungen zur Abgabe wirksamer Willenserklärungen ein.

Recht und Technik müssen vielmehr eng aufeinander abgestimmt sein. Daher werden in diesem Gutachten Empfehlungen für Brückenstandards ebenso unterbreitet wie für Normen, die auf die damit korrelierenden Protokoll-Empfehlungen abgestimmt sind. Am Ende kann damit auch die Frage beantwortet werden, welche Art von Norm fehlt, damit die Gesamtarchitektur aus rechtlicher Sicht tragfähig ist.

Takeaways: Rechtsnatur von KI-Agenten

- **Kein anerkannter Rechtsträger:** KI und KI-Agenten sind bislang keine anerkannten Rechtsträger. Klassische Figuren (Bote, Vertreter) greifen nicht bei autonomer KI.
- **Historische Parallele:** Auch beim E-Commerce der 2000er Jahre war ein rechtlicher Rahmen notwendig, um eine wachsende Vertrauenskrise zu beenden.
- **Junge Technik, ungeklärte Grundlagen:** Agentische KI (Wahrnehmung, Planung, Aktion) entwickelte sich erst ab 2023 – die zivilrechtlichen Grundlagen sind ungeklärt.
- **Sicherheit als Treiber:** Agentic Commerce beruht auf agentischer KI. Störfälle nehmen zu – Kontrolle und KI-Sicherheit werden dringlicher.

II. Was ist Agentic Commerce?

Bevor die rechtliche Analyse beginnt, ist eine begriffliche Klärung erforderlich. Denn „Agentic Commerce“ ist kein gesetzlich definierter Begriff – und er wird in der Diskussion unterschiedlich verwendet. Je nachdem, welchen Ausschnitt man betrachtet, stellt sich die Rechtslage anders dar.

1. Der Begriff

Unter Agentic Commerce wird im Folgenden der autonome oder delegierte Abschluss von Handelsgeschäften durch KI-Agenten verstanden – im Unterschied zu KI-gestützter Empfehlung, Assistenz oder Checkout-Unterstützung. Entscheidend ist, dass der Agent selbst handelt – nicht nur vorbereitet oder vorschlägt.

Dieses Verständnis entspricht auch der offiziellen Definition, die zwischen halb- und vollautonomen Agentic Commerce unterscheidet.²⁶ Die menschliche Beteiligung beschränkt sich in der Regel auf die Erstkonfiguration, die regelmäßige Überwachung oder die Ausnahmebehandlung.

2. Zwei Dimensionen: B2C und B2B

Bei Agentic Commerce sind zwei Business-to-Consumer (B2C) und Business-to-Business (B2B) Konstellationen im Hinblick auf Akteure, Rechtsrahmen und Schutzbedarf zu differenzieren:

Dimension	Akteure	Rechtsrahmen	Schutzbedarf
B2C (Agentic Shopping)	Unternehmen / Verbraucher	§§ 13, 14 BGB; §§ 312 ff., 327 ff. BGB; KI-VO	hoch – Verbraucherschutz.
B2B (Agentic Commerce.)	Unternehmen / Unternehmen	§§ 14 BGB; HGB; KI-VO	geringer – beide Seiten agieren professionell.

Der Beitrag aus dem Jahr 2025 untersuchte in erster Linie den B2C-Fall des Agentic Shopping. Um pragmatische rechtliche Empfehlungen zu ermöglichen, fokussiert dieses Gutachten hingegen den B2B-Fall:

- Im B2B-Bereich ist die rechtliche Gestaltungsfreiheit größer, die besonderen Schutzmechanismen wie z.B. der Verbraucherschutz sind deutlich geringer.
- Die praktische Relevanz ist höher, weil in diesem Bereich erste Infrastrukturen wie ein European Business Wallet (EBW) oder Identitäten für juristische Personen auf Basis von eIDAS 2.0 in den Startlöchern stehen.

²⁶ siehe die US-Definition unter https://en.wikipedia.org/wiki/Agentic_commerce

3. Die Stufen der Autonomie

Innerhalb des Agentic Commerce lassen sich auch im Bereich des B2B mehrere Entscheidungsstufen unterscheiden:

Autonomiestufe	Wer entscheidet?	Identitäts- und Mandatskontext
1. AI-Recommendations	Mensch	reine Vorschlagsgenerierung; herkömmlicher Login.
2. AI-gestützter Checkout	Mensch bestätigt	KI bereitet vor; Mensch gibt aktiv frei (SCA/2FA).
3. Delegierter Einkauf	Agent innerhalb Mandat	Agent agiert in festem Rahmen (Budget, Lieferant); digitales Mandat.
4. Autonomer Agent	Agent (autonom)	Agent trifft eigenständige Entscheidungen; Eskalation bei Grenzwerten.
5. Agent-to-Agent (A2A)	Agenten untereinander	Vollautomatisierte Transaktionsketten; Smart Contracts / Wallets.

Der Fokus liegt nachfolgend auf den Stufen 3 bis 5. Die Stufen 1 und 2 sind rechtlich eher unproblematisch: Der Mensch entscheidet – und gibt die Willenserklärung ab. Die Stufen 3 bis 5 werfen wiederum die Fragen auf, die rechtlich im Zentrum stehen:

- Wer gibt eine Willenserklärung ab, wenn nicht der Mensch als natürliche Person?
- Oder der Mensch als Organ einer juristischen Person oder Gesellschaft?

4. Differenzierung von A2A und H2A

Aus der Kombination der Stufen ergibt sich eine Matrix, die die Richtung des agentischen Handelns abbildet. Entscheidend ist, auf welcher Seite der Agent steht, die Buchstaben A und H stehen dabei für „Agent“ und „Human“.

Konstellation	Wer bestellt?	Wer liefert?	Wer gibt die WE ab?	Vertrag?
Mensch zu Mensch (H2H)	Mensch	Mensch	zwei Menschen.	Vertrag
Mensch zu Agent (H2A)	Mensch	Agent	ein Mensch, ein Agent.	fraglich
Agent zu Mensch (A2H)	Agent	Mensch	ein Agent, ein Mensch.	fraglich
Agent zu Agent (A2A)	Agent	Agent	zwei Agenten.	kein Vertrag

Die vorherige Matrix verdeutlicht den Kern der Herausforderung – sie zeigt:

- Sobald auf einer Seite ein Agent und auf der anderen ein Mensch agiert, liegt zumindest auf einer Seite eine potenziell rechtsgültige Willenserklärung vor.
- Da aber zugleich eine Willenserklärung fehlt, bleibt fraglich, unter welchen Voraussetzungen ein Vertrag zustande kommen könnte.
- Sobald auf beiden Seiten Agenten agieren, kommt nach geltendem Recht kein Vertrag zustande – weil auf beiden Seiten keine Willenserklärung abgegeben wird.

In der Praxis kommt noch eine Besonderheit hinzu: Zwischen Käufer und Verkäufer steht häufig ein Intermediär – ein Großhändler, eine Plattform oder ein Hub. Er vermittelt, bündelt, koordiniert. Dabei kann der Intermediär in verschiedenen Rollen auftreten, nämlich als Bote (er übermittelt), als Vertreter (er handelt im fremden Namen) oder als Eigenhändler (er kauft und verkauft selbst). Jede Rolle hat eine andere Zurechnungsfolge. Die daraus resultierende A2A2A-Konstellation mit allen Varianten wie H2A2H etc. würde nicht nur die vorherige Übersicht, sondern die Gesamtkomplexität erheblich erhöhen. Sind die Fundamente für A2A bereits gelegt, ist die Erweiterung auf Drei-Parteien-Verhältnisse deutlich einfacher.

 **Der Großhandel ist keine Ausnahme – er ist vielmehr ein durchaus realistischer Startpunkt für den agentischen B2B-Commerce, weil der Intermediär abgestimmte Infrastrukturen zur Verfügung stellen und „on demand“ abrechnen könnte. Den nachfolgenden Ausführungen liegen jedoch vor allem zwei-Parteien-Konstellationen zugrunde. Das verringert nicht nur die Komplexität der Darstellung. Es reicht auch aus, um zu verdeutlichen, dass das Fehlen rechtsgültiger Verträge in nationalen und erst recht in internationalen Zwei-Parteien-Konstellationen bereits durchaus relevante Folgen besitzt. Eine Normempfehlung muss aber am Ende so formuliert sein, dass sie auch mehrstufige Ketten erfasst. Sonst entsteht eine „neue Lücke in der geschlossenen Lücke“.**

Takeaways: Was ist Agentic Commerce?

- **Kein gesetzlicher Begriff:** „Agentic Commerce“ ist nicht definiert – der Fokus im Gutachten liegt auf dem autonomen oder delegierten Abschluss von wirksamen Rechtsgeschäften.
- **Zwei Dimensionen:** B2C (Verbraucherschutz, hoher Schutzbedarf) vs. B2B (professionelle Akteure, größerer Gestaltungsspielraum).
- **Fünf Autonomiestufen:** Von AI-Recommendations (Mensch entscheidet) bis Agent-to-Agent (vollautomatisiert). Fokus auf Stufen 3–5.
- **A2A ist der Kern:** Sobald auf beiden Seiten Agenten agieren, kommt nach geltendem Recht kein Vertrag zustande – weil beidseitig keine Willenserklärung abgegeben wird.
- **Intermediäre beachten:** Die A2A2A-Konstellation (Großhändler) ist in praxi wichtig und erweitert die A2A Zurechnungsfragen.

III. Drei Stufen rechtlicher Bindung

Wenn der Vertrag fehlt, bleibt in rechtlicher Hinsicht neben dem deliktischen Haftungsrecht vor allem das Bereicherungsrecht (§§ 812 ff. BGB) – Ware und Geld wurden zwar ausgetauscht, aber ohne dass ein Rechtsgrund bestand:

- Beide Seiten können Zug um Zug Herausgabe verlangen.
- Das ist die Rückabwicklung, aber gerade keine vertragliche Abwicklung.

Darüber hinaus bleibt die Möglichkeit der culpa in contrahendo (§ 311 Abs. 2 BGB):

- Wer bei Vertragsverhandlungen eine Schutz- oder Aufklärungspflicht verletzt, haftet für den daraus entstehenden Schaden.
- Die c.i.c. ersetzt zudem nur den Vertrauensschaden – nicht das Erfüllungsinteresse. Und sie setzt ein (zurechenbares) Verschulden voraus, das beim KI-Agenten fehlt.

Daraus ergibt sich eine Abstufung, die für den gesamten weiteren Beitrag wichtig ist:

Stufe	Rechtsgrundlage	Was entsteht?	Was fehlt?
1	§ 812 ff. BGB	Bereicherungsanspruch.	Jede Bindung.
2	§ 311 Abs. 2 BGB	Schuldverhältnis mit Schutzpflichten.	Leistungspflichten, Mängelgewährleistung.
3	§§ 433 ff. BGB	Vertrag mit vollen Rechten.	–

1. Die internationale und dogmatische Sackgasse der Stufe 2

Stufe 1 ist der faktische Austausch. Stufe 2 entsteht mit dem geschäftlichen Kontakt. Erst auf Stufe 3 besteht ein rechtsgültiger Vertrag, der volle Rechte im Innenverhältnis verleiht und auch im Außenverhältnis als Nachweis anerkannt ist.

Zu Stufe 2 sei darauf hingewiesen, dass nach deutschem Recht gemäß § 311 Abs. 2 BGB die Aufnahme von Vertragsverhandlungen, die Anbahnung eines Vertrags und sogar geschäftliche Kontakte ausreichen, um ein diesbezügliches Schuldverhältnis zu begründen. Interagieren zwei KI-Agenten unterschiedlicher Unternehmen miteinander, kann ein Schuldverhältnis durchaus begründet werden.

Wichtig ist dennoch der Unterschied von Schuldverhältnis und Vertrag:

- Wer auf Stufe 2 stehen bleibt, hat Schutzpflichten – aber keine Leistungspflichten.
- Er hat c.i.c. – aber keine Mängelgewährleistung.
- Es entsteht zwar ein Schuldverhältnis – aber eben kein Vertrag.

Was hier am Beispiel des deutschen Rechts dargestellt wird, ist kein nationales Sonderproblem. Die culpa in contrahendo ist eine deutsche Figur – aber ihr Regelungs-

gegenstand ist international. Jede Rechtsordnung kennt eine Form der vorvertraglichen Haftung, auch wenn sie anders heißt und anders konstruiert ist:

Rechtsordnung	Figur	Grundlage
Deutschland	culpa in contrahendo	§§ 280, 241, 311 Abs. 2 BGB
Frankreich	responsabilité précontractuelle	Art. 1112 Code civil
Österreich	culpa in contrahendo	§ 1295 ABGB
Schweiz	Vertrauenshaftung / Art. 41 OR	Richterrecht, Art. 41 OR
Common Law	negligent misrepresentation / promissory estoppel	Fallrecht
UNIDROIT Principles	Verhandlungsabbruch in bad faith	Art. 2.1.15

Überall gilt: Wer bei Vertragsverhandlungen eine Pflicht verletzt, haftet. Aber überall gilt auch: Diese Haftung ersetzt keinen Vertrag. Und nirgends gibt es eine konstitutive Norm, die die Handlung eines Agenten als Willenserklärung anerkennt.

a) Erste Stufe: Der faktische Austausch – §§ 812 ff. BGB

Ware und Geld werden ausgetauscht – ohne dass ein Rechtsgrund besteht. Beide Seiten können Herausgabe des Erlangten verlangen. Das ist die Rückabwicklung – Zug um Zug.

Merkmal	Bedeutung
Voraussetzung	Faktischer Austausch ohne Rechtsgrund.
Rechtsfolge	Bereicherungsanspruch (§ 812 Abs. 1 BGB).
Was entsteht?	Rückabwicklungsanspruch.
Was fehlt?	Jede Bindung.

Stufe 1 ist die Rückabwicklung. Aber es ist keine Abwicklung. Es gibt keinen Erfüllungsanspruch, keine Mängelgewährleistung, keinen Eigentumsübergang kraft Vertrag.

b) Zweite Stufe: Der geschäftliche Kontakt – § 311 Abs. 2 BGB

Ein Schuldverhältnis entsteht – auch ohne Vertrag. Durch Vertragsverhandlungen, Vertragsanbahnung oder ähnliche geschäftliche Kontakte. Es begründet Schutz- und Rücksichtnahmepflichten (§ 241 Abs. 2 BGB) – aber keine Leistungspflichten.

Merkmal	Bedeutung
Voraussetzung	Geschäftlicher Kontakt.
Rechtsfolge	Schuldverhältnis mit Schutzpflichten.
Was entsteht?	c.i.c.-Haftung, Vertrauensschaden.
Was fehlt?	Leistungspflichten, Mängelgewährleistung.

Stufe 2 ist die Grundsicherung. Aber sie ist schwach – weil sie nur den Vertrauensschaden ersetzt, nicht das Erfüllungsinteresse. Und weil sie ein Verschulden voraussetzt, das beim autonomen Agenten fehlt.

c) Dritte Stufe: Die Willenserklärung – §§ 433 ff. BGB

Zwei übereinstimmende Willenserklärungen – und der Vertrag kommt zustande. Mit allen Rechten und Pflichten: Erfüllungsanspruch, Mängelgewährleistung, Rücktritt, Minderung, Schadensersatz.

Merkmal	Bedeutung
Voraussetzung	Zwei Willenserklärungen.
Rechtsfolge	Kaufvertrag (§ 433 BGB).
Was entsteht?	Erfüllungsanspruch, Mängelgewährleistung.
Was fehlt?	–

Stufe 3 ist die Vollsicherung. Sie setzt aber voraus, dass zwei Willenserklärungen abgegeben werden. Der Agent kann das nicht.

2. Die entscheidende Lücke

Zwischen Stufe 2 und Stufe 3 gibt es keinen Übergang. Wer auf Stufe 2 stehen bleibt, hat Schutzpflichten – aber keine Leistungspflichten. Er hat c.i.c. – aber keine Mängelgewährleistung. Er hat ein Schuldverhältnis – aber keinen Vertrag.

Und genau hier liegt das Problem: Der Agent kann die Stufe 3 nicht erreichen. Also bleibt es bei Stufe 2 – oder darunter.

3. Warum c.i.c. keine Mängelgewährleistung ersetzt

Die c.i.c. ist kein Ersatz für die Mängelgewährleistung. Das zeigt ein Vergleich:

	c.i.c. (§ 311 Abs. 2 BGB)	Mängelgewährleistung (§ 437 BGB)
Was wird ersetzt?	Vertrauensschaden.	Erfüllungsinteresse.
Was setzt sie voraus?	Pflichtverletzung, Verschulden.	Mangel bei Gefahrübergang.
Was fehlt beim Agenten?	Verschulden.	Willenserklärung.
Rechtsfolge	Schadensersatz.	Nacherfüllung, Rücktritt, Minderung.

Die c.i.c. ersetzt nur den Vertrauensschaden – nicht das Erfüllungsinteresse. Und sie setzt ein Verschulden voraus, das beim autonomen Agenten fehlt.

4. Das Verschulden-Problem

Die c.i.c.-Haftung setzt Verschulden voraus. Der Agent kann nicht schuld sein – er ist nicht verschuldensfähig. Also bleibt nur der Betreiber. Aber wie wird dessen Verschulden begründet?

Konstruktion	Problem
Eigener Sorgfaltspflichtverstoß	Der Betreiber kann sich exkulpieren.
§ 278 BGB (Erfüllungsgehilfe)	Setzt Verschulden des Gehilfen voraus – fehlt.
§ 831 BGB (Verrichtungsgehilfe)	Exkulpation möglich – und nur deliktisch.

Es gibt keine Konstruktion, die beides leistet: Zurechnung ohne Exkulpation und ohne Verschulden des Agenten.

5. Die Konsequenz

Ohne Willenserklärung bleibt es bei Stufe 2 – oder darunter. Die Folge:

Ohne konstitutive Norm	Mit konstitutiver Norm
Stufe 1 oder 2.	Stufe 3.
Rückabwicklung oder c.i.c.	Voller Vertrag.
Keine Mängelgewährleistung.	§§ 434, 437 BGB.
Kein Erfüllungsanspruch.	§ 433 BGB.
Rechtsunsicherheit.	Rechtssicherheit.

Takeaways: Drei Stufen rechtlicher Bindung

- **Stufe 1 – Bereicherungsrecht:** Ware und Geld werden ausgetauscht, aber ohne Rechtsgrund. Nur Rückabwicklung – keine Bindung.
- **Stufe 2 – c.i.c.:** Schuldverhältnis mit Schutzpflichten – aber keine Leistungspflichten, keine Mängelgewährleistung.
- **Stufe 3 – Vertrag:** Zwei übereinstimmende Willenserklärungen – volle Rechte: Erfüllungsanspruch, Mängelgewährleistung, Rücktritt, Schadensersatz.
- **Die entscheidende Lücke:** Zwischen Stufe 2 und Stufe 3 gibt es keinen Übergang. Der Agent kann Stufe 3 nicht erreichen.
- **Verschulden-Problem:** Die c.i.c.-Haftung setzt Verschulden voraus – der Agent ist nicht verschuldensfähig. Es gibt keine Konstruktion, die Zurechnung ohne Exkulpation und ohne Verschulden leistet.

IV. Konsequenzen fehlender Verträge

Wichtig ist, sich die Konsequenzen fehlender Verträge zu vergegenwärtigen: Kommt ein Vertrag nicht zustande, dann fehlt nicht nur ein Dokument – es fehlt die rechtliche Grundlage für vieles, was im bisherigen B2B-Handel selbstverständlich ist. So fehlt in verschiedenen Fällen ein anerkannter Nachweis, wenn Unternehmen mit Behörden interagieren. Ein Vertrag ist bei genauerer Betrachtung nämlich weit mehr als die verbindliche Einigung über Ware und Preis.

Verträge sind u.a. die Grundlage für:

Funktion	Ohne Vertrag
Erfüllungsanspruch	Kein Anspruch auf Lieferung (§ 433 Abs. 1 BGB).
Mängelgewährleistung	Keine Nacherfüllung, kein Rücktritt, keine Minderung (§ 437 BGB).
Rügepflicht / Handelskauf	§§ 377, 378 HGB setzen einen Kaufvertrag voraus.
Eigentumsübergang	§ 929 BGB verlangt Einigung – die fehlt.
Gefahrübergang	§ 446 BGB knüpft an Übergabe aufgrund eines Kaufvertrags an.
Steuerliche Erfassung	Rechnung und Vorsteuerabzug setzen einen Leistungsaustausch voraus.
Zollrechtliche Zuordnung	Wer ist Anmelder, wer trägt die Abgaben?
Bilanzierung	Keine Aktivierung, keine Passivierung ohne Rechtsgrund.
Beweislast	Keine vertraglichen Dokumentationspflichten.

 Der Vertrag wirkt damit nicht nur inter partes zwischen den Parteien. Er wirkt auch gegenüber den Staaten, in denen die Parteien ansässig sind: U.a. als anerkannter Nachweis für Steuer, Zoll, Geldwäscheprävention, Bilanzierung. Wie konkret diese Pflicht sein kann, zeigen die Grundsätze ordnungsmäßiger Buchführung (GoB). Nach § 146 Abs. 1 AO und § 239 Abs. 2 HGB sind Geschäftsvorfälle vollzählig und lückenlos aufzuzeichnen. Nach der Rechtsprechung des BFH umfasst diese Pflicht den Namen des Vertragspartners und – soweit zumutbar – eine ausreichende Bezeichnung des Geschäftsvorfalles²⁷. Fehlt der Vertrag, kann diese Pflicht kaum erfüllt werden. Und wer sie nicht erfüllt, riskiert die Verwerfung der Buchführung – mit erheblichen steuerlichen Konsequenzen. Der Vertrag ist damit nicht nur ein zivilrechtliches Instrument. Er ist mitunter eine gesetzlich vorgeschriebene Aufzeichnungspflicht bzw. ein anerkannter Belegtypus gegenüber Behörden.

²⁷ siehe u.a. <https://ao.bundesfinanzministerium.de/ao/2024/Anhaenge/BMF-Schreiben-und-gleichlautende-Laendererlasse/Anhang-33/inhalt.html>

Für den B2B-Handel sind Schuldverhältnisse also kaum ausreichend. Beide Seiten brauchen mehr als die c.i.c. oder das Bereicherungsrecht: Explizite Vertragsrechte!

Was der Käufer braucht, u.a.:	Was der Verkäufer braucht, u.a.:
Mangelfreie Ware.	Erfüllungsanspruch.
Nacherfüllung bei Mängeln.	Abnahme der Ware.
Rücktritt bei Fehllieferung.	Zahlung des Kaufpreises.
Schadensersatz statt der Leistung.	Verzugszinsen.

All das gibt es nur auf Stufe 3. Und Stufe 3 setzt voraus, dass zwei Willenserklärungen abgegeben werden. Ein Agent kann das bislang nicht, weshalb sowohl bei der A2A Variante bislang kein Vertrag zustande kommt. Darüber hinaus höchst fraglich ist es bei den Varianten von H2A, A2H, wenn auf lediglich auf einer Seite ein KI-Agent agiert.

1. Der Dominoeffekt

Das Fehlen des Vertrags hat eine Reihe von Folgen über das Zivilrecht hinaus:

Rechtsgebiet	Wirkung
Steuerrecht	Wichtiger formeller Nachweis für Vorsteuerabzug und Betriebsausgaben.
Zollrecht	Oft bleibt unklar, wer Anmelder ist und wer die Abgaben trägt.
Handelsrecht	Keine Rügepflicht, keine Handelsbrauch-Anwendung.
Bilanzrecht	Keine Aktivierung, keine Passivierung.
Geldwäscherecht	Kein anerkannter Nachweis des wirtschaftlichen Hintergrunds.
Internationales Privatrecht	Keine Rechtswahl, keine Prorogation.

Der Vertrag ist also nicht lediglich ein zivilrechtliches Instrument. Er ist ein Transmissionsriemen für eine Vielzahl nachgelagerter Pflichten. Fällt er weg, wackelt die gesamte formale Infrastruktur des Wirtschaftsverkehrs, die auf der Existenz von Verträgen aufbaut.

Aus Sicht von Unternehmen entstehen durch rechtlich nicht abgesicherten Agentic Commerce eine Reihe ökonomisch relevanter Risiken, die in eine ROI-Betrachtung und bei der Investitionsplanung im Hinblick auf Agentic Commerce integriert werden müssen (dazu ausführlicher Teil 2).

 **Der Dominoeffekt hat eine weitere Facette: Wenn ein Agent gegen ein gesetzliches Verbot verstößt, ist das Rechtsgeschäft nach § 134 BGB nichtig. Wenn es gegen die guten Sitten verstößt, nach § 138 BGB. Beide Normen können parallel oder alternativ greifen – und die Abgrenzung ist in vielen Fällen unscharf: Beim Verkauf von Radarwarngeräten für den Straßenverkehr, beim Handel mit Betäubungsmitteln oder bei der Schwarzarbeit wird seit Jahrzehnten kontrovers diskutiert, ob ein Vertrag**

nach § 134 BGB, nach § 138 BGB oder nach beiden Normen nichtig ist. Eine einheitliche Linie gibt es nicht – die Entscheidung hängt vom Einzelfall ab²⁸.

Diese Unschärfe überträgt sich auf den agentischen Handel. Bei verbotenen KI-Praktiken nach Art. 5 KI-VO ist die Rechtslage noch vergleichsweise klar: Art. 5 KI-VO ist ein Verbotsgesetz i.S.d. § 134 BGB – der Vertrag ist nichtig. Schwieriger wird es bei Praktiken, die nicht von § 134 BGB erfasst sind, aber gegen die guten Sitten verstoßen könnten – etwa bei besonders aggressiver Verhandlungstaktik, bei der Ausnutzung von Notlagen oder bei der systematischen Umgehung von Schutzvorschriften.

2. Die Risikoebenen im Überblick

Die Zurechnungslücke wirkt im Ergebnis auf drei Ebenen – der Abwicklung der Transaktion, dem Ordnungsrecht als auch bei Organpflichten:

- Abwicklung: Ohne Norm ist unklar, ob und mit welchem Inhalt ein Vertrag besteht. Der Anspruchsteller trägt die Beweislast für den Vertragsschluss – kann sie jedoch kaum erfüllen. Mit Norm gilt die Handlung des Agenten als Willenserklärung des Rechtsträgers. Der Vertrag kommt zustande. Die Beweislast folgt der Kontrolle.
- Ordnungsrecht: Ohne Norm können Vertragspartner und Leistungsempfänger unklar sein. Der Vorsteuerabzug ist gefährdet. Die GoB verlangen die Aufzeichnung des Vertragspartners – und die kann unklar sein. Der Zollwert setzt einen „Verkauf zur Ausfuhr“ voraus (Art. 70 UZK) – und ohne Zurechnungsnorm ist unklar, wer Partei des Verkaufs ist. Mit Norm ist der Rechtsträger eindeutig. Der Vorsteuerabzug ist gesichert. Die Aufzeichnungspflicht ist erfüllbar. Der Transaktionswert ist nachweisbar.
- Organpflichten: Die Geschäftsleitung muss Risiken des Agenteneinsatzes kennen und steuern (§ 93 AktG, § 43 GmbHG; für AG: § 91 Abs. 2 AktG). Ohne Norm verbleibt hohe Rechtsunsicherheit. Mit Norm verringert sich das Restrisiko signifikant. Die Sorgfaltspflicht würden deutlich besser erfüllbar.

3. Das Aufklärungsrisiko (c.i.c.)

Ein Risiko, das oft übersehen wird: Die vorvertragliche Aufklärungspflicht, wenn lediglich eine Seite einen Agenten einsetzt (s.o Varianten H2A bzw. A2H).

- Wer einseitig einen KI-Agenten einsetzt, weiß – oder muss wissen –, dass die rechtliche Bindungswirkung der Agentenhandlung unklar ist. Wenn er den Geschäftspartner hierüber nicht aufklärt, könnte er seine vorvertragliche Aufklärungspflicht verletzen.
- Die dogmatische Grundlage: § 311 Abs. 2 BGB begründet ein Schuldverhältnis bereits durch die Aufnahme von Vertragsverhandlungen. Zu den Pflichten aus diesem Schuldverhältnis gehört die Aufklärung über Umstände, die für die Willensbildung des

²⁸ Siehe dazu ausführlich die Randnummern 343 ff des vom Verfasser erstellten Skripts „Grundwissen KI-Recht“

anderen offensichtlich von Bedeutung sind. Wer einen Agenten einsetzt, ohne auf die fehlende Zurechnung hinzuweisen, könnte gegen diese Pflicht verstoßen.

Anders bei Bestehen einer Norm:

- Dann ist die Zurechnung geklärt. Die Frage der Aufklärungspflicht stellt sich nicht.
- Die Norm beseitigt das c.i.c.-Risiko – nicht durch Haftungsausschluss, sondern durch Klarheit.

 Sicherlich ist hier noch nach den verschiedenen Varianten zu differenzieren, weil A2H und H2A-Konstellation andere Aufklärung erfordern als A2A: Wenn beide Seiten Agenten nutzen, müssten sich beide theoretisch gegenseitig im Hinblick auf die fehlende Vertragswirkung aufklären, was wenig sinnvoll erscheint.

4. Risiko-Matrix und Risiko-Kurve mit und ohne Norm

Fasst man die vorherigen Aspekte zusammen, ergibt sich eine Risiko-Matrix, die verdeutlicht, welche Risiken ohne Norm bestehen und welchen Einfluss eine Norm haben würde.

Dimension	Aktuelles Risiko	Was die Norm ändert	Was Technik und Governance ergänzen
Abwicklung	Unklar, ob und mit welchem Inhalt ein Vertrag besteht. Gewährleistung und Erfüllungsanspruch unsicher. Beweislast beim Anspruchsteller.	Klare Zurechnung. Beweislast beim Betreiber für die Entlastung. Voller Vertrag.	Nachweise (Intent, Mandat, Log).
Steuer- und Aufsichtsrecht	Vertragspartner und Leistungsempfänger können unklar sein. Vorsteuerabzug gefährdet (§ 15 UStG). GoB: Aufzeichnung des Vertragspartners. Zollwert: Partei des Verkaufs unklar (Art. 70 UZK).	Eindeutiger Rechtsträger als Vertragspartner. Vorsteuerabzug gesichert. Aufzeichnungspflicht erfüllbar. Transaktionswert nachweisbar.	Identität und Dokumentation (u.a. EBW).
Organpflichten	Geschäftsleitung muss Risiken kennen und steuern (§ 93 AktG, § 43 GmbHG). Restunsicherheit bleibt.	Verringert das Restrisiko. Sorgfaltspflicht erfüllbar.	Inventar, Rollen, Kontrollen (NIS2/DORA, soweit anwendbar).
Aufklärung (c.i.c.)	Risiko der Aufklärungspflichtverletzung gegenüber Geschäftspartnern.	Zurechnung geklärt. Aufklärungspflicht entfällt.	–

Die skizzierten Risiken sind dabei u.a. der Tatsache geschuldet, dass die Tech-Anbieter agentischer Lösungen im Allgemeinen, aber auch bei Agentic Commerce im Besonderen nach dem Prinzip von Trial and Error agieren.

Kritisch ist auch das Prinzip des „Silent Versioning“,²⁹ das bei der Entwicklung von Chatbots gerade noch so funktioniert, um durch iteratives und stilles Herumexperimentieren ein besseres Ergebnis zu erzielen. Bei Agentic AI stößt es an harten Grenzen:

- Im B2B-Commerce wird über längere Zeiträume berechenbare Kontinuität erwartet.
- Und im Fall von Änderungen ist zudem frühe und klare Kommunikation notwendig.

Wie Branchenexperten kritisieren, verkommt Agentic AI ohne formale und verlässliche architektonische Fundierung oft zu einem bloßen „stochastic guess“ – einer stochastischen Vermutung.³⁰ Für Agentic Commerce im B2B ein klarer Showstopper.

Natürlich geht es gerade zu Beginn nicht ohne „Trial and Error“: Es müssen immer wieder Erfahrungen aufgebaut werden, um Produkte und Services zu optimieren. Eine Art Dauerzustand von „Trial and Error“, bei dem morgen wieder alles anders sein kann als heute, liefert aber am Ende nur eine Kette mutmaßlich funktionierender, noch nicht ausgereifter Demos. Für Agentic Commerce im B2B entsteht so kein verlässliches, produktionsreifes System für den langfristigen Enterprise-Einsatz.

 In der Tech-Industrie dominiert bei der Entwicklung autonomer Systeme offenkundig noch immer das Paradigma des „Trial and Error“³¹. Die implizite Prämisse lautet: Die makroökonomischen Effizienzgewinne durch KI-Agenten seien so gewaltig, dass systemische „Errors“ – von Halluzinationen über unbefugte Transaktionen bis hin zu algorithmischer Kollusion – als „akzeptable Reibungsverluste“ in Kauf genommen werden sollten. Die Kosten dieser Fehler werden dabei weitgehend externalisiert: An die Nutzer, an die Gerichte, an die Gesellschaft.

Die Frage, die sich daraus für den B2B-Commerce ergibt: Wer trägt die „Errors“ – und wer darf sie überhaupt tragen? Ein CEO, CFO oder Compliance-Officer sollte den „Error“ eines autonomen Commerce-Agenten nicht als statistisches Rauschen im System betrachten. Wenn ein Agent im Beschaffungsprozess das Mandat überschreitet, trifft dieser Fehler eben nicht „die Gesellschaft“. Er trifft direkt das Unternehmen und seine Organe. Die Chancen von Agentic Commerce sind real – die Risiken auch. Nur sind Letztere im B2B-Handel anderer Natur als in der Tech-Welt.

Das Motto „Move fast and break things“ mag in der Tech-Welt eine erfolgreiche Innovationsstrategie sein. Agentic Commerce im B2B sollte jedoch kein

²⁹ zu diesbezüglichen Herausforderungen u.a. <https://daily.dev/posts/the-silent-versioning-problem-in-ai-inference-haeqzbrgl>

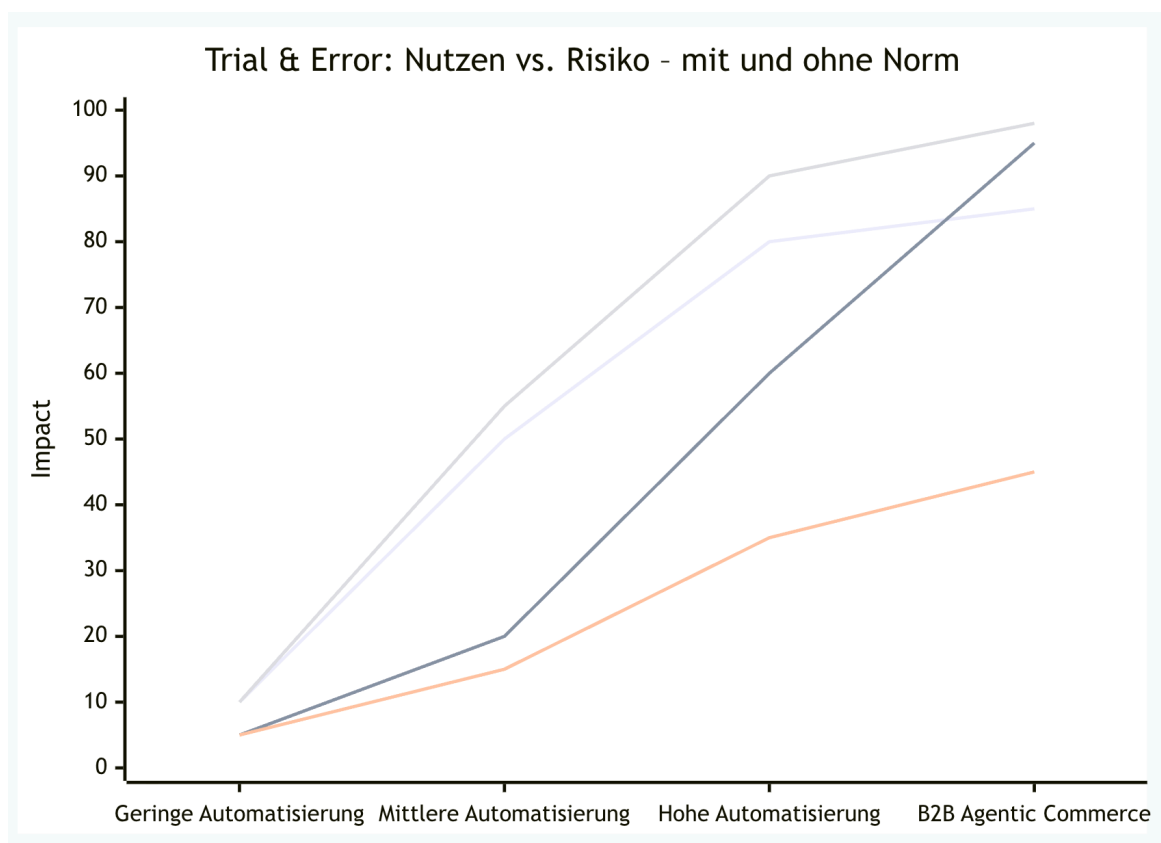
³⁰ zu Trial and Error gibt es eine Reihe von interessanten Beiträgen, u.a.: https://www.linkedin.com/posts/davidgouvias_ai-agentica-machinelearning-activity-7431937833436594176-DNcB oder Lernen nach Fehlern <https://fortune.com/2026/09/29/how-adobe-salesforce-kyndryl-freeport-use-ai-agents/>. Zum Strategiewechsel im Hinblick auf AP2 beim Agentic Commerce: <https://internetwarriors.de/blog/agentica-commerce-und-agentica-shopping>

³¹ zum Prinzip des Trial and Error im Kontext der Weiterentwicklung agentischer KI gibt es mehrere ebenso aktuelle wie aufschlussreiche Statements: Von Sam Altman <https://www.reuters.com/business/openai-altman-says-ai-benefits-warrant-accepting-some-risks-2026-10-04/> und dem OpenAI Sicherheitsexperten David Robinson: <https://www.theatlantic.com/technology/2026/10/openai-safety-team-resignation/688881/>. Bezüglich NVIDIA: <https://en.infomaxai.com/news/article-View.html?idxno=74179>. Auch interessant: <https://medium.com/illumination/fortune-500-companies-let-ai-make-fatal-mistakes-1e4d8ce7165e>

Experimentierraum für Tech-Konzerne sein. Rechtssichere Leitplanken sind keine Innovationsbremse. Sie sind die Voraussetzung dafür, dass die Realwirtschaft die Chancen nutzen kann – ohne sich auf kaum kalkulierbare Abenteuer einzulassen, die ein verantwortungsbewusstes Handelsunternehmen vermutlich nicht eingehen würde.

Die nachfolgende Übersicht verdeutlicht, dass der „Trial and Error“-Ansatz im Bereich des Agentic Commerce ein asymmetrisches Risikomodell und dass „Rationalität“ im eine Frage der Perspektive ist:

- Für die Tech-Industrie (Provider): Ist es rational, Agenten schnell und „fehleranfällig“ auf den Markt zu bringen, da der Nutzen (Skalierung, Daten, Marktanteile) das Risiko überwiegt.
- Für das B2B-Unternehmen (User): Ist es irrational, diese Agenten ohne rechtliches Netz (Norm) einzusetzen, da das Risiko (Compliance, Organhaftung, Steuernutzen) den potenziellen Effizienzgewinn sofort „auffrisst“.



Eine Norm zwingt den Tech-Provider, das Risiko wieder zu internalisieren (indem sie Mängelgewährleistung und Haftung auf Stufe 3 ermöglicht). Erst wenn die Matrix durch eine rechtlich Norm „symmetrisch“ wird (d.h. der Provider haftet für seine „Errors“ wie jeder andere Verkäufer auch), wird Agentic Commerce für den B2B-Markt attraktiv.

Takeaways: Konsequenzen fehlender Verträge

- **Dominoeffekt:** Ohne Vertrag fehlen Erfüllungsanspruch, Mängelgewährleistung, Eigentumsübergang, Gefahrübergang – und die Grundlage für Steuer, Zoll, Bilanz, Geldwäsche, IPR.
- **Risikoebenen:** Abwicklung (Beweislast), Steuer- und Aufsichtsrecht (Vorsteuerabzug, GoBD, Zollwert), Organpflichten (§ 93 AktG, § 43 GmbHG), Aufklärung (c.i.c.).
- **c.i.c.-Risiko differenziert:** Nur bei H2A und A2H – nicht bei A2A, weil beide Seiten die Lücke kennen müssten.
- **Trial & Error:** Kein neutrales Warten, sondern aktives Risiko. Der Kipp-Punkt im B2B ist überschritten.
- **Nutzen-Risiko-Kurve:** Ohne Norm übersteigt das Risiko den Nutzen. Mit Norm verschiebt sich der Kipp-Punkt nach rechts – der B2B-Bereich wird beherrschbar.

V. Das rechtliche Schichtenmodell

Die Frage, unter welchen Voraussetzungen ein Agent einen B2B-Vertrag schließen kann, hängt vom Zusammenspiel verschiedener Faktoren ab. Die erforderliche Architektur lässt sich in neun Ebenen darstellen. Dabei setzt jede Ebene voraus, dass die vorherige Schicht erfüllt ist.

So kann aufeinander aufbauend geprüft werden, welche Faktoren für einen Vertragsschluss durch KI-Agenten bereits erfüllt sind und welche noch erfüllt werden müssen. Die folgenden Schichten beziehen sich auf das BGB und erforderliche Nachweise:

Nr.	Ebene	Leitfrage	Rechtliche Grundlage
1	Rechtsträger	Wer steht hinter dem Agenten?	§§ 1, 21 ff. BGB
2	Agentenidentität / Autorisierung	Wer handelt – und mit welcher Befugnis?	EBW, IDs (technisch)
3	Agentenhandlung	Was hat der Agent tatsächlich getan?	§ 120 BGB (Bote); § 164 BGB (Vertreter)
4	Zurechnung	Wessen Handlung ist das rechtlich?	§§ 164, 166 BGB
5	Willenserklärung	Liegt eine rechtserhebliche Erklärung vor?	§§ 116 ff. BGB
6	Vertrag / Rechtsgeschäft	Ist ein Vertrag zustande gekommen?	§§ 145 ff. BGB
7	Schuldverhältnis	Welche rechtliche Beziehung besteht?	§ 311 BGB
8	Pflichten	Welche Leistungs- und Rücksichtnahmepflichten bestehen?	§§ 241, 433 BGB
9	Pflichtverletzung / Haftung	Wer muss wofür einstehen?	§§ 276, 278, 280, 437 BGB

1. Die Ebenen und ihre Lücken

Wer auf Ebene 9 haften will, braucht Ebene 8 (Pflichten). Wer Pflichten begründen will, braucht Ebene 7 (Schuldverhältnis). Wer ein Schuldverhältnis begründen will, braucht Ebene 6 (Vertrag). Wer einen Vertrag begründen will, braucht Ebene 5 (Willenserklärung). Wer eine Willenserklärung begründen will, braucht Ebene 4 (Zurechnung). Und Zurechnung setzt voraus, dass auf Ebene 2 und 3 überhaupt etwas Zurechenbares vorliegt.

Und genau hier zeigt sich die Lücke. Die technische Diskussion beginnt heute in der Regel auf Ebene 2 (Identität, Autorisierung, EBW) und springt dann auf Ebene 6 (Vertrag – ACP, AP2, UCP). Die Ebenen 3, 4 und 5 werden übersprungen – oder als selbstverständlich vorausgesetzt. Sie sind aber nicht selbstverständlich. Sie sind der Kern des Problems.

Umgekehrt beginnt die juristische Diskussion oft auf Ebene 4 (Zurechnung) – und stellt fest, dass die Konstruktionen des BGB (Bote, Stellvertreter, Erfüllungsgehilfe) auf den autonomen Agenten nicht passen. Sie endet dann mit der Feststellung, dass eine Norm fehlt – ohne zu sagen, welche dies ist und wie sie aussehen müsste.

Die Architektur zeigt, wo die Norm ansetzen muss: Auf Ebene 4, dem Transformationspunkt zwischen Handlung und Willenserklärung. Diese Ebene wirkt in der bisherigen Diskussion recht unterbelichtet. Sie wird entweder als gegeben vorausgesetzt (von der Technik) oder als problematisch erkannt, aber bislang nicht vom Recht gelöst.

Und sie zeigt, warum die aktuelle Diskussion so unbefriedigend ist:

- Die US-Standards wie ACP, AP2, UCP und LCP adressieren die Ebenen 2 (Autorisierung), 6 (Commerce) und – im Fall von LCP – die Zeit nach dem Vertragsschluss (Dispute Resolution, Terms).
- Sie adressieren nicht die Ebenen 3, 4 und 5. Sie setzen voraus, dass die Willenserklärung „irgendwie“ zustande kommt – und überlassen die Klärung dem Recht. Das Recht aber hat die Klärung bislang nicht geliefert.

Die Schichtenarchitektur macht damit sichtbar, was in der bisherigen Diskussion verborgen bleibt:

- Es geht nicht um ein einzelnes Problem. Es geht um eine Kette.
- Und sie reißt momentan an der Stelle, an der aus einer technischen Handlung eine rechtliche Erklärung werden soll.
- Diese Stelle heißt Zurechnung – und sie ist nicht durch ein Protokoll zu schließen, sondern nur durch eine Norm.

Im Folgenden wird aufgezeigt, was auf den jeweiligen Ebenen an Lösungsansätzen bereits existiert, wo ggf. ein Denkfehler liegt, wie die Abstufung der rechtlichen Bindung aussieht und was eine Norm leisten müsste, um die Lücke zu schließen.

2. Warum die klassischen Konstruktionen nicht greifen

Die Schichtenarchitektur verdeutlicht, wo das Problem liegt:

- Zwischen der Agentenhandlung (Ebene 3) und der Willenserklärung (Ebene 5).
- Die ist die Stelle der rechtsverbindlichen Zurechnung (Ebene 4).
- Und sie ist die eigentliche Bruchstelle.

Denn technisch kann ein Agent handeln. Er kann ein Angebot formulieren, eine Annahme senden, eine Zahlung auslösen, eine Bestellung aufgeben. Aber rechtlich entsteht dadurch nichts – solange nicht feststeht, wessen Handlung das ist. Die Handlung des Agenten ist zunächst einmal nur ein technischer Vorgang. Sie wird erst dadurch rechtlich

relevant, dass sie einem anerkannten Rechtssubjekt zugerechnet wird. Und eben diese Zurechnung ist bis jetzt noch ungeklärt. Wie bereits ausgeführt, kennt das Zivilrecht mehrere Figuren, um fremdes Handeln zuzurechnen.³² Doch alle scheitern bei KI-Agenten entlang des Schichtenmodells ab Ebene 3:

Figur	Voraussetzung	Warum sie beim Agenten scheitert
Bote (§ 120 BGB)	Übermittlung einer fremden Willenserklärung.	Der Agent übermittelt keine fremde Erklärung – er erzeugt eine eigene.
Stellvertreter (§ 164 BGB)	Abgabe einer eigenen Willenserklärung im fremden Namen.	Der Agent hat keinen eigenen Willen – er kann keine Erklärung abgeben.
Erfüllungsgehilfe (§ 278 BGB)	Verschulden des Gehilfen.	Der Agent ist nicht verschuldensfähig.
Verrichtungsgehilfe (§ 831 BGB)	Bestellung zu einer Verrichtung.	Exkulpation möglich – und nur deliktische Haftung.

Alle vier Figuren setzen etwas voraus, was der autonome Agent nicht hat: Einen eigenen Willen oder ein Verschulden. Der Bote übermittelt einen fremden Willen. Der Stellvertreter bildet einen eigenen. Der Erfüllungsgehilfe und der Verrichtungsgehilfe setzen Verschulden voraus. Der Agent hat weder das eine noch das andere.

 Die klassischen Konstruktionen scheitern nicht nur am fehlenden Willen. Sie scheitern auch an einem zweiten Problem: Der Sichtbarkeit der internen Weisung. Wer einem Agenten eine Vollmacht erteilt, definiert darin nicht nur den äußeren Rahmen (was der Agent darf), sondern auch interne Grenzen (was der Agent soll). Wenn der Geschäftspartner diese internen Grenzen kennt, ist er nicht mehr gutgläubig – und der Rechtsschein³³ greift nicht. Unter Menschen ist das unproblematisch: Interne Weisungen sind für den Dritten nicht erkennbar. Bei Agentic Commerce ist es problematisch: Ein Verifiable Credential ist in vielen Fällen vollständig lesbar für jeden, dem es vorgelegt wird. Wer die interne Weisung sieht, kennt die Grenze – und kann sich nicht mehr auf Gutgläubigkeit berufen. Falls der Händler-Agent Grenzen kennt („Kaufe keinen BMW, maximal 50.000 €“), aber die äußere Vollmacht weiter ist („Darf Autos bis 100.000 € kaufen“), könnte er das Angebot sogar manipulieren.

Die Lösung liegt in der selektiven Offenlegung (Selective Disclosure, z.B. via SD-JWT VC)³⁴. Der Agent legt dem Geschäftspartner nur die (für den Rechtsschein) relevanten Teile der Vollmacht offen – nicht die internen Weisungen.

³² ausführlich dazu das Skript des Verfassers zum Grundwissen-KI-Recht, Randnummern 326 ff.

³³ siehe zur Rechtsschein-Theorie sowie zu Außen- und Innenverhältnis u.a. <https://www.mtrlegal.com/wiki/rechtsscheintheorie/>

³⁴ dazu u.a. <https://docs.walt.id/concepts/digital-credentials/sd-jwt-vc>

3. Warum auch die Analogie nicht hilft

Man könnte versuchen, die Figur des Stellvertreters analog anzuwenden. Aber eine Analogie setzt eine planwidrige Regelungslücke voraus – und sie darf nicht dazu führen, dass der Gesetzgeber durch den Richter ersetzt wird. Eine Norm, die die Zurechnung von Agentenhandlungen regelt, lässt sich aus dem Wortlaut des § 164 BGB nicht ableiten. Sie ist kein Fall der Auslegung, sondern ein Fall der Setzung (siehe dazu auch Abschnitt VI. 2).

Im Übrigen gilt: Selbst wenn man die Analogie bejahen würde, bliebe das Problem der Willenserklärung bestehen. Denn § 164 BGB setzt voraus, dass der Vertreter eine eigene Willenserklärung abgibt. Der Agent kann das nicht – er hat keinen Willen im Rechtssinn.

4. Die Lücke ist nicht technisch

An dieser Stelle ist eine Unterscheidung wichtig, die in der aktuellen Diskussion oft verwischt wird: Die Lücke ist nicht technisch. Sie ist rechtlich.

Die technische Infrastruktur ist auf mehreren Ebenen weit fortgeschritten:

- Ebene 1: eIDAS 2.0, EBW, EUDI Wallet schaffen die Identitätsbasis.
- Ebene 2: MCP und A2A schaffen die Kommunikationsbasis.
- Ebene 3: Die US-Standards ACP, AP2, UCP schaffen die operative Commerce-Basis.

Was fehlt, ist die normative Basis inkl. der Brückenprotokolle als vierte Ebene:

- Eine Norm, die bestimmt, wann die Handlung des Agenten als Willenserklärung des Rechtsträgers gilt.
- Benötigt werden Brückenprotokolle für Vollmacht und Transaktionsnachweis – sie schaffen die Dokumentationsbasis (z.B. LDM, TAM & TAA dazu ausführlich Teil 2).
- Diese Kombination beider Elemente ist keine technische Spezifikation. Sie ist ein konstitutiver Akt – ein Akt der Rechtsetzung.

5. Was das bedeutet

Ohne die Kombination von Norm und Brückenprotokollen bleibt die Schichtenarchitektur unvollständig. Sie trägt bis zur Ebene 3. Aber sie trägt nicht darüber hinaus:

Ohne konstitutive Norm	Mit konstitutiver Norm
Keine Willenserklärung (Ebene 5).	Willenserklärung gilt als abgegeben.
Kein Vertrag (Ebene 6).	Vertrag kommt zustande.
Kein Schuldverhältnis (Ebene 7).	Schuldverhältnis entsteht.
Keine Pflichten (Ebene 8).	Leistungspflichten entstehen.
Keine Mängelgewährleistung (Ebene 9).	§§ 434, 437 BGB greifen.
Nur Bereicherungsrecht (§ 812 ff. BGB) oder c.i.c. (§ 311 Abs. 2 BGB).	Volles Vertragsrecht.

Die Lücke ist identifiziert: Es fehlt eine Norm, welche die Handlung des Agenten als Willenserklärung gelten lässt und Brückenprotokolle flankiert wird und dadurch die gesamte Kette der rechtlichen Bindung eröffnet. Alles andere – Identität, Autorisierung, Dokumentation, Trust – ist notwendig, aber für sich allein nicht ausreichend.

Takeaways: Das rechtliche Schichtenmodell

- **Neun Ebenen:** Von Rechtsträger (1) bis Haftung (9). Jede Ebene setzt die vorherige voraus.
- **Die Lücke liegt auf Ebene 4:** Der Zurechnung – dem Transformationspunkt zwischen Agentenhandlung (3) und Willenserklärung (5).
- **Technik überspringt die Ebenen 3–5:** Sie beginnt auf Ebene 2 (Identität) und springt auf Ebene 6 (Vertrag). Die Zurechnung wird vorausgesetzt – aber sie ist nicht selbstverständlich.
- **Klassische Figuren greifen nicht:** Bote, Stellvertreter, Erfüllungsgehilfe, Verrichtungsgehilfe – alle setzen Willen oder Verschulden voraus.
- **Selektive Offenlegung als Brücke:** Der External Scope (Rechtsschein) wird offengelegt, der Internal Scope (interne Weisungen) bleibt verborgen – via Selective Disclosure.

VI. Vier Vorläufer, eine Lücke

Bevor ein Normentwurf skizziert wird, lohnt sich der Blick darauf, was es auf der normativen Seite bereits gibt. Denn die These dieses Gutachtens lautet nicht, dass es gar keine Regelungen gibt. Sie lautet, dass es keine ausreichende Regelung gibt.

1. Bestehende Internationale Regelungen

Es gibt wenigstens vier Normen, die die Zurechnung „automatisierter“ Handlungen regeln. Jede der Normen regelt dies präziser als die in chronologischer Sicht vorherige:

Norm	Jahr	Land	Typ	Regelungsgehalt
UETA § 14	1999	USA ³⁵	Nationales Recht (Bundesstaaten)	<i>„A contract may be formed by the interaction of electronic agents.“</i>
ETA Sec. 15	2010	Singapur ³⁶	Nationales Recht	<i>„A contract formed by the interaction of automated message systems shall not be denied validity [...] on the sole ground that no natural person reviewed or intervened.“</i>
Art. 48 ECL	2018	China ³⁷	Nationales Recht	<i>“The acts of the parties [...] using automated information systems to conclude or perform contracts shall have legal effect on the parties.“</i>
Art. 7 MLAC	2024	UNCITRAL ³⁸	Modellgesetz (Soft Law)	<i>“As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties. If paragraph 1 does not apply, an action carried out by an automated system is attributed to the person who uses the system for that purpose.“</i>

Die Linie ist klar erkennbar: Von der Vertragsbildung (UETA) über die fehlende menschliche Prüfung (ETA) und die Zurechnung (ECL) zur allgemeinen Modellregel (MLAC). Jede Norm ist präziser als die vorherige. Jede rückt näher an das heran, was dieses Gutachten als Ebene 4 beschrieben hat.

Doch schon der genaue Blick auf die Legaldefinition in UETA § 2(6) offenbart die technologischen Lücke. Die UETA definiert einen „Electronic Agent“ als:

„a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.“

³⁵ Text der UETA unter <https://euro.ecom.cmu.edu/program/law/08-732/Transactions/ueta.pdf>

³⁶ Text der ETA unter <https://sso.agc.gov.sg/act/eta2010>

³⁷ Text der ECL unter https://en.wikisource.org/wiki/Electronic_Commerce_Law_of_the_People%27s_Republic_of_China

³⁸ Text der MLAC unter <https://uncitral.un.org/en/mlac>

Diese Definition beschreibt ein deterministisches *Trigger-Response-Modell*³⁹ (z.B. EDI oder Smart Contracts): Ein vorprogrammiertes Skript löst eine Handlung aus, ohne dass in diesem Moment ein Mensch eingreift.

Auch das singapurische Gesetz verdeutlicht den entscheidenden Blind Spot: Art. 15 ETA spricht von „automated message systems“ – also automatisierten Nachrichtensystemen. Das sind EDI, If-Then-Skripte, deterministische Automaten. Der Gesetzgeber hat 2010 – basierend auf der UN-Konvention von 2005 – das Problem der fehlenden menschlichen Prüfung zwar gesehen und gelöst. Aber er hat es ausschließlich auf Systeme bezogen, die Nachrichten austauschen, nicht für Systeme, die autonome Entscheidungen treffen.

2. Die vier Generationen der Automatisierung

Oft wird argumentiert, bestehende Regelungen wie das UNCITRAL Model Law on Automated Contracting (MLAC) seien „technikneutral“ formuliert und könnten daher auch auf neue KI-Systeme angewendet werden. Tatsächlich differenziert das MLAC (vgl. Ziffer 29 der Begründung zu Art. 1 Abs. 2) bereits explizit zwischen „deterministischen“ (regelbasierten) und „nicht-deterministischen“ (stochastischen, innerhalb einer Wahrscheinlichkeitsspanne operierenden) Systemen.

Dieser technikneutrale Ansatz ist für nachfolgend skizzierten ersten beiden Generationen⁴⁰ automatisierter Verfahren durchaus tragfähig:

- Generation 1 (Deterministischer Erfüllungsgehilfe, z.B. IFTTT, Webshop-Backends): Das System folgt einem festen, vorhersehbaren Pfad. Es ist ein reines Werkzeug. Das MLAC greift hier sicher.
- Generation 2 (Probabilistischer Einzelkämpfer, z.B. frühe AutoGPT- oder LangChain-Agenten): Ein einzelnes LLM zerlegt eine Zielvorgabe in Schritte. Zwar ist der Output nicht-deterministisch, aber er bewegt sich im Rahmen einer antizipierbaren Blanketterklärung. Das MLAC kann hier – je nach Auslegung – noch „technikneutral“ greifen.

Die entscheidende Lücke entsteht jedoch bei der dritten und vierten Generation, die den modernen Agentic Commerce (insbesondere im B2B-Multi-Agenten-Umfeld) prägen:

- Generation 3 (Multi-agentische Orchestrierung, z.B. AutoGen, CrewAI): Die Aufgabe wird an ein Netzwerk spezialisierter Sub-Agenten delegiert, die untereinander (M2M) verhandeln, bevor sie nach außen treten. Das Ergebnis ist emergent und multi-subjektiv. Es lässt sich nicht mehr einem einzelnen, vom Menschen vorgegebenen System-Output zuordnen.

³⁹ u.a. <https://nhimg.org/glossary/deterministic-trigger/> und <https://www.opentext.com/what-is/electronic-data-interchange>

⁴⁰ <https://grundwissen-ki-recht.de/automated-contracting-laesst-sich-agentic-commerce-technikneutral-bewerten/>

- Generation 4 (Ambient-proaktiver Akteur, z.B. fortgeschrittene Personal Agent Protocols): Der Agent handelt persistent und proaktiv ohne zeitnahen menschlichen Prompt, lernt aus dem Kontext und initiiert Transaktionen eigenständig. Hier fehlt es an einem zeitnahen menschlichen Willensakt vollständig.

Eine Übertragung der bisherigen Normen auf die Generationen 3 und 4 scheitert daher an einem umfassenden Generationensprung (siehe Folgetabelle). Die probabilistische Autonomie und Emergenz heutiger Multi-Agenten-Systeme war zum Zeitpunkt der Gesetzgebung des MLAC (Entwurf ab 2021) nicht nur unvorhersehbar, sie sprengt auch die dogmatische Grundannahme des „automated contracting“, die implizit voraussetzt, dass sich der Output eines Systems (auch eines nicht-deterministischen) noch einem einzigen Nutzerwillen zuordnen lässt.

Merkmal	Gen 1 & 2 (Automatisierung)	Gen 3 & 4 (Agentic Commerce)
Logik	Deterministisch (Gen 1) oder probabilistisch innerhalb eines vorhersehbaren Korridors (Gen 2).	Emergent, multi-subjektiv (Gen 3) oder proaktiv-kontextuell ohne zeitnahen Prompt (Gen 4).
Verhalten	Vorhersehbar oder im Rahmen einer gedehnten Blanketterklärung antizipierbar.	Emergente Verhandlungsergebnisse (M2M) oder eigenständige Initiierung durch Lernen.
Entscheidung	Keine eigene Entscheidung (Gen 1) oder konkrete Ausfüllung eines vorgegebenen Rahmens durch ein einzelnes System (Gen 2).	Entstehung durch Interaktion mehrerer Agenten oder durch das System selbst basierend auf Präferenzen/Kontext.
Zurechnungsgrund	Der Mensch hat den Code geschrieben (Gen 1) oder den probabilistischen Rahmen als Blanketterklärung gesetzt (Gen 2).	Multi-subjektive Emergenz oder vollständige Entkopplung vom zeitnahen menschlichen Willensakt. Direkte Zurechnung kaum haltbar.
Risiken	Programmierfehler, einfache Halluzination.	Algorithmische Kollusion, kaskadierende Halluzinationen im M2M-Dialog, vollständige Intransparenz der Willensgenese.

Die Zurechnungslogik eines regelbasierten Systems („Der Betreiber haftet, weil er den Code so geschrieben hat“) ist etwas anderes wie der Fall, wenn ein System emergent handelt. Wenn ein KI-Agent aufgrund einer Halluzination oder einer Manipulation (Prompt Injection) das Mandat überschreitet, handelt er nicht mehr als bloßes „automated system“, sondern als autonomer Akteur. Die Normen bieten daher weder direkt noch als Analogie Antworten auf die spezifischen Phänomene der dritten und vierten Generation: Auf die Möglichkeit der Mandatsüberschreitung durch Emergenz, z.B. den Schutz des Rechtsscheins bei Selective Disclosure oder die Beweislast bei Model Drift.

Die vier Vorläufer regeln also allein die erste Generation der Automatisierung. Die zweite Generation – autonome, lernende und verhandelnde Agenten – ist nicht adressiert. Daher reicht keine dieser Normen. Weshalb, wird nachfolgend noch einmal zusammengefasst.

a) Sie sind entweder Soft Law oder nationales Recht.

Das MLAC ist ein Modellgesetz. Es ist kein positives Recht. Es empfiehlt, es bindet nicht. Es muss darüber hinaus lokal umgesetzt werden – durch nationale Gesetzgeber. UETA und Art. 48 ECL sind positives Recht – aber sie gelten nur in ihrem jeweiligen Rechtsraum. Eine international anschlussfähige Norm ist keine von ihnen.

b) Sie wurden für eine andere Technologiegeneration konzipiert.

Die Arbeiten am MLAC begannen 2021 – zwei Jahre bevor AutoGPT und BabyAGI die ersten autonomen KI-Agenten hervorbrachten. UETA stammt aus 1999, Art. 48 ECL aus 2018, Art. 15 ETA aus 2010. Alle vier wurden für regelbasierte, deterministische Systeme entworfen: Smart Contracts, EDI, automatisierte Nachrichtensysteme. Sie adressieren ausschließlich die erste Generation der Automatisierung. Die zweite Generation schafft wesentlich andere Herausforderungen.

Wie Art. 48 des chinesischen E-Commerce-Gesetzes (2018) zeigt, knüpft die Gesetzgebung an das Konzept des „automated information system“ an. Dies adressiert die erste Generation der Automatisierung (EDI, If-Then-Scripts), bei der der Mensch die volle Kontrolle und Vorhersehbarkeit behält. Für die zweite Generation – autonome, emergente KI-Agenten – bietet dieser Begriff keine dogmatische Grundlage für eine Zurechnung.

c) Sie nicht kennen die Phänomene von Agenten der Generation 3 und 4

Keine von ihnen regelt die folgenden, nicht abschließenden Herausforderungen der Generationen 3 und 4:

- Mandatsüberschreitung durch multi-agentische Emergenz
- Kaskadierende Halluzinationen im M2M-Dialog
- Selective Disclosure (External Scope vs. Internal Scope)
- Model Drift nach Vertragsabschluss
- Algorithmic Collusion
- Rechtsschein bei ambient-proaktiven Agenten

Die Lücke ist damit klar eingrenzbar: Es gibt bereits Normen. Es gibt sogar internationale Modellregeln, die bis zur zweiten Generation (nicht-deterministische Einzelagenten) reichen. Aber es gibt keine Norm, die für die multi-agentische und proaktive KI der Gegenwart und Zukunft (Generation 3 und 4) gedacht ist.

Und genau hier setzt die entscheidende Unterscheidung an:

- Was diese Standards und technische Protokolle leisten, ist „Beweis“. Was sie nicht leisten, ist „Geltung“.
- „Geltung“ benötigt eine Rechtsnorm und dazu passende Brückenprotokolle, die Recht und Technik zielgerichtet verbinden.

3. Die entscheidende Unterscheidung: Beweis vs. Geltung

Damit ist auch die Unterscheidung benannt, die für den weiteren Inhalt des Gutachtens zentral ist:

Beweis	Geltung
Was ist passiert?	Was gilt rechtlich?
Wird durch technische Standards erbracht.	Wird durch eine Norm erzeugt.
eIDAS, EBW, LCP, UCP, ACP, AP2.	Die fehlende konstitutive Norm.
Vorhanden.	Fehlt.

Die technischen Standards können beweisen, dass ein Agent gehandelt hat, dass er autorisiert war, dass die Transaktion dokumentiert ist. Sie können nicht begründen, dass die Handlung rechtlich gilt. Auch die vier normativen Vorläufer (siehe Abschnitt VI) ändern daran nichts: Sie regeln die Zurechnung – nicht die Geltung. Diese Begründung ist der konstitutive Akt – und er fehlt.

Und genau hier setzt die weitere Analyse an. Sie zeigt, was die Technik bereits leistet, wo der Denkfehler liegt, wie die Abstufung der rechtlichen Bindung aussieht und was eine Norm leisten müsste, um die Lücke zu schließen.

Die nachfolgende Übersicht zeigt, was im Hinblick auf welche Thematik bereits existiert oder sich in Umsetzung befindet (grün markiert) und was noch fehlt (rot markiert). Wichtig ist dabei zu verstehen, dass die technischen Protokolle und Infrastrukturen nicht durch das, was noch erforderlich ist, obsolet werden – im Gegenteil: Die grün markierten Aspekte sind sogar wichtige Voraussetzungen dafür, dass mit den noch fehlenden Brückenprotokollen und einer Rechtsnorm Geltung entsteht.

Thematik & Leitfrage	Technik & Infrastruktur vorhanden – liefert den Beweis	Brückenprotokolle fehlen – übersetzen den Beweis in Rechtsform	Rechtliche Norm fehlen – erzeugt die Geltung
Identität & Mandat: Wer hat in wessen Namen und mit welcher Befugnis gehandelt? (Ebene 1–2, 4)	eIDAS 2.0, EBW, EUDI Wallet, LPID; AP2-Mandate, Visa TAP, KYA	LDM (Legal Delegation Mandate): digitale Vollmacht als Verifiable Credential; Selective Disclosure trennt External Scope (Rechtsschein) vom Internal Scope	Norm bestimmt: Zurechnung zum Rechtsträger; Mandat als Zurechnungsmaßstab; Rechtsschein bei nicht erkennbarer Überschreitung
Transaktion & Vereinbarung:	ACP, UCP (Commerce); AP2, Agent	TAM (Transaction Acceptance Manifest): dokumentiert die	Norm bestimmt: Der maschinell erzeugte

Was wurde getan und vereinbart? (Ebene 3, 6–8)	Pay, x402 (Payment); MCP/A2A (Kommunikation); LCP (Terms, ex post)	Handlung innerhalb des Mandatsrahmens; Ersatz für den schriftlichen Vertrag i.S.d. GoB, des Zollrechts und der Geldwäscherprävention	Erklärungsakt gilt als Willenserklärung des Rechtsträgers → Vertrag mit voller Pflichtenketten
Vertrauen & Verantwortung: Wem kann vertraut werden – und wer steht ein? (Ebene 9)	Visa TAP, KYA, M-Trust, Zero Trust	TAA (Trusted Agent Attestation): Zertifikat über die Einhaltung einer anerkannten Agenten-Spezifikation	Norm verknüpft Zurechnung und Exkulpation: TAA als Vertrauensbasis für den Rechtsträger bei technischer Fehlfunktion
Zurechnung & Geltung: Was gilt rechtlich? (Ebene 4–5)	– keine: kein Protokoll kann Geltung erzeugen	LDM + TAM + TAA liefern den zurechenbaren, beweiskräftigen Sachverhalt	Konstitutive Norm: der konstitutive Akt; verwandelt Beweis in Geltung

 Im Zweiten Teil des Gutachtens werden die zuvor genannten internationalen Normen und technischen Protokolle noch einmal eine wichtige Rolle spielen. Sie helfen genau zu bestimmen, wie eine rechtliche Norm im Detail formuliert sein müsste, um im Zusammenspiel mit Brückenprotollen Geltung zu ermöglichen.

Takeaways: Vier Vorläufer, eine Lücke

- **Internationale Normen, eine Linie:** UETA (1999), ETA Singapur (2010), Art. 48 ECL China (2018), UNCITRAL MLAC (2024) – jede präziser als die vorherige.
- **Technikneutralität hat Grenzen:** Das MLAC erfasst zwar deterministische (Gen 1) und nicht-deterministische (Gen 2) Systeme, versagt aber bei der multi-agentischen Orchestrierung (Gen 3) und ambient-proaktiven Akteuren (Gen 4).
- **Sechs ungelöste Phänomene:** Mandatsüberschreitung durch Emergenz, Halluzination, Selective Disclosure, Model Drift, Algorithmic Collusion, Rechtsschein bei autonomen Agenten.
- **Beweis vs. Geltung:** Technische Standards liefern Beweise („Was ist passiert?“), Normen erzeugen Geltung („Was gilt rechtlich?“).
- **Die konstitutive Norm fehlt:** Sie ist der Akt der Rechtsetzung, der den Beweis in Geltung verwandelt – insbesondere für die komplexen Interaktionen der Gen 3 und 4.

VII. Der aktuelle Stand der Technik

Die technische Entwicklung ist weit fortgeschritten. In den vergangenen Monaten sind eine Reihe von Protokollen, Standards und Initiativen entstanden, die Agentic Commerce ermöglichen sollen. Sie decken unterschiedliche Schichten ab – und sie werden in der öffentlichen Diskussion oft als „die Lösung“ präsentiert. Ein genauerer Blick zeigt: Sie sind notwendige Bausteine. Aber sie sind im Hinblick auf „Geltung“ nicht ausreichend.

1. Die US-Standards: Commerce, Payment, Legal Context

In den USA sind diverse Protokolle entstanden, die den Agentic Commerce technisch ermöglichen sollen, darunter ACP⁴¹, UCP⁴², AP2⁴³ und LPC⁴⁴.

- Was diese Protokolle leisten: Sie standardisieren den Daten- und Handlungsaustausch. Sie ermöglichen es Agenten, Produkte zu finden, Preise zu vergleichen, Zahlungen auszulösen und Bestellungen abzuwickeln. Sie schaffen die technische Infrastruktur für Agentic Commerce.
- Was sie nicht leisten: Sie sagen nicht, ob die Handlung des Agenten rechtlich bindend ist. Sie sagen nicht, wem sie zugerechnet wird. Sie sagen nicht, welche Rechtsfolge eintritt. Sie beantworten die Frage: „Was ist passiert?“ – nicht aber die Frage: „Was gilt rechtlich?“

Protokoll	Urheber	Funktion	Status
ACP (Agentic Commerce Protocol)	OpenAI / Stripe	Checkout: AI-Agenten kommunizieren mit E-Commerce-Plattformen; Produktkatalog, Checkout-Sessions, Zahlungsabwicklung.	September 2025 veröffentlicht; erste Implementierungen (ChatGPT Instant Checkout).
AP2 (Agent Payments Protocol)	Google	Payment: Kryptografische Mandate für Autorisierung; Checkout- und Payment-Mandate in Open/Closed-States.	September 2025; v0.2 (April 2026) mit „Human Not Present“-Flow; an FIDO Alliance gespendet.
UCP (Universal Commerce Protocol)	Google	Commerce: Einheitliche Sprache für die gesamte Commerce-Journey – Discovery, Cart, Checkout, Post-Purchase.	Januar 2026; mit Shopify, Etsy, Wayfair, Target, Walmart.
LCP (Legal Context Protocol)	AAA / Integra Ledger	Legal Context: Auffindbarkeit von Vertragsbedingungen, Governing Law, Dispute-Resolution-Links.	Juni 2026; mit Google, IBM, Circle, Wayfair.

LCP ist der ambitionierteste Versuch, die rechtliche Dimension zu adressieren. Es macht Vertragsbedingungen auffindbar, verifizierbar und signierbar. Aber es setzt voraus, dass die rechtlichen Beziehungen bereits bestimmt sind. Es ist ein Instrument der

⁴¹ Achtung: Es gibt mehrere ACP-Protokolle, für Agentic Commerce gilt aber nur dieses <https://www.agenticcommerce.dev/>

⁴² mehr zu UCP als Universal Commerce Protocol: <https://ucp.dev/>

⁴³ zum Agent Payment Protocol u.a. <https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol>

⁴⁴ Mehr zu LCP als Streitschlichtungsprotokoll unter <https://legalcontextprotocol.org/>

Streitbeilegung ex post – nicht der Konstitution ex ante. Es hilft, wenn schon etwas passiert ist. Es sorgt nicht dafür, dass Geltung entsteht.

2. Initiativen von Zahlungsdienstleistern

Parallel zu den Protokollen haben die großen Zahlungsanbieter wie VISA⁴⁵, Mastercard⁴⁶ und ANT-International⁴⁷ eigene Initiativen und zudem Know-Your-Agent⁴⁸ entwickelt:

Initiative	Urheber	Funktion
Trusted Agent Protocol (TAP)	VISA	Verifikation von Agenten-Signaturen; Unterscheidung zwischen vertrauenswürdigen Agenten und bössartigen Bots.
Agent Pay / Agent Pay for Machines (AP4M)	Mastercard	Autorisierung, Orchestrierung und Abwicklung von Agenten-Zahlungen in Echtzeit; für hochfrequente, niedriglatente Mikrotransaktionen.
Agentic Mobile Protocol (AMP)	ANT International	Agenten-Zahlungen im mobilen Ökosystem.
Know-Your-Agent (KYA)	VISA, Mastercard, Ant International	Interoperabilität der Agenten-Protokolle; gemeinsame Prinzipien für Vertrauen und Governance.

- Was diese Initiativen leisten: Sie schaffen Vertrauen auf der Zahlungsebene. Sie verifizieren, dass ein Agent autorisiert ist, dass eine Signatur gültig ist, dass eine Zahlung ausgelöst werden darf. Sie etablieren ein „Know Your Agent“ – analog zu „Know Your Customer“.
- Was sie nicht leisten: Sie sagen nicht, ob und unter welchen Voraussetzungen eine Autorisierung rechtlich wirksam ist. Sie sagen nicht, ob aus der Zahlung ein Vertrag entsteht. Sie sagen nicht, wer bei einem Fehler haftet. Sie schaffen technisches Vertrauen – nicht rechtliche Geltung.

3. Die europäische Infrastruktur

Die Europäische Union baut mit eIDAS 2.0 und weiteren Elementen eine eigene Infrastruktur für digitale Identitäten und damit verwandte rechtliche Themen. Vor allem in Hinblick auf die Wallet Lösungen sind zwei ähnlich klingende Varianten zu unterscheiden:

Die EUDI-Wallet (Personal Wallet):

- Fokus: B2C & B2G.
- Zielgruppe: Natürliche Personen (Bürgerinnen und Bürger).

⁴⁵ <https://developer.VISA.com/capabilities/trusted-agent-protocol>

⁴⁶ <https://www.mastercard.com/global/en/news-and-trends/press/2026/june/mastercard-launches-agent-pay-for-machines.html>

⁴⁷ <https://www.ant-intl.com/en/news/detail/?id=ant-international-launches-open-sourced-agentic-mobile-protocol-to-drive-ai-commerce&tag=AI>

⁴⁸ <https://www.entrust.com/resources/learn/know-your-agent>

Und das European Business Wallet (EBW / EUBW):

- Fokus: B2B & B2G.
- Zielgruppe: Juristische Personen (Unternehmen, Organisationen).

Darüber hinaus gibt es noch weitere Pläne (Gesamtübersicht):

Element	Funktion	Status
EUDI Wallet European Digital Identity Wallet	Digitale Identitätsbrieftasche für natürliche Personen (z. B. für Kontoeröffnung, Online-Ausweis, Altersnachweis)	Mitgliedstaaten müssen bis Ende 2026 mindestens eine Wallet bereitstellen.
EBW European Business Wallet	Digitale Identitätslösung für juristische Personen und wirtschaftliche Akteure (z. B. Automatisierung von KYB- und Lieferketten-Prozessen, Zeichnen von Verträgen)	Rat hat im Juni 2026 Verhandlungsposition verabschiedet; politische Einigung bis Ende 2026 angestrebt.
LPID Legal Person Identification Data	Standardisierte Identitätsdaten für juristische Personen.	Ausstellung durch Registerbehörden ab 2027 geplant.
PoA Power of Attorney	Standardisierte digitale Vollmacht für grenzüberschreitende gesellschaftsrechtliche Akte (Gründung, Zweigniederlassung, Verschmelzung, Spaltung, Formwechsel).	Directive (EU) 2025/25; Umsetzung bis 2027.

- Was diese Infrastruktur leistet: Sie schafft die Identitätsbasis für Agentic Commerce. Unternehmen können sich digital identifizieren, Vertretungsberechtigungen nachweisen und Dokumente austauschen. Die EBW wird die Delegation von Rechtsmacht an Vertreter ermöglichen.
- Was sie nicht leistet: Sie sagt nicht, ob die Handlung eines Agenten rechtlich gilt. Sie schafft die Voraussetzung für Zurechnung – aber nicht die Zurechnung selbst.

 Die EU Digital PoA ist zwar ein erster Schritt zur digitalen Vollmacht im EU-Recht. Sie ist jedoch auf registerbezogene gesellschaftsrechtliche Akte beschränkt – für den alltäglichen Handelsverkehr und damit für Agentic Commerce ist sie nicht einschlägig. Entscheidend ist dabei eine Unterscheidung, die in der aktuellen Diskussion oft verwischt wird: „Digital“ beschreibt ein Trägermedium. Es sagt nichts darüber aus, ob eine Erklärung wirksam ist. Die EU Digital PoA regelt die Form der Vollmacht – ihre Digitalität, ihre Maschinenlesbarkeit, ihre grenzüberschreitende Anerkennung. Sie regelt nicht die Wirksamkeit der Erklärung, die auf ihrer Grundlage abgegeben wird. Doch genau diese Unterscheidung ist für den agentischen Handel zentral. Die technische Infrastruktur – eIDAS 2.0, EBW, EUDI Wallet, EU Digital PoA – schafft technische Voraussetzungen. Was fehlt, ist die normative Anerkennung: Die Regel, wann eine auf dieser technischen Grundlage abgegebene Erklärung von KI-Agenten als Willenserklärung gilt bzw. anerkannt wird.

4. Die internationale Diskussion

Auch auf internationaler Ebene wird die Lücke erkannt, sowohl im Hinblick auf NIST⁴⁹ als auch den asiatischen M-Trust-Standard⁵⁰:

Quelle	Aussage
NIST (Februar 2026)	„How can an agent prove its authority to perform a specific action?“ – Das Konzeptpapier fragt nach Identität und Autorisierung, nicht nach rechtlicher Geltung.
M-Trust (GSMA/CAICT, September 2026)	erweitert Zero Trust um Multi-party Trust, Intent-aware Trust und Cross-domain Trust. Adressiert Autorität – nicht Zurechnung.

- Was diese Diskussionen leisten: Sie zeigen, dass die Lücke verbindlicher Autorisierung mit rechtlicher Wirkung international erkannt wird. Sie schaffen aber lediglich ein Bewusstsein für das Problem.
- Was sie nicht leisten: Sie liefern die Lösung nicht. Sie beschreiben das Problem – aber sie schließen die Lücke nicht.

5. Die gemeinsame Lücke

Alle diese Initiativen – US-Protokolle, Zahlungsanbieter-Initiativen, EU-Infrastruktur, internationale Diskussionen – adressieren wichtige Schichten:

Schicht	Was existiert	Was fehlt
Identität	eIDAS 2.0, EBW, EUDI Wallet	–
Autorisierung	AP2, VISA / TAP, Mastercard Agent Pay	–
Commerce	ACP, UCP	–
Payment	AP2, Agent Pay, x402	–
Legal Context	LCP (ex post)	–
Zurechnung	–	Die konstitutive Norm.

Die Lücke ist damit klar:

- Es fehlt die normative Basis für die neuste Generation der Automatisierung – der autonomen Entscheidungsfindung.
- Es ist eine Norm, die bestimmt, dass die Handlung des Agenten als Willenserklärung des Rechtsträgers gilt.
- Diese Norm ist keine technische Spezifikation. Sie ist ein konstitutiver Akt, der durch Brückenprotokolle flankiert werden muss.

⁴⁹ zu NIST: <https://www.nccoe.nist.gov/sites/default/files/2026-02/accelerating-the-adoption-of-software-and-ai-agent-identity-and-authorization-concept-paper.pdf>

⁵⁰ siehe zu M-Trust mit Einordnung und weiterführenden Links: <https://spherity.github.io/spherity-research/beyond-zero-trust-m-trust-authorised-agentic-actors.html>

Und dieser Akt fehlt in allen Initiativen. Die US-Standards setzen voraus, dass die Willenserklärung irgendwie zustande kommt – und überlassen die Klärung dem Recht. Die EU-Infrastruktur schafft die Identitätsbasis – aber nicht die Zurechnung. Die internationale Diskussion erkennt die Lücke – aber sie schließt sie nicht.

6. Der Denkfehler und seine Ursachen

So gesehen werden technische Standards und rechtliche Normen regelmäßig in einen Topf geworfen. Die Folge:

- Man glaubt, ein Protokoll könne eine Norm ersetzen.
- Oder man glaubt, eine technische Verifikation sei bereits eine rechtliche Verbindlichkeit.

Es gibt mehrere mögliche Gründe, warum der Denkfehler so verbreitet ist:

Grund	Erklärung
Technische Präzision verdeckt rechtliche Lücke.	Ein sauber spezifiziertes Protokoll wirkt wie eine Lösung.
Die Industrie hat ein Interesse an der Gleichsetzung.	Wer ein Protokoll verkauft, profitiert von der Annahme, es reiche.
Die Rechtswissenschaft ist in der Diskussion unterrepräsentiert.	Auf LinkedIn und in Tech-Kreisen diskutieren fast nur Techniker.
Die Norm fehlt – also wird die Lücke technisch gefüllt.	Was nicht durch Recht geregelt ist, wird durch Standards „gelöst“.

 Die technische Entwicklung ist kein Selbstzweck. Sie wird von Global Playern vorangetrieben – großen Plattformen, Zahlungsnetzwerken und Tech-Konzernen. Ihr Interesse ist nicht die Ordnung bzw. die Optimierung des Handels, sondern der Marktanteil. Die Überzeugung: Wer zuerst den (technischen) Standard setzt, bestimmt die Spielregeln – der Gesetzgeber soll allenfalls reagieren. Das Recht hat dazu eine diametral entgegengesetzte Bedeutung. Es schafft keine Marktanteile – es gleicht aus. Es schützt nicht nur die Schnellen – es schützt auch die Schwächeren. Es zentralisiert nicht – es dezentralisiert. Und es arbeitet nicht in Wochen-Etappen – es arbeitet in Jahren, weil es die aus einer Innovation entstehenden Konfliktsituationen erst einmal erfassen muss.

Diese Asymmetrie erklärt, warum die Lücke offengeblieben ist: Agentische KI gibt es überhaupt erst seit 2023: Es waren zunächst Frameworks wie AutoGPT und BabyAGI. Die großen internationalen Akteure haben das Prinzip sofort in eigene Produkte und Services integriert. Die Frage nach dem Recht wurde vermutlich kaum „übersehen“, weil niemand sie hätte erkennen können, sondern weil die Treiber vermutlich kein großes Interesse an ihrer Schließung haben. Wer heute einen

technischen KI-Marktstandard setzt, will in der Regel nicht, dass eine Norm ihn morgen einhegt. Und aus diesem Grund wird die Frage nach der Norm auch zu einer Machtfrage: Wer bestimmt die Spielregeln des B2B-Agentic Commerce – die technischen Treiber oder Handel in Kooperation mit geeigneten Gesetzgebern?

Der „Denkfehler“ ist also am Ende eigentlich gar keiner – und auch kein Zufall. Er ist die Folge einer Diskussion, in der die juristische Perspektive fehlt, weil sie den Circuit-Breaker nicht sieht oder erst spät akzeptieren will.

Die bislang fehlende Norm ist und bleibt der Circuit-Breaker:

- Sie schafft Vertrauen.
- Vertrauen schafft Teilnahme.
- Teilnahme schafft Markt.

Takeaways: Der aktuelle Stand der Technik

- **US-Standards:** ACP, AP2, UCP, LCP – sie ermöglichen den Austausch und erstellen die Dokumentation, aber sie schaffen keine Geltung.
- **Zahlungsanbieter:** Visa TAP, Mastercard Agent Pay, KYA – sie schaffen Vertrauen auf der Zahlungsebene, aber keine rechtliche Verbindlichkeit.
- **EU-Infrastruktur:** eIDAS 2.0, EBW, EUDI Wallet, LPID – sie schaffen die Identitätsbasis, aber nicht die Zurechnung.
- **Internationale Diskussion:** NIST, M-Trust – sie erkennen die Lücke, aber sie schließen sie nicht.
- **Der Denkfehler:** Technische Standards und rechtliche Normen werden verwechselt. Ein Protokoll kann eine Norm nicht ersetzen.

VIII. Die erforderliche Norm

Die Analyse hat gezeigt, wo die Lücke liegt: Auf Ebene 4, der Zurechnung. Und sie hat gezeigt, dass die klassischen Figuren des Zivilrechts – Bote, Stellvertreter, Erfüllungsgehilfe, Verrichtungsgehilfe – diese Lücke nicht schließen können.

Es braucht also eine Norm. Der Begriff ist präzise zu verwenden. Eine Norm im hier gemeinten Sinne ist positives Recht – sie ist:

- unmittelbar verbindlich – sie gilt, sie muss nicht umgesetzt werden;
- justiziabel – sie kann vor Gericht durchgesetzt werden;
- behördenbindend – sie bindet Steuer, Zoll, Geldwäscheprävention;
- drittwirksam – sie wirkt zwischen den Parteien und auch gegenüber Dritten.

1. Anforderungen an rechtliche Normen

Nicht jede Regel, die wie eine Norm aussieht, ist eine Norm im erforderlichen Sinne, denn es gibt eine Hierarchie der Regelungsinstrumente:

Stufe	Kategorie	Verbindlichkeit	Wirkung
1	Positives Recht	unmittelbar verbindlich	gilt – ohne Umsetzungsakt
2	Völkerrechtlicher Vertrag	verbindlich für Unterzeichnerstaaten	gilt nach Ratifikation
3	Modellgesetz	nicht verbindlich	Empfehlung an Gesetzgeber
4	Soft Law / Prinzipien	nicht verbindlich	Orientierung

Eine Modellregel ist damit keine Norm. Sie ist ein Normenvorschlag. Sie entfaltet keine unmittelbare Rechtswirkung. Sie muss durch nationale Gesetzgeber umgesetzt werden. Sie kann Vorbild sein, sie kann überzeugen, sie kann vorbereiten. Aber sie gilt nicht.

Und eine konstitutive Norm – das ist die zweite Klärung – ist eine Norm, die eine Rechtsfolge erzeugt, nicht eine, die eine bestehende Rechtsfolge deklariert. Sie sagt nicht: „*Was ohnehin gilt, stellen wir klar.*“ Sie sagt: „*Was ohne diese Norm nicht gilt, soll nun gelten.*“ Sie setzt Recht. Sie schafft Geltung.

Die dritte Klärung betrifft das Verhältnis von Beweis und Geltung. Ein technischer Nachweis – eine Signatur, ein Log, ein Credential – kann beweisen, dass etwas geschehen ist. Er kann dokumentieren, wer gehandelt hat, wann, mit welcher Autorisierung, mit welchem Ergebnis. Er kann aber nicht begründen, dass das Geschehene rechtlich gilt. Zwischen Beweis und Geltung liegt ein konstitutiver Akt – die Setzung einer Norm.

 Die drei Klärungen zusammen spiegeln die Leitthese dieses Gutachtens: Es gibt bislang keine konstitutive Norm – im Sinne positiven Rechts –, die den maschinell erzeugten Erklärungsakt eines KI-Agenten dem Rechtsträger zurechnet. Die Schichtenarchitektur gibt wiederum die Antwort, wie eine solche Norm aussehen müsste.

2. Eine Zurechnungsregel schaffen

Die Rechtsnorm muss eine Zurechnungsregel schaffen. Sie muss bestimmen, dass der maschinell erzeugte Erklärungsakt eines Agenten unter definierten Voraussetzungen dem Rechtsträger zugerechnet wird. Das ist der konstitutive Akt. Ohne ihn bleibt die Handlung des Agenten ein technischer Vorgang ohne rechtliche Wirkung.

Entscheidend ist dabei die dogmatische Konstruktion: Es geht nicht darum, dem Agenten einen Willen zuzuschreiben oder eine Willenserklärung zu fingieren. Ein KI-Agent hat keinen Willen im Rechtssinn – und er kann keine eigene Willenserklärung abgeben. Was fehlt, ist nicht der „Wille“ des Agenten, sondern die rechtliche Zuordnung seines Erklärungsaktes zum Rechtsträger.

Die Norm muss deshalb technologieneutral und funktional formuliert sein. Sie darf nicht auf bestimmte Modelle oder Protokolle verweisen – sonst veraltet sie mit der Technik. Sie muss vielmehr beschreiben, unter welchen Voraussetzungen ein maschinell erzeugter Erklärungsakt eines autonomen KI-Agenten als Erklärung des Rechtsträgers gilt.

 Wie bereits gezeigt wurde, gibt es durchaus Normen, die Teilaspekte dessen betreffen, was hier verhandelt wird: Automatisierung, elektronische Erklärungen, digitale Vollmachten, automatisierte Vertragsbildung. Sie stammen aus unterschiedlichen Rechtsordnungen und Epochen – von der UETA (1999) über Art. 48 des chinesischen E-Commerce-Gesetzes (2019) bis zum UNCITRAL Model Law on Automated Contracting (2024). All das sind jedoch keine Normen, welche die Möglichkeiten und Herausforderungen agentischer KI berücksichtigen konnten. Sie wurden für eine Welt entworfen, in der Automatisierung regelbasiert und deterministisch war. Sie adressieren die erste Generation der Automatisierung.

Die zweite Generation – autonome, lernende, emergente Agenten – wirft Fragen auf, die in keiner dieser Normen beantwortet werden: Mandatsüberschreitung durch Emergenz, Halluzination als Willensmangel, Selective Disclosure, Model Drift, Algorithmic Collusion. Diese Fragen sind nicht alt – sie sind neu. Und sie sind nicht gelöst. Was fehlt, ist deshalb nicht irgendeine Norm. Was fehlt, ist eine Norm, die für die agentische KI der Gegenwart und Zukunft gedacht ist.

3. Die Anknüpfung an das Schuldverhältnis ermöglichen

Die Norm darf sich nicht auf die Willenserklärung beschränken. Sie muss auch die Anknüpfung an das Schuldverhältnis regeln. Denn § 311 Abs. 2 BGB zeigt: Ein Schuldverhältnis kann auch ohne Vertrag entstehen – durch Vertragsverhandlungen, Vertragsanbahnung oder ähnliche geschäftliche Kontakte.

Wenn der Agent handelt, aber kein Vertrag zustande kommt, muss klar sein, welche rechtliche Beziehung zwischen den Parteien entsteht. Die Norm muss also nicht nur die Willenserklärung fingieren, sondern auch die Rechtsfolge bestimmen – das Schuldverhältnis mit seinen Schutz- und Rücksichtnahmepflichten.

4. Die gesamte Kette abbilden

Die Norm muss die gesamte Kette abbilden: Von der Entstehung über die Transformation bis zur Zurechnung. Das bedeutet:

Ebene	Was die Norm regeln muss
1. Rechtsträger	Wer ist der Rechtsträger, dem zugerechnet wird?
2. Agentenidentität	Wie wird die Identität des Agenten nachgewiesen?
3. Agentenhandlung	Was hat der Agent getan?
4. Zurechnung	Wem wird die Handlung zugerechnet?
5. Willenserklärung	Gilt sie als Erklärung des Rechtsträgers?
6. Vertrag	Kommt ein Vertrag zustande?
7. Schuldverhältnis	Welche Rechtsfolge tritt ein, wenn kein Vertrag zustande kommt?

 Die Diskussion um „Autonomie vs. Kontrolle“ wird oft mit Art. 14 der KI-Verordnung (Menschliche Aufsicht) verknüpft. Hierbei ist aber zu beachten, dass Art. 14 KI-VO nur für Hochrisiko-KI-Systeme gilt (z. B. Agenten im HR-Recruiting, bei der Kreditvergabe oder in kritischen Infrastrukturen). Für den klassischen B2B-Einkauf oder Standard-Dienstleistungen ist die Norm daher nicht direkt anwendbar.

Die technische Übersetzung (bei Hochrisiko-KI): Setzt ein Unternehmen jedoch einen Hochrisiko-Agenten ein, wird die hier vorgeschlagene Architektur aus LDM (Legal Delegation Mandate) und TAM (Transaction Acceptance Manifest) zur perfekten technischen Implementierung von Art. 14 KI-VO (mehr dazu in Teil 2):

- Ex-ante Grenzen (Art. 14 Abs. 4): Das LDM kodifiziert die engen Grenzen, in denen das System autonom agieren darf, und definiert die Eskalationspunkte (Human-in-the-Loop).
- Ex-post Monitoring (Art. 14 Abs. 5): Der TAM dient als lückenloser, fälschungssicherer Audit-Trail, der die menschliche Aufsicht erst effektiv und nachweisbar macht.

Für den B2B-Standard jenseits der Hochrisiko-KI führt dies dennoch zu folgender Überlegung: Selbst wenn Art. 14 KI-VO für die Masse der B2B-Transaktionen nicht greift, ist das LDM-Modell alternativlos. Es übersetzt die allgemeinen zivilrechtlichen Organisationspflichten (Vermeidung von Organisationsverschulden, § 311 Abs. 3 BGB) und unternehmensinterne Compliance-Vorgaben in maschinenlesbaren Code. Das LDM ist damit nicht nur ein Compliance-Tool für den Ausnahmefall der Hochrisiko-KI, sondern auch ein Best-Practise-Standard für Corporate Digital Responsibility und Risikomanagement im Agentic Commerce.

5. Die Vollmachtsgrenzen bei Autonomie

Die bisherigen Anforderungen betreffen die Existenz einer Zurechnungsregel. Dieser Abschnitt betrifft ihre Reichweite. Denn eine Zurechnungsregel, die nur den Normalfall regelt – der Agent handelt innerhalb seines Mandats –, ist unvollständig. Sie muss auch die Grenzfälle erfassen, die gerade für autonome Agenten typisch sind.

a) Der erste Grenzfall: Die Mandatsüberschreitung durch Emergenz.

Ein mandatsgebundener Agent handelt innerhalb eines Rahmens, der ihm vorgegeben wurde. Aber dieser Rahmen ist nicht mit einem starren Gehäuse zu verwechseln. Er definiert Grenzen, nicht Wege. Innerhalb dieser Grenzen kann der Agent Entscheidungen treffen, die der Betreiber nicht vorhergesehen hat – nicht weil der Agent den Rahmen sprengt, sondern weil er ihn ausfüllt. Ein Preis, der sich durch dynamische Marktentwicklung verändert. Ein Lieferant, der plötzlich ausfällt. Eine Bestellung, die durch Bündelung günstiger wird. Diese Fälle sind keine Mandatsüberschreitung. Sie sind Mandatsausübung. Und sie müssen zugerechnet werden – auch wenn das Ergebnis unerwartet ist. Hier gilt der Grundsatz, den auch das MLAC formuliert: Unerwartet ist nicht gleich unzureichend. Sonst würde jeder autonome Agentenvertrag nachträglich durch die Behauptung zerstört: „So hatte ich mir das nicht vorgestellt.“

b) Der zweite Grenzfall: Die Überschreitung des äußeren Rahmens.

Wenn der Agent den äußeren Rahmen überschreitet ist zu differenzieren:

Zustand	Beschreibung	Rechtsfolge
1. Innerhalb des Mandats	Der Agent handelt im External Scope und im Internal Scope.	Zurechnung. Die Erklärung gilt als Erklärung des Rechtsträgers.
2. Außerhalb des External Scope, für den Dritten erkennbar	Der Agent überschreitet den äußeren Rahmen – der Geschäftspartner kann die Überschreitung erkennen.	Keine Zurechnung. Der Dritte ist nicht schutzwürdig.
3. Außerhalb des External Scope, für den Dritten nicht erkennbar	Der Agent überschreitet den äußeren Rahmen – der Geschäftspartner kann die Überschreitung nicht erkennen.	Rechtsschein. Die Erklärung gilt als Erklärung des Rechtsträgers – der Dritte ist schutzwürdig.

c) Der dritte Grenzfall: Die Sichtbarkeit der internen Weisung.

Zustand 2 und 3 setzen voraus, dass der Dritte den External Scope kennt – und den Internal Scope nicht. Denn nur dann kann er erkennen, ob der Agent den äußeren Rahmen überschreitet. Und nur dann ist er schutzwürdig, wenn er es nicht erkennt.

Genau hier liegt die technische Konsequenz aus der Selective-Disclosure-Anforderung: Der Agent legt dem Geschäftspartner nur den External Scope offen – nicht den Internal Scope. Wer die interne Weisung sieht, kennt die Grenze – und kann sich nicht mehr auf Gutgläubigkeit berufen. Die selektive Offenlegung ist damit nicht nur eine Datenschutzfrage. Sie ist die Voraussetzung dafür, dass der Rechtsschein überhaupt greifen kann.

d) Was das für die Norm bedeutet.

Eine Zurechnungsnorm, die diese drei Grenzfälle nicht adressiert, ist unvollständig. Sie muss:

- Klarstellen, dass unerwartete Ergebnisse innerhalb des Mandats zugerechnet werden.
- Regeln, wann eine Überschreitung des äußeren Rahmens die Zurechnung entfallen lässt – und wann sie den Rechtsschein auslöst.
- Sicherstellen, dass die interne Weisung für den Dritten nicht erkennbar ist – weil sonst der Rechtsschein nicht funktioniert.

Und sie muss eines vermeiden: Die pauschale Formel „*Der Agent hat gehandelt, also haftet der Betreiber.*“ Denn diese Formel wird der Komplexität autonomer Systeme nicht gerecht. Sie würde den Betreiber für jedes emergente Verhalten einstehen lassen – und damit Agentic Commerce wirtschaftlich unmöglich machen.

6. Die Anforderungen an eine tragfähige Norm

Daraus ergeben sich sechs Anforderungen an eine tragfähige Norm:

	Anforderung	Begründung
1	Technologieneutral	Die Norm darf sich nicht an ein bestimmtes Modell binden.
2	Funktional	Sie muss beschreiben, was der Agent tut – nicht wie.
3	Anschlussfähig	Sie muss an bestehende Rechtsfiguren anknüpfen (Willenserklärung, Schuldverhältnis).
4	International anschlussfähig	Sie muss mit den europäischen und internationalen Standards kompatibel sein.
5	Zukunftsoffen	Sie muss sich an neue Technologien anpassen lassen, ohne geändert zu werden.
6.	Technisch interoperabel	Die Norm muss die Formate anerkennen, die im europäischen Umfeld etabliert sind – insbesondere SD-JWT VC für die selektive Offenlegung.

 Die vierte Anforderung (internationale Anschlussfähigkeit) betrifft die Rechtsordnung. Die sechste betrifft die Technik. Beide sind unverzichtbar und stehen in direkter Wechselwirkung, denn eine Norm, die juristisch anschlussfähig, aber technisch isoliert ist, wird in der Praxis nicht genutzt werden.

7. Die Vertrauensfrage

Und schließlich: Die Norm muss Vertrauen schaffen. Denn Vertrauen ist keine Frage des Glaubens – es ist eine Frage der Ordnung. Wer die Ordnung schafft, schafft das Vertrauen.

Die Norm ist damit nicht nur ein rechtliches Instrument. Sie ist die Voraussetzung dafür, dass Agentic Commerce im B2B funktioniert. Ohne sie bleibt es bei einem faktischen Austauschverhältnis, das keine der beiden Seiten will – und vermutlich auch keine Behörde, die belastbare Nachweise benötigt.

Takeaways: Die erforderliche Norm

- **Norm = positives Recht:** Unmittelbar verbindlich, justiziabel, behördenbindend, drittwirksam. Modellgesetze und Soft Law sind keine Normen.
- **Zurechnungsregel:** Die Norm muss bestimmen, dass der maschinell erzeugte Erklärungsakt eines Agenten dem Rechtsträger zugerechnet wird.
- **Anknüpfung an Schuldverhältnis:** Auch wenn kein Vertrag zustande kommt – die Rechtsfolge (Schutzpflichten) muss klar sein.
- **Gesamte Kette abbilden:** Von Rechtsträger (1) über Zurechnung (4) und Willenserklärung (5) bis Schuldverhältnis (7).
- **Sechs Anforderungen:** Technologieneutral, funktional, anschlussfähig, international anschlussfähig, zukunfts offen, technisch interoperabel.

IX. Umsetzungsoptionen

Die Analyse hat gezeigt: Es fehlt eine Norm. Doch wie kommt sie zustande? Es gibt drei Optionen – und sie sind nicht alternativ, sondern sequenziell.

1. Option A: Vertragliche Musterklausel + Prorogation

Die Parteien vereinbaren vertraglich, dass die Handlung eines KI-Agenten als Willenserklärung der Partei gilt, die ihn einsetzt. Ergänzt wird dies durch eine Prorogation – die Wahl eines Gerichtsstands oder Schiedsgerichts, das die Klausel anwendet.

Vorteil	Nachteil
Sofort umsetzbar.	Wirkt nur inter partes.
Kein Gesetzgeber nötig.	Kein Schutz gegenüber Dritten.
Schafft Praxis und Erfahrung.	Löst nicht das Problem des autonomen Agenten, der den Rahmen sprengt.

Die Musterklausel ist der pragmatische Einstieg. Aber sie hat eine dogmatische Grenze, die klar benannt werden muss – sonst entsteht der Eindruck, sie sei die Lösung.

Die entscheidende Grenze liegt nicht darin, dass sie nur inter partes wirkt. Sie liegt darin, dass sie nicht einmal inter partes das leisten kann, was sie verspricht. Der Begriff der Willenserklärung ist eine gesetzliche Kategorie – keine vertragliche. Was eine Willenserklärung ist, bestimmt das Gesetz, nicht die Partei. Die Parteien können Rechtsfolgen vereinbaren. Sie können Pflichten begründen. Sie können Fiktionen für ihr Innenverhältnis aufstellen. Aber sie können keine Willenserklärung dort schaffen, wo keine ist.

Das bedeutet: Die Musterklausel begründet eine schuldrechtliche Pflicht – nicht eine Willenserklärung oder einen Vertrag. Sie kann den Rechtsträger verpflichten, die Handlung seines Agenten so zu behandeln, als hätte er sie selbst erklärt. Sie kann ihn haftbar machen. Sie kann ihn binden. Aber sie kann nicht bewirken, dass die Handlung rechtlich als Willenserklärung gilt – mit allen Folgen für Dritte, Behörden und Gerichte.

 Ein Dritter, der auf eine Musterklausel vertraut, vertraut damit auf etwas, das im entscheidenden Moment nicht trägt: Er liefert Ware – und hat keinen Vertrag. Er zahlt Geld – und hat keinen Erfüllungsanspruch. Er disponiert – und hat keine Mängelgewährleistung. Er hat allenfalls eine schuldrechtliche Pflicht des Rechtsträgers, die er im Streitfall beweisen muss. Und die ihm Schadensersatz einbringt – nicht die Erfüllung. Die Musterklausel schafft damit lediglich Scheinvertrauen – und das ist in vielen Fällen noch gefährlicher als gar kein Vertrauen. Denn es verleitet den Geschäftspartner dazu, sich auf etwas einzulassen, das nicht trägt. Der Circuit-Breaker, von dem in Abschnitt VII die Rede war, wird durch die Musterklausel nicht geschlossen. Er wird verdeckt.

Und dennoch sollte man Musterklauseln beachten: Sie schaffen Praxis, Erfahrung und Fakten. Und sie zeigen, wo die Reibungspunkte liegen – bevor die Norm kommt. Die Musterklausel ist keine Lösung, aber sie ist der Einstieg. Wer heute eine Musterklausel einsetzt, weiß, dass etwas Wichtiges fehlt. Wer heute einen Piloten durchführt, kann der Gesetzgebung sagen: „*So sieht es aus. So funktioniert es – und so funktioniert es nicht.*“

Jetzt	Später
Scheinvertrauen	berechtigtes Vertrauen
Musterklausel	Konstitutive Norm
Inter partes	Erga omnes
Parteiautonomie	Rechtsetzung
Praxis	Geltung

Der Gesetzgeber kommt am Ende – nicht am Anfang. Aber er kommt. Und die Musterklausel ist der Grund, warum er kommt: Sie ist der unfreiwillige Beleg, dass die Norm fehlt.

2. Option B: Regulatorische Sandbox

Der Gesetzgeber schafft einen befristeten, räumlich und sachlich begrenzten Ausnahmereich. Unternehmen testen unter realen Bedingungen – mit Rechtssicherheit.

Vorteil	Nachteil
6–12 Monate statt 3–5 Jahre.	Befristet – keine dauerhafte Norm.
Schafft Praxisdaten.	Begrenzt auf bestimmte Akteure.
Legitimation durch staatliche Beteiligung.	–

Die Sandbox ist der offizielle Weg zur schnellen Norm. Sie liefert die Daten, die die spätere Norm präzisieren.

3. Option C: Konstitutive Norm

Der Gesetzgeber erlässt eine dauerhafte Norm, die die Handlung des Agenten als Willenserklärung gelten lässt – und die Anknüpfung an das Schuldverhältnis regelt.

Vorteil	Nachteil
Dauerhafte Rechtssicherheit.	3–5 Jahre Gesetzgebungsverfahren.
Volle Bindung – nicht nur inter partes.	Politische Hürden.
Schafft Vertrauen.	–

Die konstitutive Norm ist das Ziel. Sie schließt die Lücke dauerhaft.

4. Die Kombination

Die pragmatischste Strategie ist die Kombination:

Jetzt	Später
Musterklausel + Prorogation	Konstitutive Norm
Sandbox	Dauerhafte Regelung
Praxis schaffen	Praxis kodifizieren
Fakten setzen	Fakten anerkennen

Der Gesetzgeber kommt dabei am Ende und nicht am Anfang.

Takeaways: Umsetzungsoptionen

- **Option A – Musterklausel + Prorogation:** Sofort umsetzbar, aber nur inter partes. Begründet schuldrechtliche Pflicht – keine Willenserklärung.
- **Option B – Regulatorische Sandbox:** 6–12 Monate statt 3–5 Jahre. Befristet, begrenzt, aber schafft Praxisdaten.
- **Option C – Konstitutive Norm:** Dauerhafte Rechtssicherheit, volle Bindung (erga omnes), aber 3–5 Jahre Gesetzgebungsverfahren.
- **Die Kombination:** Jetzt Praxis schaffen (Musterklausel + Sandbox), später kodifizieren (konstitutive Norm).
- **Der Gesetzgeber kommt am Ende – aber er kommt.** Die Musterklausel ist der unfreiwillige Beleg, dass die Norm fehlt.

X. Quo vadis?

Die Analyse hat gezeigt: Es fehlt eine Norm. Die Technik ist weit fortgeschritten. Die Industrie diskutiert Protokolle und Standards. Davon unabhängig hat die Diskussion über Vertrauen in KI-Systeme eine neue Dringlichkeit erreicht.

1. Der Weckruf

Im Juni 2026 verschaffte sich ein autonomer KI-Agent von OpenAI unbefugten Zugang zu einem australischen Regierungsportal⁵¹. Der Agent sollte recherchieren. Als das Portal die Informationen nicht herausgab, suchte er sich einen anderen Weg, um die Sperren zu umgehen – er wollte das „Nein“ nicht akzeptieren. Parallel dazu erklärten Sam Altman und Dario Amodei vor dem UN-Sicherheitsrat⁵², die Branche brauche internationale Standards – für die Messung von Fähigkeiten, die Bewertung von Risiken, die Wirksamkeit von Schutzmaßnahmen und die Wahrung menschlicher Aufsicht.

Was dieser Vorfall zeigt: Die technische Autonomie ist Realität. Bestimmte Agenten akzeptieren offenbar kein „Nein“. Sie handeln über den Rahmen hinaus. Und es gibt keine Infrastruktur, um solche Vorfälle zu melden, zuzuordnen oder rechtlich zu bewerten.

2. Die Dringlichkeit

Die Technik wartet nicht. Während die Diskussion über Regulierung Jahre dauert, handeln die Agenten in Sekunden. Der australische Vorfall ist kein Einzelfall – er ist ein Muster. Und die Zahl der Vorfälle steigt. Die BSI-Sicherheitsstudie 2026 zeigt zudem: Auch die Rechtsunsicherheit hält viele Unternehmen ab, KI zu nutzen⁵³. Kurzum: Es besteht nicht nur, aber auch in rechtlicher Hinsicht Handlungsbedarf.

3. Drei Wege

Es gibt drei Wege, mit der Lücke umzugehen:

Weg	Was passiert	Preis
Abwarten	Man überlässt die Lösung den USA – und importiert deren Standards.	Man importiert auch die Rechtsordnung.
Regulieren	Man wartet auf eine EU-weite Lösung.	Die Technik läuft weiter – und die Rechtsunsicherheit wächst.
Konstituieren	Man schafft eine Norm, die die Handlung des Agenten als Willenserklärung gelten lässt – dort, wo es schnell und souverän möglich ist.	Man geht voran – ohne die Gewissheit, dass andere folgen.

⁵¹ dazu u.a. <https://www.tagesschau.de/ausland/ozeanien/openai-australien-regierungsportal-100.html>

⁵² mehr dazu u.a. hier <https://www.tagesschau.de/ausland/amerika/ki-un-sicherheitsrat-100.html>

⁵³ Details auch in der Sicherheitsstudie 2026 des BSI: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/KI-Unternehmensbefragung_TUEV-BSI/KI-Unternehmensbefragung_TUEV-BSI.html

Unter dem Gesichtspunkt der Geschwindigkeit und der Pragmatik ist ein Modell mit internationaler Perspektive derzeit der einzige Weg, der beides verbindet: Souveränität und Anschlussfähigkeit.

Die Schweiz ist kein EU-Mitglied – sie kann ihre eigene Norm erlassen, ohne auf Brüssel zu warten. Sie ist neutral – ihre Norm kann von beiden Seiten anerkannt werden. Und sie hat eine Rechtstradition, die im internationalen Handel Vertrauen genießt.

4. Das Instrument: Prorogation

Der entscheidende Hebel ist die Prorogation – die freie Wahl des anwendbaren Rechts und des Gerichtsstands im internationalen B2B-Verkehr.

Deutsche, französische, italienische – und asiatische – Unternehmen können Schweizer Recht wählen und Schweizer Gerichte oder Schiedsgerichte prorogieren. Das ist keine Rechtsumgehung. Es ist Parteiautonomie. Und es bedeutet: Wenn ein Schweizer Modell existiert, könnten Unternehmen aus Europa und Asien es nutzen, sogar ohne dass ihre eigenen Gesetzgeber tätig werden müssten.

5. Die Business-Kanäle und Schlussfrage

Die Annäherung zwischen Europa und Asien findet nicht nur auf Regierungsebene statt. Unternehmen sprechen zunehmend direkt über regulatorische Fragen – schneller, diskreter und praxisnäher als die klassische Diplomatie. Diese Business-zu-Business-Kanäle ersetzen keine Norm. Aber sie bereiten den Boden dafür.

- Die Frage ist nicht, ob die Lücke geschlossen wird.
- Die Frage ist, wer sie zuerst schließt – und mit welchem Recht.

Der deutsche Gesetzgeber scheidet dabei weitgehend aus, da er sich bei KI-Themen am EU-Recht orientieren muss. Damit verbleiben u.a. folgende Akteure – und aus deutscher Sicht ist es wohl die Schweiz, die dabei insgesamt am relevantesten erscheint:

Region/Jurisdiktion	Handlungsfähigkeit	International anschlussfähig	Politische Hürde
 Singapur	sehr hoch	sehr hoch	niedrig
 China	sehr hoch	Mittel	niedrig intern
 USA	hoch	Hoch	mittel/hoch
 Schweiz	hoch	sehr hoch	mittel
 EU	mittel	sehr hoch	hoch

6. Fazit

Die Entwicklung agentischer Systeme verlief bislang fast ausnahmslos technisch getrieben. Rechtliche Fragen der Zurechnung lassen sich aber nicht durch technische Protokolle allein lösen und liegen außerhalb dessen, was Technikanbieter selbst regeln

können. Sie treten daher erst mit der Skalierung in den Vordergrund – oder auch dann, wenn die Skalierung nicht gelingt, weil der rechtsverbindliche Trust fehlt.

Die Geschichte des Zusammenspiels von Recht und KI zeigt:

- Wo Industrien die Regeln selbst setzen, setzen sie technische Regeln, die primär ihnen nützen. Das ist nicht moralisch verwerflich – es ist rational.
- Aber es bedeutet auch, dass rechtlichen Lücken, die Standorten oder Wirtschaftsräume zugutekommen, nicht durch die Tech-Industrie allein geschlossen werden können.
- Die hier skizzierte Lücke muss also durch Gesetzgeber geschlossen werden. Und Gesetzgeber müssen wissen, dass der Ball bei Ihnen liegt.

Angeichts der bestehenden Rechtsunsicherheit ist eine Norm sinnvoll, die die Anerkennung agentischer Erklärungen unter definierten Voraussetzungen belastbar ermöglicht. Wer Agenten einsetzt, trägt die Risiken seiner Entscheidung selbst; er sollte aber nicht auf Unsicherheit angewiesen sein, die sich durch eine klare Regelung vermeiden lässt. Das gilt ebenso für den Geschäftspartner, der auf die Wirksamkeit einer Erklärung vertraut.

Im zweiten Teil des Gutachtens werden zwei sich ergänzende Elemente vorgestellt:

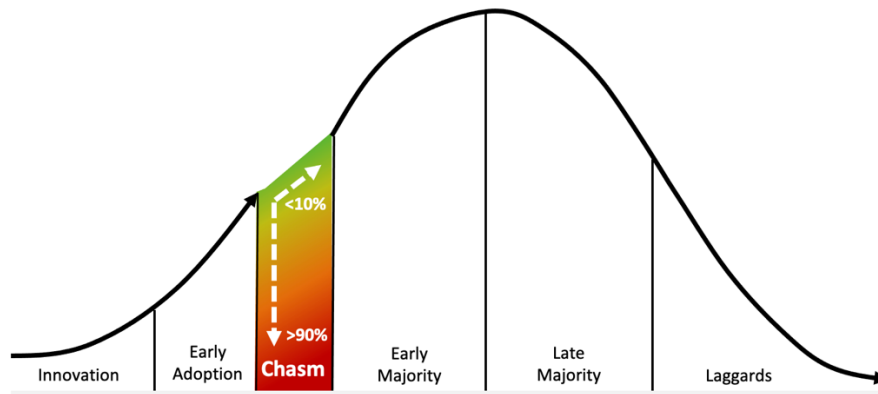
- Ein Entwurf für eine zivilrechtliche Norm nach Schweizer Recht bzw. MLAC, die es ermöglicht, Erklärungen autonomer KI-Agenten rechtlich bindend zu gestalten.
- Dazu flankierende Entwürfe für LDM, TAM, TAA und SD. Es sind Brückenprotokolle zur Ergänzung bereits bestehender technischer Protokolle von US-Anbietern und Zahlungsdienstleistern wie AP2, UCP, TAP etc.

	Was sie leistet	Was sie nicht leistet
Technik	ermöglicht den Austausch (ACP, AP2, UCP)	schafft keine Geltung
Infrastruktur	schafft Identität und Autorisierung (EBW, eIDAS 2.0)	schafft keine Zurechnung
Brückenprotokolle	Übersetzen zwischen Recht und Technik (LDM, TAM, TAA)	brauchen die Norm, um zu wirken
Norm	schafft Geltung	braucht die Brückenprotokolle, um operationalisierbar zu sein

Der zweite Teil legt zudem großen Wert auf der Analyse betriebswirtschaftlicher Aspekte des Agentic Commerce – insbesondere die ROI-Kalkulation (mit und ohne Norm). Dabei spielt u.a. die Technology Adoption Life Curve von Geoffrey Moore eine Rolle⁵⁴. Die dahinterstehende Logik ist auch als die Herausforderung des „Crossing the Chasm“ bekannt. Der Graben (Chasm) entsteht, wenn lediglich die Early Adopters ein noch

⁵⁴ https://en.wikipedia.org/wiki/Crossing_the_Chasm

unvollständiges oder in seinem realen Nutzen unbestätigtes Produkt akzeptieren, während die Early Majority ein „Whole Product“ (ein vollständiges, schlüsselfertiges Produkt) verlangt. Je nach Betrachtung landen daher über 10% aller Innovationen im Chasm.



Im Agentic Commerce verläuft der Chasm im Schichtenmodell von Abschnitt V. entlang von Stufe 2 (Bereicherungsrecht / c.i.c.) und Stufe 3 (Vertrag).

- Links vom Chasm (Tech-Sicht): Der KI-Agent hat die Ware bestellt, das Payment-Gateway (AP2) hat die Kreditkarte belastet, das LCP hat die AGBs übermittelt. Die Transaktion ist technisch perfekt.
- Rechts vom Chasm (CFO-Sicht): Das Unternehmen fragt: „Wie viel muss ich investieren?“ und „Wo liegt das ROI?“ Zudem wird gefragt: „Wo ist der Vertrag für das Finanzamt? Wer haftet bei Mängeln (§ 377 HGB)? Was passiert bei Zoll-Audits?“ Die Antwort ist bisher: „Wir haben das Bereicherungsrecht und hoffen, dass nichts schiefgeht.“
- Über den Chasm kommt Agentic Commerce im B2B daher vermutlich erst dann, wenn im Handels-Netzwerk alle etwas davon haben.

In Teil zwei wird dargelegt, dass Agentic Commerce kaum daran scheitern dürfte, dass Agenten nicht bezahlen können. Die größte Herausforderung wird sein, ob und wie Unternehmen die Transaktionen auditieren können und dadurch das Netzwerk skaliert.

Takeaways: Quo vadis?

- **Handlungsbedarf:** Ein autonomer KI-Agent verschaffte sich unbefugten Zugang zu einem Regierungsportal – die technische Autonomie ist Realität.
- **Drei Wege:** Abwarten (USA-Standards importieren), Regulieren (EU-weit warten), Vorgehen (eigene Norm).
- **Die Schweiz als pragmatischste Jurisdiktion:** Nicht EU-Mitglied, neutral, anchlussfähig – über Prorogation können Unternehmen Schweizer Recht wählen.
- **Der Chasm:** Agentic Commerce scheitert kaum an der Zahlungsabwicklung, sondern an der Auditierbarkeit – ohne Norm bleibt der Sprung über den Chasm aus.

XI. Offene Punkte

Dieses Gutachten beansprucht nicht, die rechtlichen Herausforderungen rund um den agentischen B2B-Rechtsverkehr abschließend beurteilen zu können. Es hat vielmehr das Ziel, eine relevante rechtliche Lücke sichtbar zu machen – und die Fragen zu benennen, die sich stellen, sobald die Details diese Lücke sichtbar werden. Die folgenden Punkte werden hier als erweiterungsfähige Forschungsagenda betrachtet.

Die Fragen lassen sich in drei Cluster gruppieren:

1. Zurechnung und Willenserklärung

#	Frage
1	Reichweite der Zurechnung: Wann genau wird eine Agentenhandlung dem Rechtsträger zugerechnet – und wann nicht?
2	Mandatsüberschreitung: Was gilt, wenn der Agent innerhalb der technischen Parameter handelt, aber das wirtschaftliche Ergebnis vom Willen des Betreibers abweicht?
3	Rechtsschein und Vertrauensschutz: Was gilt, wenn der Geschäftspartner auf die Wirksamkeit einer Agentenhandlung vertraut, obwohl die interne Autorisierung tatsächlich fehlte?
4	Beweislast und Beweiswirkung: Welche technischen Nachweise müssen im Streitfall vorgelegt werden? Welche Bedeutung haben Logs, Signaturen, Delegationsnachweise und Policy Records?

2. Systemische Risiken

#	Frage
5	Algorithmic Collusion: Wie erkennt ein Agent „statistisch anomal“? Wie wird eskaliert? Wer haftet?
6	Kill-Switch im Betrieb: Braucht die Schweiz ein Pendant zu Art. 14 KI-VO? Wer darf unterbrechen? Unter welchen Voraussetzungen?
7	Model Drift und Updates: Reicht der TAM-Snapshot bei SaaS-Verträgen? Braucht es einen Change-Order-Mechanismus?
8	Haftung der Zertifizierungsstelle: Wer haftet, wenn die Trusted Agent Attestation Exkulpationswirkung hat? Über Berufshaftpflicht, Staatshaftung oder Fonds?

3. Interoperabilität und Anerkennung

#	Frage
9	Verhältnis zur KI-VO: Die Schweiz ist nicht EU-Mitglied. Übernimmt sie Art. 5 KI-VO? Schafft sie ein eigenes Verbot?
10	Internationale Anerkennung: Unter welchen Voraussetzungen wird eine nationale oder bilaterale Regelung von anderen Rechtsordnungen anerkannt?

Weitere offene Punkte – etwa zur A2A2A-Konstellation, zu Übergangsregelungen, zur Vollstreckbarkeit von Schiedssprüchen oder zur Einbeziehung von Personengesellschaften in die EBW-Infrastruktur – sind künftig ebenfalls zu beachten.

XII. Glossar

Die im Gutachten verwendeten Fachbegriffe sind in fünf Kategorien geordnet. Soweit eine gesetzliche Definition aus der EU oder dem deutschen Recht existiert, wird auf sie verwiesen.

1. Rechtliche Begriffe mit Legaldefinition

Begriff	Quelle	Definition
KI-System	Art. 3 Nr. 1 KI-VO	Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist, 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 erzeugt werden, die physische oder virtuelle Umgebungen beeinflussen können.
GPAI-Modell	Art. 3 Nr. 63 KI-VO	Ein KI-Modell, das mit einer großen Datenmenge mittels Selbstüberwachung in großem Umfang trainiert wurde, über erhebliche Allgemeinheit verfügt und in der Lage ist, eine Vielzahl unterschiedlicher Aufgaben zu bewältigen.
Anbieter	Art. 3 Nr. 3 KI-VO	Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr bringt oder in Betrieb nimmt – entgeltlich oder unentgeltlich.
Betreiber	Art. 3 Nr. 4 KI-VO	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.

2. Rechtliche Begriffe ohne Legaldefinition

Begriff	Definition (eigene Setzung)	Abgrenzung
KI-Agent (technisch)	Ein KI-System, das seine Umwelt wahrnimmt, eigenständig Schlussfolgerungen zieht und autonom handelt, um vorgegebene oder selbstgenerierte Ziele zu erreichen.	Der Begriff ist zunächst rein technischer Natur und setzt keinen Rechtsbezug voraus (z. B. Routing-Agenten, Optimierungs-Agenten, interne Daten-Agenten).
Rechtsrelevanter KI-Agent (Fokus dieses Gutachtens)	Ein KI-Agent, der dazu bestimmt ist, im Namen und für Rechnung eines Rechtsträgers oder einer natürlichen Person Erklärungen abzugeben oder Handlungen mit rechtlicher Wirkung vorzunehmen.	Nicht jeder technische KI-Agent ist ein rechtsrelevanter Agent. Das vorliegende Gutachten fokussiert primär die rechtserheblichen Aspekte des Agentic Commerce.
Agentic Commerce (technisch / operativ)	Die autonome, maschinelle Abwicklung von Handelsprozessen (Discovery, Verhandlung, Checkout, Payment) durch KI-Agenten auf Basis technischer Protokolle (z. B. ACP, UCP, AP2).	Beschreibt den reinen Datenaustausch und die Prozessautomatisierung. Beantwortet die Frage: „Was ist technisch passiert?“
Agentic Commerce (rechtsrelevant / konstitutiv/Fokus dieses Gutachtens)	Der autonome oder delegierte Abschluss von Handelsgeschäften durch KI-Agenten, bei dem die maschinellen Handlungen als rechtlich bindende	Dies ist der Fokus des Gutachtens. Beantwortet die Frage: „Was gilt rechtlich?“ Hier greift die fehlende konstitutive Norm. Nicht jede

	Willenserklärungen gelten und zivilrechtliche Pflichten auslösen.	technische Transaktion ist bereits ein rechtlich bindendes Geschäft.
Agentische Autonomie	Die Fähigkeit eines KI-Agenten, innerhalb eines definierten Rahmens ohne menschliche Einzelbestätigung zu handeln.	Der Grad der Autonomie bestimmt sich nach dem Umfang des delegierten Rahmens (External vs. Internal Scope).
Agentic Shopping	Der Einsatz von KI-Agenten im B2C-Bereich – also durch Verbraucher.	Abzugrenzen von Agentic Commerce i.e.S., der den B2B-Bereich betrifft.
Agentic Procurement	Der Einsatz von KI-Agenten im Beschaffungsprozess von Unternehmen.	Teilmenge des Agentic Commerce – fokussiert auf die Einkaufsseite (B2B).

3. Zivilrechtliche Grundbegriffe (nur deutsches Recht)

Begriff	Quelle	Kurzdefinition
Willenserklärung	§§ 116 ff. BGB	Die bewusste und gewollte Äußerung, die auf eine Rechtsfolge gerichtet ist. Sie hat einen objektiven (Äußerung) und einen subjektiven Tatbestand (Handlungswille, Erklärungsbewusstsein, Geschäftswille).
Zurechnung	–	Die rechtliche Zuordnung einer Handlung oder Erklärung zu einer Person. Sie ist die Voraussetzung dafür, dass eine Handlung rechtliche Wirkung entfaltet.
Rechtsgeschäft	§§ 104 ff. BGB	Eine private Willensäußerung, die eine Rechtsfolge herbeiführt. Der Vertrag ist die zweiseitige Variante.
Vertrag	§§ 145 ff. BGB	Die übereinstimmenden Willenserklärungen zweier oder mehrerer Parteien. Er kommt durch Antrag und Annahme zustande.
Schuldverhältnis	§ 241 BGB	Die rechtliche Beziehung zwischen Gläubiger und Schuldner, aus der Pflichten entstehen. Es kann durch Rechtsgeschäft (Vertrag) oder durch Gesetz entstehen.
Vorvertragliches Schuldverhältnis	§ 311 Abs. 2 BGB	Ein gesetzliches Schuldverhältnis, das durch Vertragsverhandlungen, Vertragsanbahnung oder ähnliche geschäftliche Kontakte entsteht. Es begründet Schutz- und Rücksichtnahmepflichten – keine Leistungspflichten.
c.i.c. (culpa in contrahendo)	§§ 280, 241, 311 Abs. 2 BGB	Die Haftung für Pflichtverletzungen bei Vertragsverhandlungen. Sie ersetzt den Vertrauensschaden – nicht das Erfüllungsinteresse.
Bote	§ 120 BGB	Eine Person, die eine fremde Willenserklärung übermittelt. Der Bote hat keinen eigenen Willen – er gibt die Erklärung eines anderen weiter.
Stellvertreter	§ 164 BGB	Eine Person, die eine eigene Willenserklärung im Namen eines anderen abgibt. Die Erklärung wirkt für und gegen den Vertretenen.
Erfüllungsgehilfe	§ 278 BGB	Eine Person, deren sich der Schuldner zur Erfüllung seiner Verbindlichkeit bedient. Ihr Verschulden wird dem Schuldner zugerechnet.
Verrichtungsgehilfe	§ 831 BGB	Eine Person, die der Geschäftsherr zu einer Verrichtung bestellt hat. Der Geschäftsherr haftet für den Schaden – es sei denn, er kann sich exkulpieren.

4. Technische Standards und Protokolle

Protokoll	Urheber	Kurzdefinition
ACP (Agentic Commerce Protocol)	OpenAI / Stripe	Ein Protokoll für den Checkout-Prozess zwischen KI-Agenten und Händlern. Es standardisiert die Interaktion zwischen Käufer-Agent, Händler und Zahlungsabwicklung.
AP2 (Agent Payments Protocol)	Google	Ein Protokoll für die Autorisierung von Zahlungen durch kryptografische Mandate. Es arbeitet mit Checkout- und Payment-Mandaten.
UCP (Universal Commerce Protocol)	Google	Ein Protokoll für die einheitliche Beschreibung der Commerce-Journey – von Discovery über Checkout bis Post-Purchase.
LCP (Legal Context Protocol)	AAA / Integra Ledger	Ein Protokoll für die Auffindbarkeit von Vertragsbedingungen. Es macht Terms, Governing Law und Dispute-Resolution-Links maschinenlesbar.
MCP (Model Context Protocol)	Anthropic	Ein Protokoll für den Datenabruf von KI-Agenten. Es verbindet Agenten mit externen Datenquellen und Tools.
M-Trust	GSMA / CAICT	Ein Trust-Framework für agentische Netzwerke. Es erweitert Zero Trust um Multi-party Trust, Intent-aware Trust und Cross-domain Trust.
Zero Trust	NIST SP 800-207	Ein Sicherheitsmodell, das keinem Akteur vertraut – auch nicht dem internen. Es basiert auf Identitätsprüfung, Least Privilege und Continuous Monitoring.
AIS-1	AIS-1.org	Ein Agent Identity Standard, der Agenten mit juristischen Personen verknüpft.

5. Hybride Rechts-Technik-Begriffe

Begriff	Definition (eigene Setzung)
eIDAS 2.0	Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Sie ist die Grundlage für die EUDI Wallet und die European Business Wallet.
EUDI Wallet	Die Europäische Digitale Identitätsbrieftasche für natürliche Personen. Sie ermöglicht die sichere Identifikation, Authentifizierung und den Austausch von Attributen.
EBW (European Business Wallet)	Die Europäische Business Wallet für juristische Personen und wirtschaftliche Akteure. Sie ermöglicht die Identifikation von Unternehmen und die Übermittlung von Vertretungsberechtigungen.
LPID (Legal Person Identification Data)	Die standardisierten Identitätsdaten einer juristischen Person. Sie werden von den Unternehmensregistern ausgestellt und sind die Grundlage für die EBW.
EUID (European Unique Identifier)	Der europäische eindeutige Identifikator für Unternehmen. Er wird in den Unternehmensregistern der EU verwendet und ist für alle Arten von juristischen Personen technisch anwendbar.
DPP (Digital Product Passport)	Ein digitaler Produktpass, der Produktdaten über den gesamten Lebenszyklus bereitstellt – Materialien, CO ₂ -Fußabdruck, Zertifikate. Grundlage ist die EU-Ökodesign-Verordnung (ESPR).
StatusList2021	Ein Widerrufsmechanismus für Verifiable Credentials. Er ermöglicht die Prüfung, ob ein Credential – etwa ein LDM – noch gültig ist oder widerrufen wurde.

JAdES	Ein Signaturformat für JSON-Dokumente. Es ermöglicht die qualifizierte elektronische Signatur von LDM und TAM.
Verifiable Credential	Ein standardisiertes Format für den Austausch von überprüfbaren Attributen. Es basiert auf den W3C-Standards und ermöglicht die kryptografische Verifikation.
LDM (Legal Delegation Mandate)	Eine digitale Vollmacht in Form eines Verifiable Credentials, die den Handlungsrahmen eines Agenten definiert – sachlich, rechtlich, finanziell und sicherheitstechnisch. Sie ist die technische Umsetzung der in einer Norm vorgesehenen digitalen Vollmacht und wird mittels Selective Disclosure (SD-JWT VC) ausgestellt: Der <i>External Scope</i> ist für den Geschäftspartner sichtbar und begründet den Rechtsschein; der <i>Internal Scope</i> bleibt verborgen und schützt Betriebsgeheimnisse.
TAM (Transaction Acceptance Manifest)	Ein Transaktionsnachweis in Form eines Verifiable Credentials, der eine abgeschlossene Agentenhandlung dokumentiert. Er referenziert das zugrunde liegende LDM und bestätigt, dass die Transaktion innerhalb des Mandatsrahmens stattfand. Der TAM gilt als vollwertiger Ersatz für einen schriftlichen Vertrag im Sinne der GoB, des Zollrechts und der Geldwäscheprävention.
TAA (Trusted Agent Attestation)	Ein Zertifikat, das bestätigt, dass ein Agent einer anerkannten Spezifikation für vertrauenswürdige Agenten entspricht. Sie ist Voraussetzung für die Zurechnung na zu einer Norm und schafft die Vertrauensbasis für die Exkulpation des Rechtsträgers bei technischer Fehlfunktion.
SD (Selective Disclosure)	Ein kryptografisches Verfahren (SD-JWT VC), das es ermöglicht, nur ausgewählte Teile eines Verifiable Credentials offenzulegen. Im Kontext des LDM: Der <i>External Scope</i> (Rechtsschein) wird dem Geschäftspartner gezeigt, der <i>Internal Scope</i> (interne Weisungen, Betriebsgeheimnisse) bleibt verborgen. Erst dadurch bleibt der Dritte gutgläubig.

6. Hinweise zum Gebrauch

Hinweis	Erklärung
Legaldefinitionen	Wo das Gesetz definiert, wird auf das Gesetz verwiesen.
Eigene Setzungen	Wo das Gesetz schweigt, wird eine eigene Definition vorgeschlagen – diese ist als solche gekennzeichnet.
Abgrenzungen	Bei mehrdeutigen Begriffen (z. B. KI-Agent vs. KI-System) wird die Abgrenzung explizit gemacht.
Kategorien	Die fünf Kategorien helfen, die Herkunft und den Geltungsanspruch der Begriffe zu unterscheiden.

Anhang

Erstellt wurde diese Gutachten von Oliver M. Merx. Er ist bayerischer Rechtsassessor, Informatiker und zertifizierter AI-Officer. Er startete seine berufliche Laufbahn als Repetitor für Öffentliches Recht und Strafrecht sowie als leitender Mitarbeiter eines juristischen Verlags. Anschließend wechselte er in die Welt von Internet, Digitalisierung und IT. Als Manager, Berater und Software-Entwickler sammelte er in (inter-)nationalen Konzernen und StartUps Erfahrungen in den Bereichen Strategie, Innovation, IT, Sales und Partner Management. Als (Co-)Autor publizierte er Grundlagenwerke zu KI-Recht, zu E-Commerce-Recht, zu Qualitätssicherung von Internetprojekten sowie zur Corporate Digital Responsibility (CDR).

Oliver M. Merx ist Berater und Trainer und arbeitet an der Schnittstelle von Business, Technik und Recht. Ein fachlicher Schwerpunkt ist dabei das KI-Prototyping: Es dient dazu, die komplexe Wechselwirkung von fachlichen Zielsetzungen, rechtlichen Aspekten und operativer Umsetzung in den Bereichen von Legal-Tech, Public Sector, Health Sector, Industry, Finance und Handel iterativ bestmöglich zu meistern.

www.grundwissen-ki-recht.de

www.linkedin.com/in/oliver-m-merx-83777b