Einführung

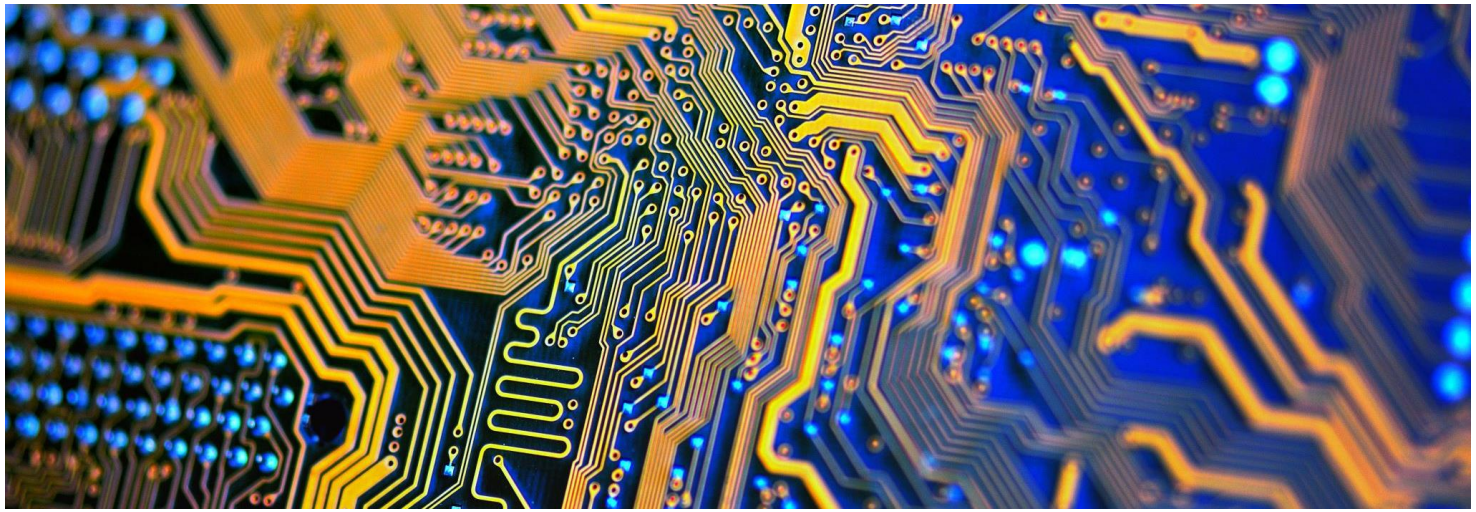
Dr. Sandra Marmy, Schiffbau Rechtsanwälte, Zürich

DigitUP 13. Mai 2025 – Zürich

Was sind KI-Agenten?

*„KI-Agenten sind **Softwaresysteme, die KI verwenden**, um im Namen von Nutzern **Ziele zu verfolgen und Aufgaben zu erledigen**. Sie zeigen logisches Denken, können **planen und sich erinnern** und haben ein gewisses Maß an Autonomie, um **Entscheidungen** zu **treffen**, zu lernen und sich anzupassen.“*

(Quelle: Google Cloud, abgerufen unter https://cloud.google.com/discover/what-are-ai-agents?hl=de)



Wie unterscheiden sich KI-Agenten von «herkömmlicher» KI?

- Hauptunterscheidungsmerkmal: **Grad an Autonomie** - Grenzen sind aber fliessend

	KI-Agenten	Herkömmliche KI
Handlungsweise	Vorschlagen, umsetzen und ausführen **Proaktiv**	Antworten **reaktiv**
Umsetzung von Aufgaben	Eigenständig neue Aufgaben definieren und ausführen	Auf vorgegebene Aufgaben reagieren
Interaktion mit anderen Webseiten und Plattformen	Eigenständig; bspw. abschliessen einer Reservation, senden einer Mail, etc.	Keine oder sehr begrenzte Interaktion; bspw. Vorschlag, was man tun könnte, aber keine eigenständige Umsetzung

Relevante rechtliche Aspekte?

- KI-Agenten – Anwendung in der Praxis (insb. Schichtplanung und Produktion, Daniela Gnaegi, Accenture)
- KI-Vertragsthemen (Roland Mathys, Schellenberg Wittmer AG)
- Haftungsrechtliche Fragen im Zusammenhang mit KI-Agenten (Sven Kohlmeier, Wicki Partners AG)
- Immaterialgüterrechtliche Fragen rund um KI-Agenten (Alesch Staehelin, Uto Legal)
- KI-Agenten und EU-Regulierung (Carmen de la Cruz, Axians Schweiz AG)

KI Agenten: Anwendung in der Praxis

#DigitUp 2025 - Zürich, 13. Mai 2025

Daniela Gnaegi Bernstein
Fürsprecherin, LLM
Accenture - Industry X

Wichtige Begriffe: KI, Gen KI KI-Agent

Künstliche Intelligenz (KI)

Die **Technologie**, wie «machine learning», oder Bilderkenning, die Maschinen in die Lage versetzt, Aufgaben zu lernen und auszuführen.

Bsp: Datenanalyse, Prognosemodelle

Generative KI (Gen AI)

Ein Katergorie von KI, welche **neue Inhalte zu erzeugen**. Diese Inhalte können z. B. **Texte, Bilder, Audio, Videos, Softwarecode** oder sogar **Designs** sein.

Bsp: ChatGPT, GitHub

KI-Agent

Ein spezialisierter Anwendungsbereich von KI-Technologie, der **aktiv handelt**, um autonom Aufgaben zu erledigen und Ziele zu erreichen.

Bsp: Prozessautomatisierung

KI Agent – Anwendung

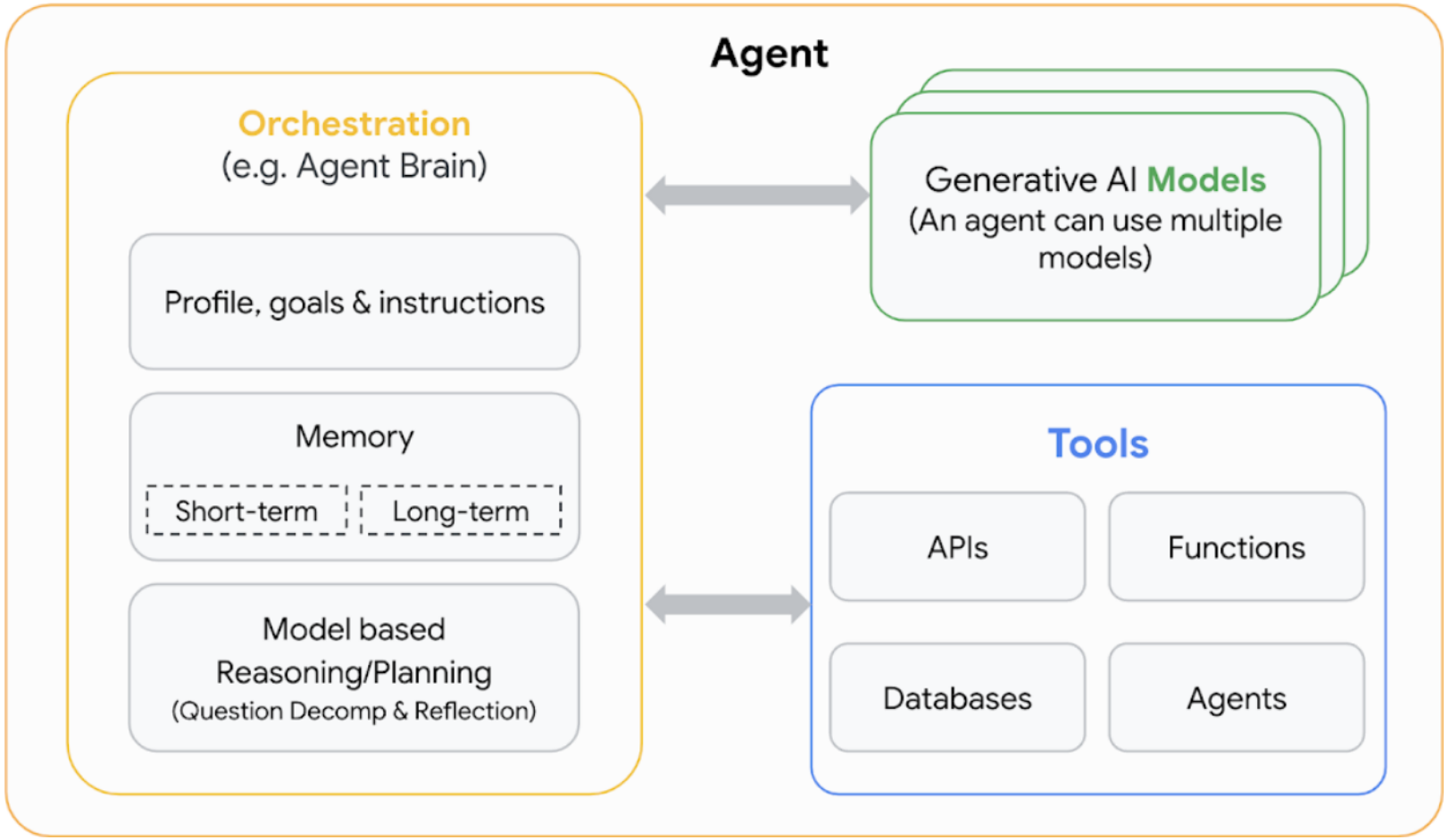


*Abbildung: KI-Agent-Anwendung**

Quelle*:
https://cloud.google.com/vertex-ai/docs/ai-agent-ecosystem-overview?hl=de

Anwendung: Schichtplanung

Herausforderung

- Produktionsbedarf erfüllen
- Maschinenlaufzeiten optimal nutzen
- Einhaltung gesetzliche Vorgaben (z. B. Ruhezeiten, Feiertage)
- Flexible und faire Einplanung Mitarbeiter
- kurzfristige Ausfälle (z. B. Krankheit) ausgleichen durch Nachbesetzung

Mögliche Outputs

- Schichtplan
- Fehlerbericht
- Vorschlag Fehlerbehebung
- Emailbenachrichtigung an Mitarbeiter
- Anpassung des Schichtplans bei Bedarf

Anwendung: Schichtplanung

Schichtplanung als Beispiel für ein Netzwerk von KI-Agenten?

Mitarbeiter-Agent: Verfügbarkeiten, Qualifikationen und Präferenzen
Schichtplanungs-Agent: Erstellt Dienstpläne basierend auf Produktionsbedarf und gesetzlichen Vorgaben (Arbeitszeiten, etc).
Notfall-Agent: Reagiert auf kurzfristige Änderungen wie Krankmeldungen oder Maschinenausfälle.
Fehler-Agent: Erstellt Berichte über Machinen- oder Produktionsausfälle
Fehlerbehebungs-Agent: Erstellt Vorschläge bei Maschinenausfällen oder Produktionsfehler
Optimierungs-Agent: Verfeinert Schichtpläne mit zusätzlichen Parameter, z.B. Kosten

KI-Vertragsthemen

#DigitUp 2025

Roland Mathys

Schellenberg Wittmer AG

Warum ist es wichtig?

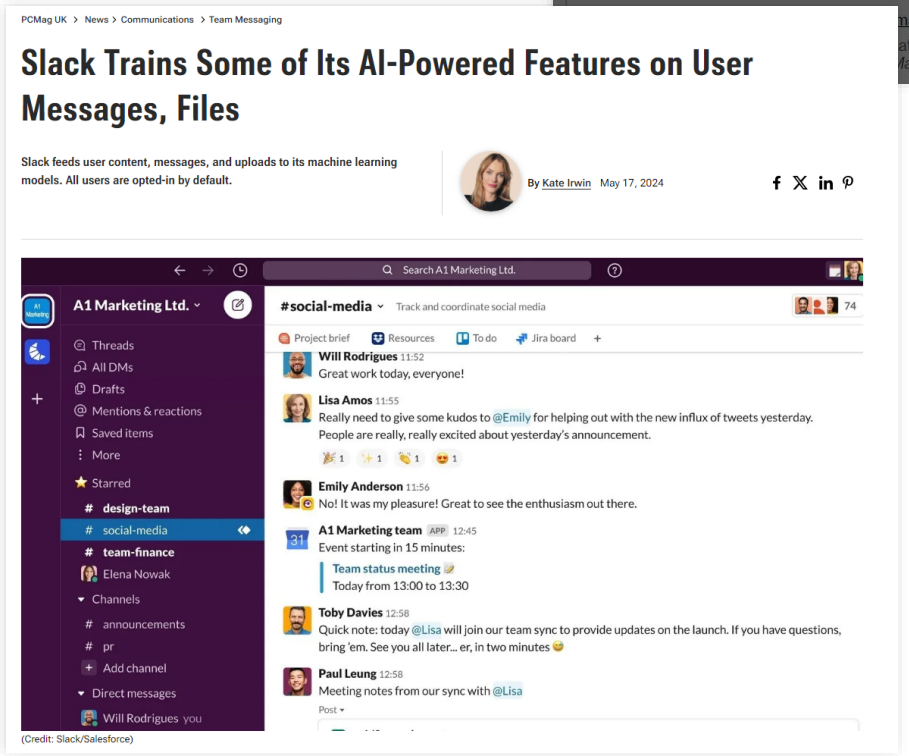
- Bislang vor allem andere Themen als Verträge im Vordergrund
- z.B. Datenschutz, IP Rechte, Haftung, …
- Bedeutung vertraglicher Themen jedoch zentral
  - Gestaltungsspielraum grösser
  - Korrektur/Anpassung gesetzlicher Regelungen
- Regelungen seitens Anbieter oft umfassend und komplex
  - Mehrstufige Vertragskonstrukte
  - Häufige Verweise auf (jederzeit änderbare) Online Terms
- Vertragliche Regelungen variieren je nach zugrundeliegendem Nutzungsmodell

Checkliste Vertragspunkte

- Freiwilligkeit der KI Nutzung
- Transparenz über den Einsatz von KI
- Sicherstellung der Kontinuität der verwendeten Modelle
- **Nutzung von Input (z.B. vertrauliche Informationen)**
- Rechte am Output (soweit Rechte bestehen)
- Einhaltung von Gesetzen
- Nachhaltigkeit / “Responsible AI” / AI Code of Conduct
- Haftung
- Aufbewahrung / Löschung

Vertraulichkeit als Beispiel

- Vertrauliche Informationen als Input
- Schutz gegen Veröffentlichung / Verwertung
- Ansätze
  - Anonymisierung?
  - Einstellungen in KI-Tools?
  - Governance (z.B. KI-Policy)
  - **Vertragliche Regelung!**



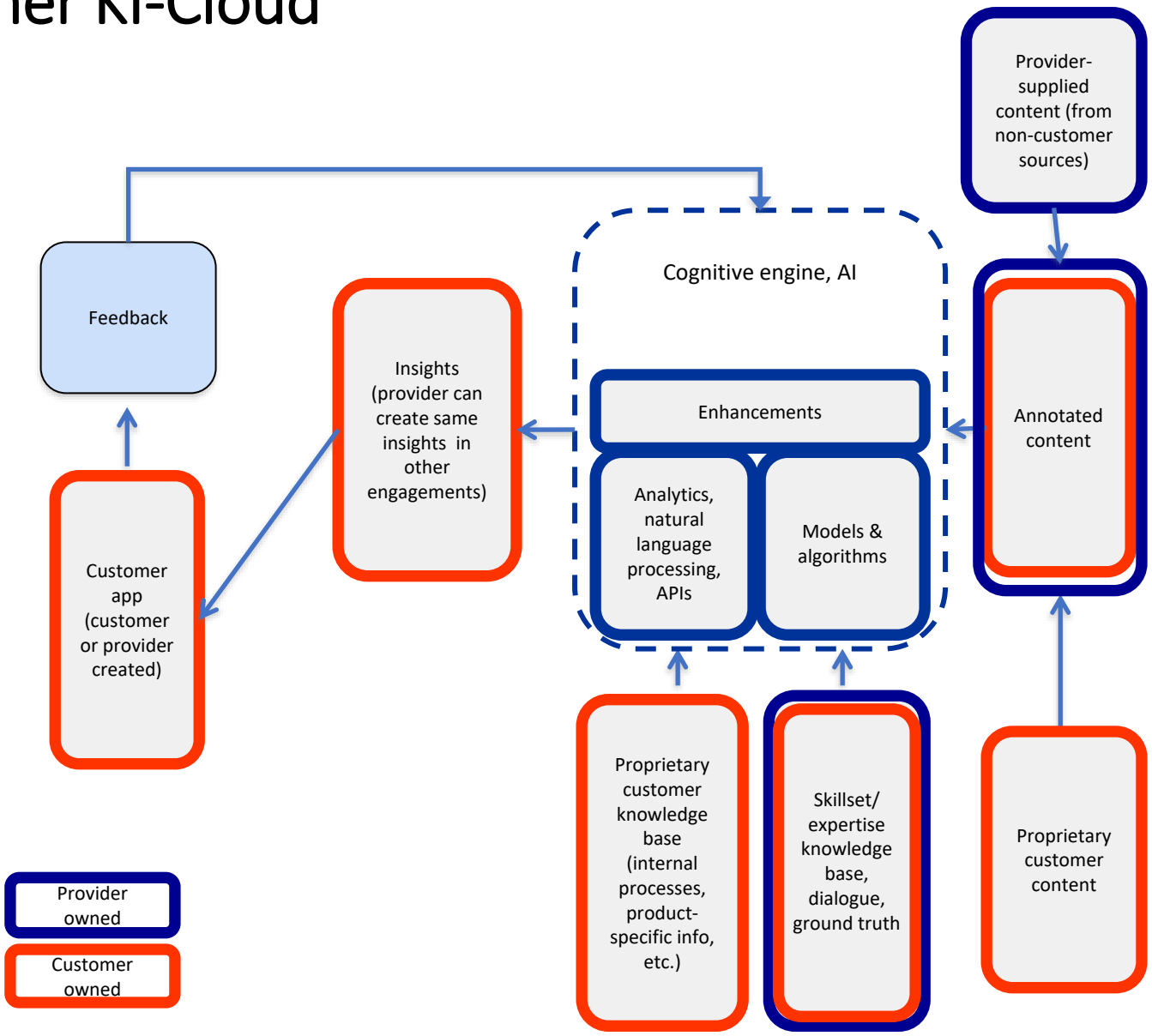
(Credit: Slack/Salesforce)

KI & Geistiges Eigentum

#DIGITUP 2025!, Zürich, 13. Mai 2025

Alesch Staehelin, Rechtsanwalt in Zürich

Der Blick auf die IP-Praxis: Eigentum & Nutzung von IP in einer KI-Cloud



Gedanken zum Urheberrecht

- Viele nationale Urheberrechtsgesetze gewähren Urheberrechtsschutz nur für Werke, die von Menschen geschaffen wurden.
- Bei computergenerierten Werken hingegen gilt in bestimmten Urheberrechtsgesetzen (z.B. in UK) die "Person, die die für die Schaffung des Werks erforderlichen Vorkehrungen getroffen hat", als Urheber, der den Urheberrechtsschutz für das computergenerierte Werk geniesst.
- Andere Rechtsordnungen (insbesondere Irland, Neuseeland, Hongkong und Indien) bieten ähnliche Lösungen an.
- Dies könnte bedeuten, dass die Person, die den Computer substantiell bedient bzw. anleitet, als Urheber des computergenerierten Werks gilt.
- Dies wäre m.E. der richtige Weg, um das Problem zu lösen und sicherzustellen, dass computergenerierte Werke urheberrechtlichen Schutz geniessen.

Gedanken zum Patentrecht

- Überwiegend können nur Menschen Erfinder im Sinn des Patentrechts sein, und nur eine Person hat das Recht, ein Patent anzumelden.
- Unter welchen Bedingungen sollen Menschen, die mit kognitiven Systemen interagieren, als Erfinder technischer Lehren angesehen werden können, die mit Hilfe kognitiver Systeme geschaffen wurden?
  - Ist es evtl. für die Einstufung als Erfinder nicht erforderlich, dass der Mensch eine technische Lehre "schafft"?
  - Könnte es, um als (Mit-)Erfinder zu gelten, evtl. ausreichen, im Output von KI eine technische Lehre zu "erkennen", die ein technisches Problem löst?
- Bei diesem Ansatz könnte ein kognitives System als (wissenschaftliches) Werkzeug betrachtet werden, das einen bestimmten Output liefert – wie jedes andere Werkzeug, das einem Erfinder hilft, zu einer Erfindung zu gelangen.
- Der Mensch, der eine technische Lehre in einem solchen Output erkennt, würde diesfalls als Erfinder einer solchen Erfindung gelten.

IP Ownership & Licensing in AI deals

Questions and things to consider:

Who owns rights in data generated by AI devices?

Be mindful of obtainable IP rights: Who claims IPRs in the data?

Ownership rights in the information derived from the data?

Do you reserve the right to transfer the data?

Multi-jurisdictional contracts necessitate cross-border expertise: Have you evaluated your contract/notice under the laws of all countries in which you do business?

- **Can an AI system create a copyrightable work, is device data copyrightable?**
- **Inventions/Patents?**
- **Other IP, otherwise protectable?**

Contracts should be clear, especially on issues of ownership, right to use and other aspects of managing data, metadata and what can be learned from data and metadata

IP ownership & licensing

AI provider

- owns all IP to Watson Core.
- owns all IP to cloud infrastructure.
- owns all future enhancements to the Watson Core and its cloud infrastructure.
- needs full freedom of action for future Watson engagements.
- will not use customer's exclusive content or customer's IP for any other purpose without customer's consent.

Customer

- will own the copyright in any deliverables (usually documents) subject to IBM ownership of embedded IBM pre-existing materials (document templates).
- will have a perpetual license to the embedded pre-existing templates.
- will retain "ownership" of the content it provides.
- will own its pre-existing IP (and any derivatives) and its proprietary information.

Typical IP discussions in an AI deal

- **AI provider must maintain full ownership and control over the AI platform.** To give ownership or control of any part to a customer would result in multiple versions of the AI ("forking" the platform), which cannot be sustained.

- **AI provider will not re-use a customer's private data** used to train or operate a specific instance of AI (without permission) and, if an instance has been specifically trained for a customer on the customer's private data, AI provider will not re-use that instance if it relies on the customer's private data**.** However, **AI provider must remain free to deploy AI with its other customers**, who may be able to develop similar or identical insights using different data, including their own private data.

- AI is delivered under **AI provider**'s standard cloud terms – with predefined operational and security terms and must be on **AI provider's** standard terms.

- Understand **AI provider**'s investment in AI & what AI is; **AI provider** must retain freedom of action to ensure repeatability of offerings.

- Articulate how the customer will access AI.

- **Customer "owns" its data (content) and copyright in insights developed from cognitive analysis of customer data; AI provider owns AI and enhancements to the platform.**

Danke

staehelin@utolegal.ch

Haftung

Sven Kohlmeier

Rechtsanwalt, Fachanwalt für IT-Recht (D)

Wicki Partners AG, Zürich

Haftung des Nutzers?

- Mangels Rechtspersönlichkeit keine Haftung des LLM oder KI-Agenten für das Ergebnis !
- Nutzer bleibt verantwortlich – arbeitsrechtlich (z.B. Arbeitsergebnis) aber auch ggf. vertraglich gegenüber Dritten (z.B. Schlechtleistung)
- Wer keine höchstpersönliche Leistung schuldet, kann sich auch eines Computers, KI oder KI-Agenten zur Unterstützung bedienen (BGer 4A_305/2021 keine unzulässige Substituierung»)
- → Interne Mitarbeiter-Guidelines erstellen

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Einkauf von KI-Agenten

- Vertrag Auftraggeber/Auftragnehmer z.B. Entwickler
- Aus Sicht Auftraggeber: Leistungsgegenstand definieren, ggf. auch Erwartung an Leistung KI-Agent
- Je nach Vertragsgegenstand: Werkvertrag oder Dienstvertrag
- Zivilrechtliche Haftung für Schlechtleistung
- Aus Sicht Auftragnehmer: keine Haftung/Schadensersatzhaftung für Output des KI-Agenten
- → klare und eindeutige Regelung im Vertrag; ggf. Verträge auf KI anpassen

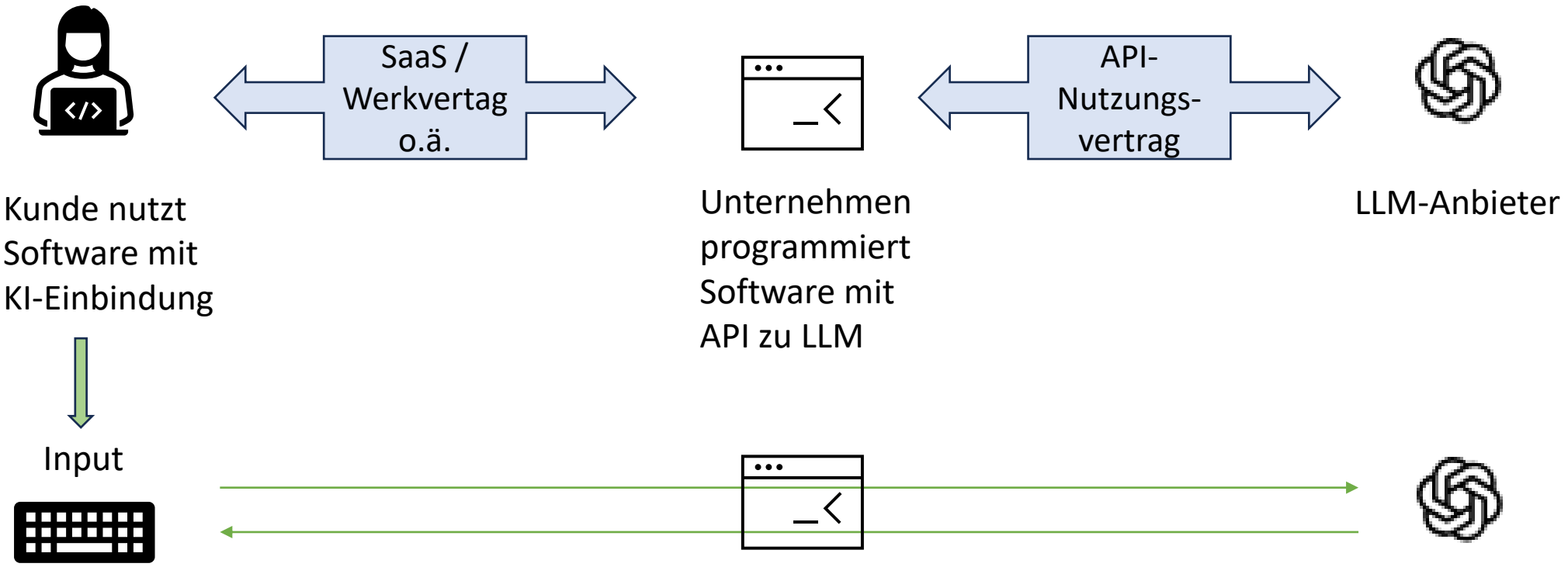
Haftung LLM-Anbieter?

- z.B. Europe Terms of Use ChatGPT
- (Stand: 29.04.2025)

Kommerzielle und geschäftliche Nutzung. Wenn Sie unsere Dienste für kommerzielle oder geschäftliche Zwecke nutzen, gelten die folgenden Bedingungen. Im Falle eines Konflikts zwischen diesem ***Addendum für die Geschäftliche Nutzung der Dienste*** und den übrigen Bedingungen hat dieses Addendum Vorrang.

Haftungsbeschränkung. WEDER WIR NOCH UNSERE VERBUNDENEN UNTERNEHMEN ODER LIZENZGEBER HAFTEN FÜR INDIREKTE, ZUFÄLLIGE, BESONDERE, FOLGE- ODER EXEMPLARISCHE SCHÄDEN, EINSCHLIESSLICH SCHÄDEN FÜR ENTGANGENEN GEWINN, FIRMENWERT, NUTZUNG ODER DATEN ODER ANDERE VERLUSTE, SELBST WENN WIR AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. UNSERE GESAMTHAFTUNG IM RAHMEN DIESER BEDINGUNGEN ÜBERSTEIGT NICHT DEN BETRAG, DEN SIE IN DEN LETZTEN 12 MONATEN VOR ENTSTEHUNG DES SCHADENS FÜR DEN DIENST, DER DEN ANSPRUCH AUSGELÖST HAT, BEZAHLT HABEN, ODER EINHUNDERT DOLLAR ($100), JE NACHDEM, WELCHER BETRAG HÖHER IST. DIE BESCHRÄNKUNGEN IN DIESEM ABSCHNITT GELTEN NUR IN DEM UMFANG , DER NACH GELTENDEM RECHT MAXIMAL ZULÄSSIG IST.

Haftung LLM-Anbieter?



Take Away und TBD

- Für KI generierte Inhalte und Ausgaben sowie deren Verwendung haftet der Verwender
- Keine Haftung der «KI», da keine Rechtspersönlichkeit und auch kein Erfüllungsgehilfe
- Haftung des Herstellers nur, wenn gesondert vereinbart – in der Regel haben Hersteller Haftungsausschlüsse
- Wohl keine Haftung nach ProdHaftG, da keine bewegliche Sache

Take Away: Verträge/AGB der Hersteller prüfen

EU-KI-Produkthaftungsrichtlinie? Von der EU-Kommission 2025 kassiert

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability)	No foreseeable agreement - the Commission will assess whether another proposal should be tabled or another type of approach should be chosen.

KI-Agenten & Regulierung

Carmen De la Cruz

Head of Legal VESIA & VE CEE ICT, Axians Schweiz AG

DigitUP 13. Mai 2025 – Zürich

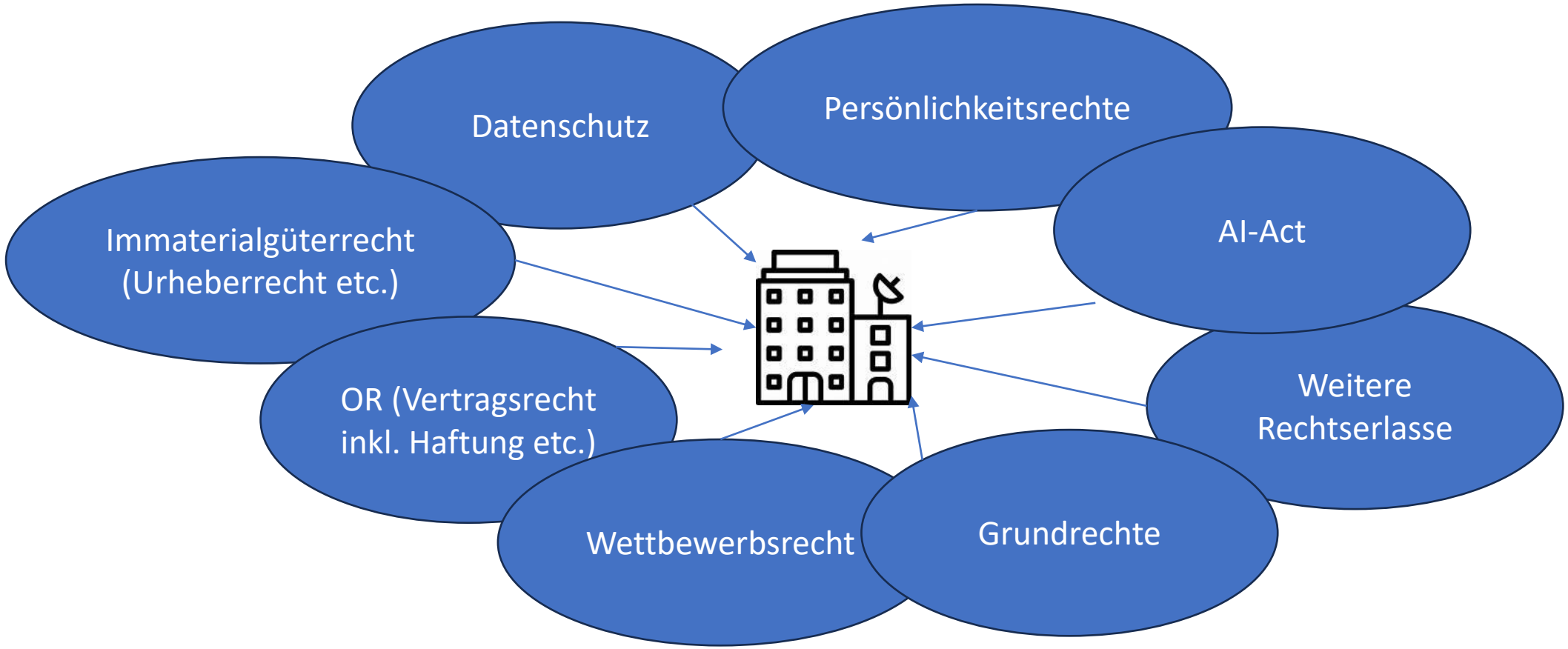
KI-Agent – die neue KI-Blackbox?

Bild: MASH

KI-Regulierung: Geheime Agenten in der Blackbox

Quelle: https://www.heise.de/select/ct/2024/23/2330613220781107871, besucht am 12.5.25

KI-Agenten & Regulierung



KI Agent – AI Act

KI-Agenten - Regulatorisches

- AI-Act auch für KI-Agenten anwendbar (sofern vom Anwendungsbereich umfasst)
- Weitere regulatorische Vorgaben hängen vom Einzelfall ab
- Sobald auf externe Datenquellen zugegriffen wird, erhöht sich das Risiko
- Datenschutz % Immaterialgüterrecht prüfen

FAQ zu KI-Agenten

Panel-Diskussion der Rechtskommission von SwissICT – moderiert von
Dr. Sandra Marmy, Schiffbau Rechtsanwälte, Zürich

DigitUP 13. Mai 2025 – Zürich

Quellen

- https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz
- https://www.accenture.com/de-de/insights/technology/technology-trends-2025
- https://www.gartner.de/de/artikel/intelligenter-ki-agent
- https://www.ibm.com/think/topics/ai-agents
- https://shyftplan.com/schichtplanung