Haftungsrechtliche Fragen der KI

16. Tagung für Informatik und Recht

Zwischen Innovation und Sicherheit – Digitales Arbeiten im Rechtswesen des 21. Jahrhunderts

Luca Dal Molin und Philippe Baumann, Homburger AG

29. August 2023

Homburger

1. Allgemeines zu den haftungsrechtlichen Risiken bei der Nutzung von KI-Tools
2. Szenarien aus der praktischen Anwendung
   - Szenario 1 – «Teilen von Daten»
   - Szenario 2 – «Verwertung geteilter Daten»
   - Szenario 3 – «Erfundene Schlussfolgerungen»
   - Szenario 4 – «Vorurteile»
   - Szenario 5 – «Fehlende Rechte»
3. Key Takeaways

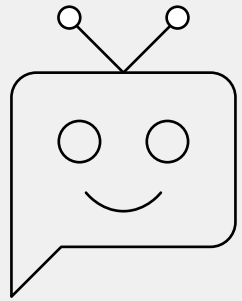
1. Allgemeines zu den haftungsrechtlichen Risiken bei der Nutzung von KI-Tools

Homburger

29. August 2023

Künstliche Intelligenz kennt heute viele mögliche Anwendungen

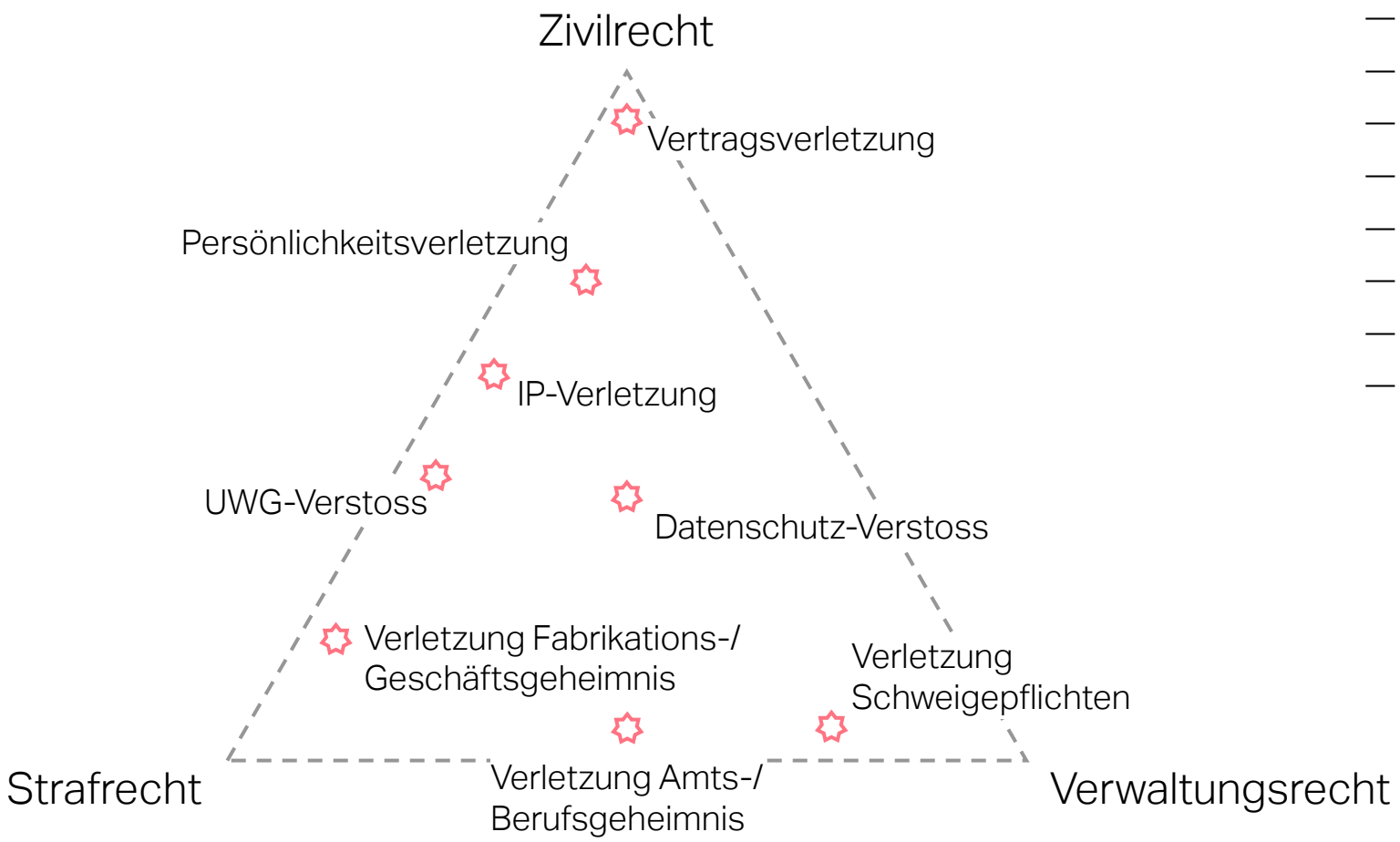
— Bild- und Spracherkennung
— Textverarbeitung und –übersetzung
— Empfehlungssysteme
— Medizinische Diagnostik
— Robotik
— Betrugsprävention im Finanzsystem
— Selbstfahrende Autos
— etc.



KI-Chatbots als Illustration

Erfahrungen aus unserer Beratungspraxis

Grundlagen

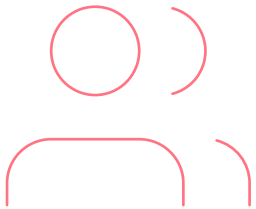


Rechtsfolgen

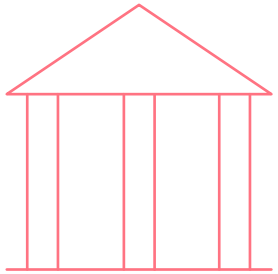
- Schadenersatz (Nachweis evtl. schwierig)
- Unterlassung / Beseitigung
- Gewinnabschöpfung
- Urteilspublikation
- Administrativsanktionen
- Bewilligungsentzug
- Bussen
- etc.

Erika und Max werden beauftragt, für ein **Unternehmen** eine **Geschäftsanalyse** zu erstellen und dazu einen Bericht zu verfassen. Das Unternehmen stellt ihnen dazu diverse interne Unterlagen zur Verfügung.

Erika und Max

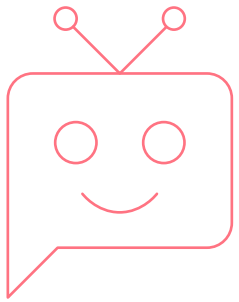


Unternehmen



Da die Unterlagen sehr umfangreich sind und Erika und Max nur wenig Zeit haben, möchten sie **«Work.AI»**, einen neuen **Chatbot basierend auf künstlicher Intelligenz**, nutzen.
Work.AI wird von einem US-amerikanischen Anbieter entwickelt und in der Cloud betrieben.

Work.AI



2. Szenarien aus der praktischen Anwendung

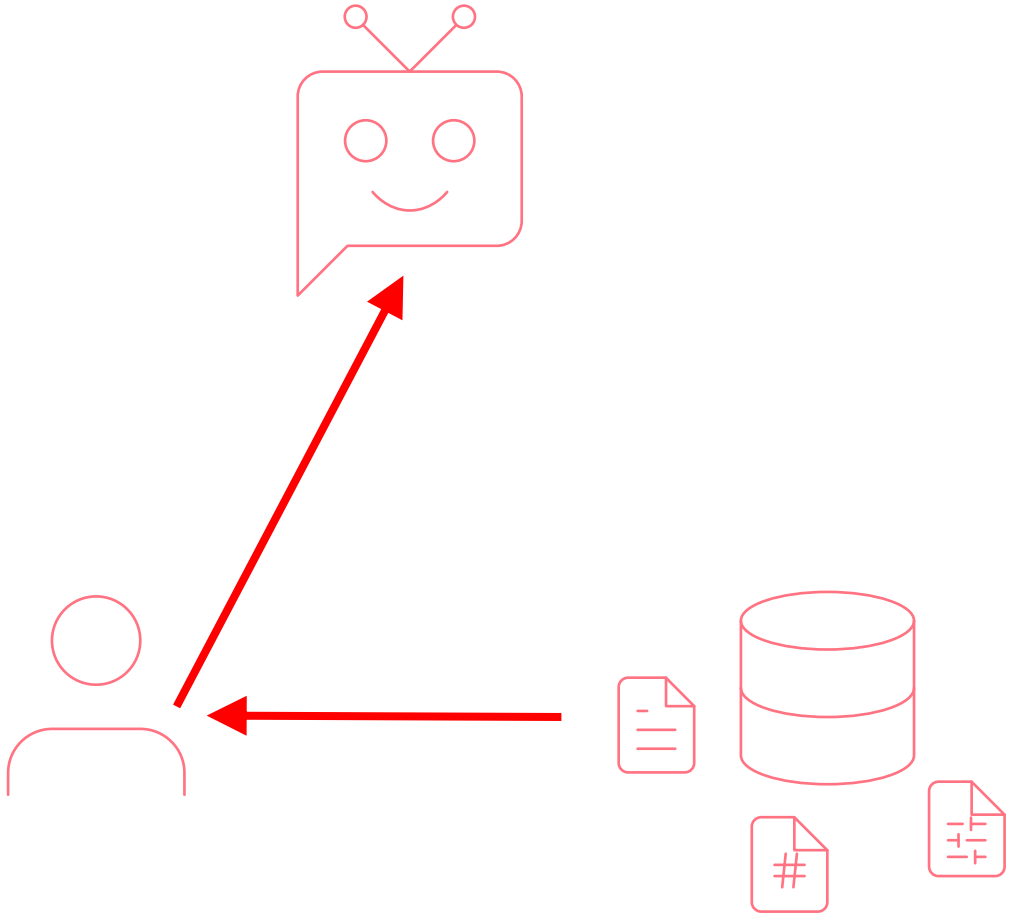
Homburger

Szenario 1 – «Teilen von Daten»

Homburger

Unter den Unterlagen für die Analyse finden sich unter anderem **Geschäftszahlen**, **Businesspläne**, **Kundeninformationen**, **Korrespondenz** und **Verträge**.

Als erstes kopiert Erika die wichtigsten Unterlagen vom Server des Unternehmens in das Analyse-Tool von Work.AI und bittet Work.AI, eine Zusammenfassung der enthaltenen Informationen zu erstellen.



Schon das Teilen von Informationen mit einem KI-Tool kann diverse Geheimhaltungspflichten verletzen und damit eine Haftung begründen. Zudem bestehen datenschutzrechtliche Risiken.

Die **AGB** von öffentlich verfügbaren KI-Tools sehen zum Teil vor, dass die Input-Informationen nicht geheim gehalten werden müssen, sondern eingesehen und **zur Verbesserung des Tools** verwendet werden können. Zudem führt das Teilen von Daten mit einem KI-Tool mitunter zur Bekanntgabe von Personendaten an den Anbieter.

Dies kann vertragliche und gesetzliche **Geheimhaltungspflichten verletzen** und zu Haftungsrisiken sowie zu Datenschutzverletzungen führen. Beim Teilen von Informationen mit KI-Tools ist deshalb Vorsicht geboten.

Potenziell einschlägige vertragliche Pflichten

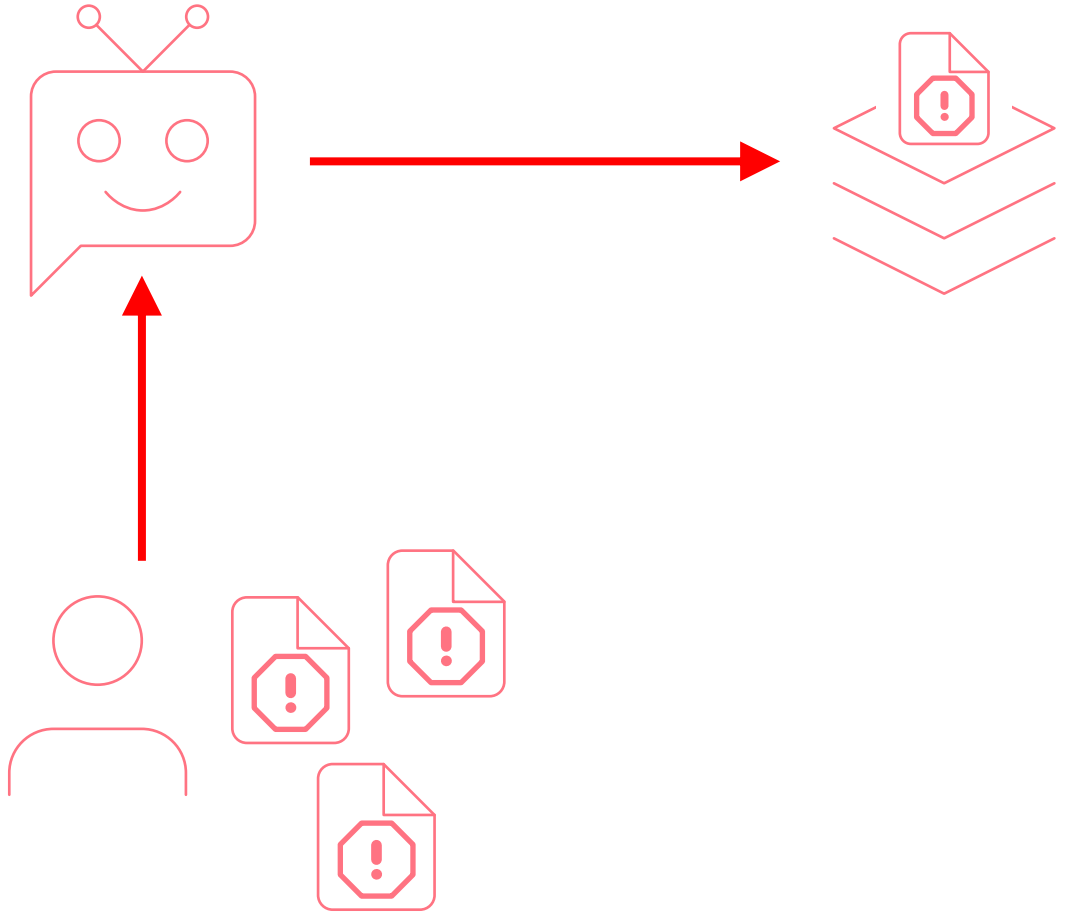
— Vertraulichkeitsvereinbarungen (NDAs)
— Vertraulichkeitsklauseln in Verträgen mit Lieferanten und Kunden
— Vertragliche Verwendungsverbote von Daten und Informationen
— Auftragsdatenverarbeitungsvereinbarungen
— Arbeitsverträge (durch die Arbeitnehmenden)

Potenziell einschlägige gesetzliche Pflichten

— Amtsgeheimnis
— Berufsgeheimnis
— Fabrikations- und Geschäftsgeheimnis
— Datenschutz
— Schweigepflichten im Gesundheits- und Sozialwesen
— etc.

Szenario 2 – «Verwertung geteilter Daten»

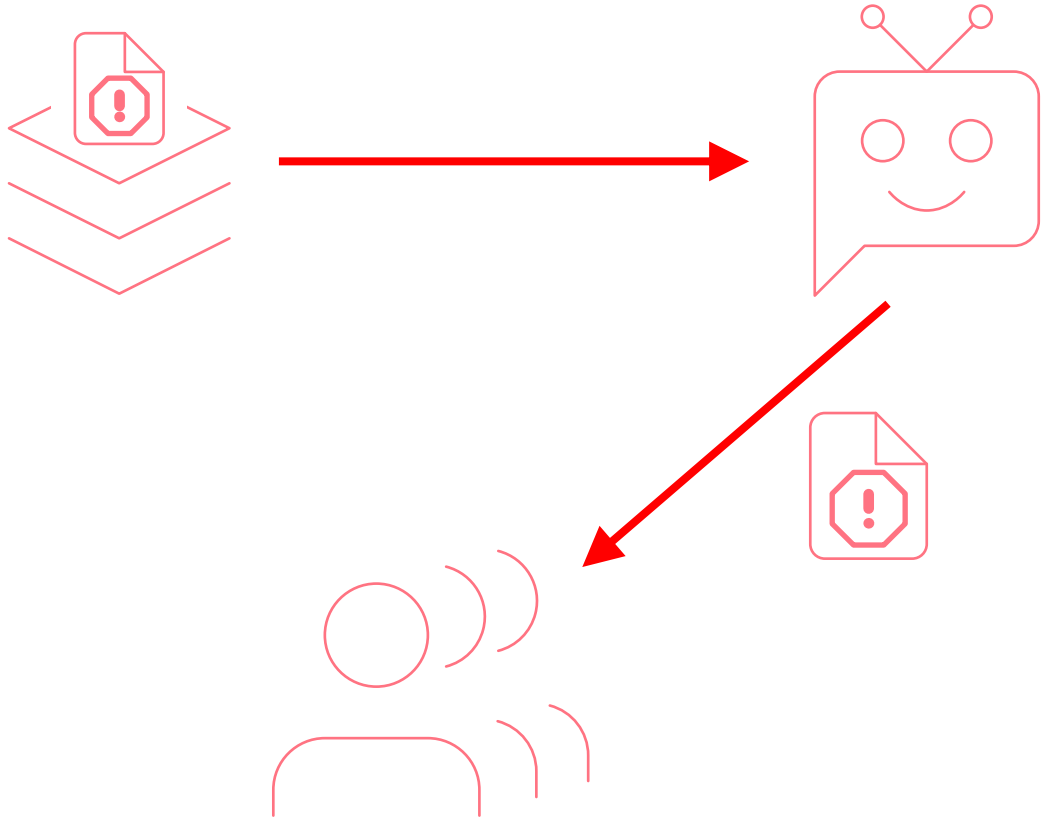
Ebenfalls unter den Unterlagen finden sich die **Sitzungsprotokolle** einer internen Arbeitsgruppe. In diesen Protokollen äussern sich Mitarbeitende mehrfach **grob herablassend** über spezifische Produkte eines Konkurrenten.



Max lädt diese Protokolle in das Analyse-Tool von Work.AI zum Abgleich mit dem Stand der Entwicklung.

Was Max nicht weiss: Work.AI benutzt diesen **Input als Trainingsdaten** zur Verbesserung des zugrundeliegenden Modells.

In der Zukunft **wiederholt Work.AI die Kommentare** über die Produkte des Konkurrenten, wenn **andere Nutzer** von Work.AI Anfragen zu diesen Produkten machen.



Nach der Herkunft dieser negativen Kommentare gefragt, nennt Work.AI die **Namen der Mitarbeitenden des Unternehmens**, welche gemäss den Protokollen an den Sitzungen teilgenommen hatten.

Mit KI-Tools geteilte Informationen können Eingang in das Modell finden und später anderen Nutzern gegenüber offengelegt werden.

KI-Tools können die von Nutzern geteilten Informationen als Input zur weiteren Verbesserung des Modells verwenden (sog. **Trainingsdaten**). Durch diese Art der Einspeisung von Informationen in ein KI-Tool kann eine **praktisch nicht mehr kontrollierbare Veröffentlichung** dieser Informationen stattfinden.

Die Informationen können sodann ganz oder teilweise oder **in sachfremden Kontexten** anderen Nutzern gegenüber preisgegeben werden.

Dies eröffnet ein ganzes Spektrum von Haftungsrisiken wie z.B.:

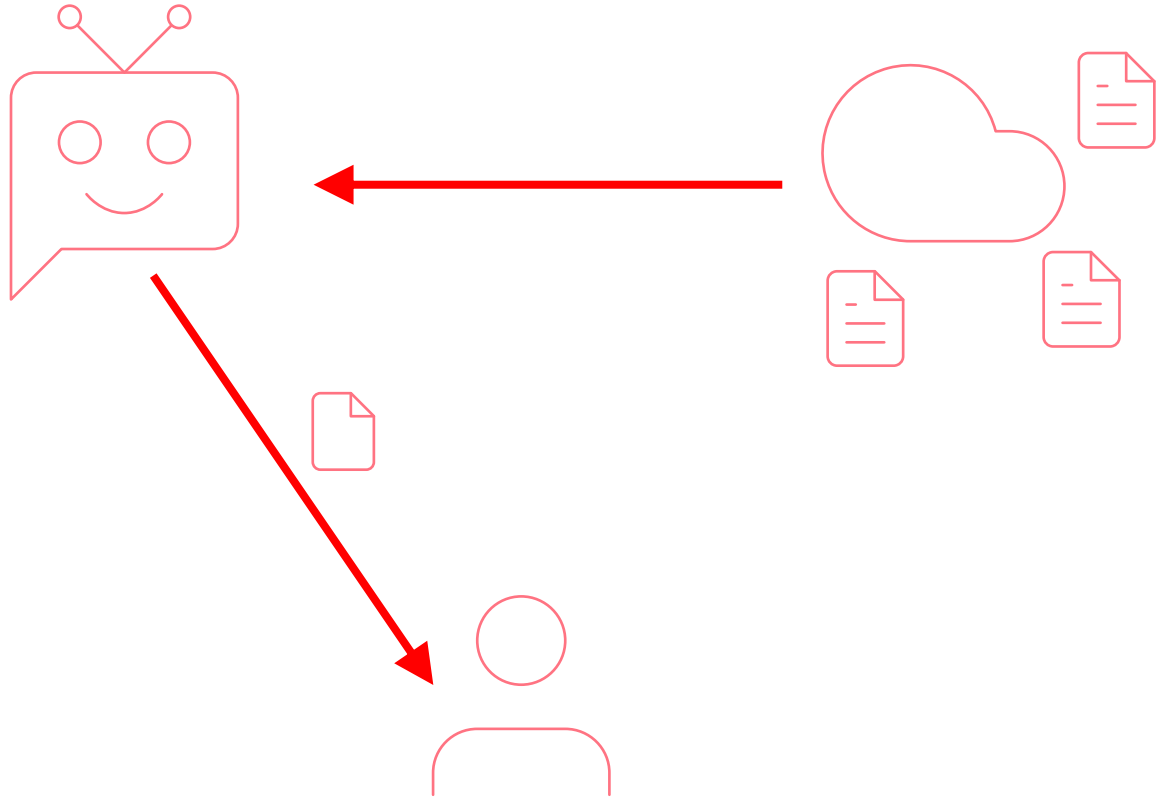
— Unlauter Wettbewerb
— Persönlichkeitsverletzungen und Ehrverletzungsdelikte
— Verletzungen des Datenschutzes
— Urheberrechtsverletzungen
— Verletzung vertraglicher Pflichten

Informationen, die einmal Eingang in das Modell eines KI-Tools gefunden haben, sind selbst für den Betreiber des Tools nur schwer zu entfernen bzw. herauszufiltern. Für einen Nutzer allein ist dies unmöglich.

Szenario 3 – «Erfundene Schlussfolgerungen»

Homburger

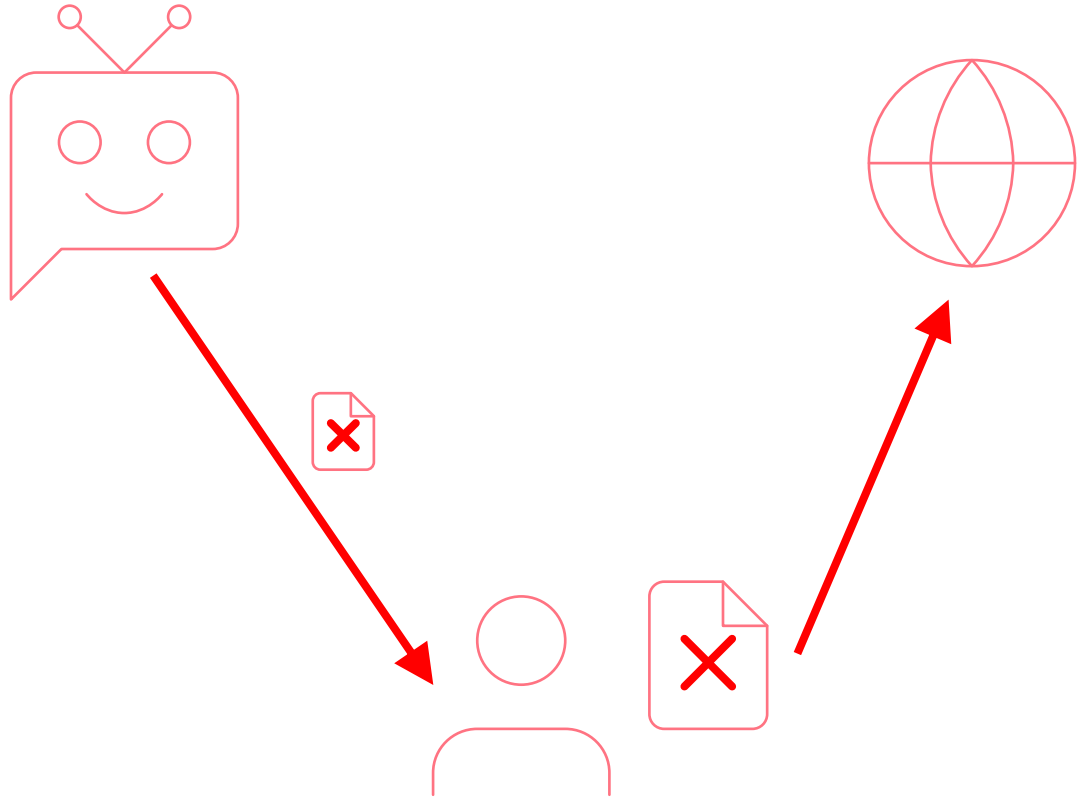
Als nächstes möchte Max einen Vergleich anstellen: Er bittet Work.AI, die Produkte des Unternehmens mit öffentlichen Informationen zu Konkurrenten und ihren Produkten zu vergleichen.



Work.AI berichtet, dass die Konkurrenten alle **auf veraltete Technologie setzen**.
Ausserdem sei die Reputation des wichtigsten Konkurrenten angeschlagen, da der **CEO wegen Betrugs verurteilt** worden war.

Max kopiert diese Aussagen in seinen Bericht.

Später werden die Aussagen zu den Konkurrenten aus dem Bericht von einer Mitarbeiterin des Unternehmens **in einem Interview wiederholt**.



Aber: Die **Aussagen sind von Work.AI frei erfunden und falsch**. Die Konkurrenten setzen auf dieselbe Technologie wie das Unternehmen. Und der CEO wurde nie des Betrugs verurteilt oder auch nur beschuldigt – der Betrüger war jemand mit demselben Familiennamen wie der CEO.

Von KI-Tools generierte Informationen können inhaltlich falsch sein, selbst wenn sie plausibel wirken.

Das direkte oder indirekte Veröffentlichen solcher Informationen kann eine Haftung auslösen.

Stand heute haben KI-Tools kein eigentliches inhaltliches Verständnis der verarbeiteten Informationen, sondern generieren Antworten auf der Basis statistischer Wahrscheinlichkeiten.

KI-basierte Chatbots können «**halluzinieren**», das heisst inhaltlich falsche oder unsinnige Aussagen machen. Solche Aussagen können auf den ersten Blick jedoch plausibel wirken. Auf die Richtigkeit der von KI-Tools generierten Informationen **darf man sich deshalb nicht verlassen**.

Wer ohne unabhängige Überprüfung Informationen von KI-Tools verwendet und wiedergibt, kann sich für die **Aussagen des KI-Tools haftbar machen**.

Da diese Probleme bekannt sind, wird ohne Überprüfung der von KI-Tools generierten Informationen wohl auch eine allfällige Sorgfaltspflicht verletzt sein.

Beispiele sind:

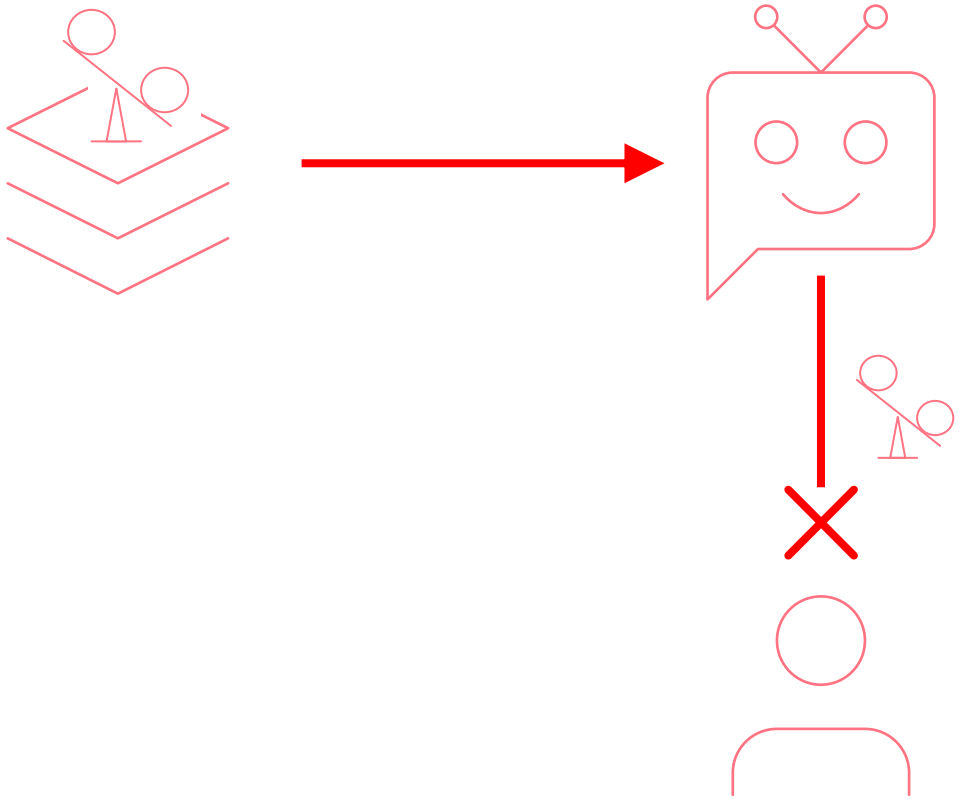
— Unlauterer Wettbewerb (Irreführung, Superlativwerbung)
— Persönlichkeitsverletzungen
— Ehrverletzungsdelikte (üble Nachrede)

Szenario 4 – «Vorurteile»

Homburger

Noch während ihres Projekts wird Erika **gekündigt**. Auf Nachfrage erklärt eine Mitarbeiterin des HR, man setze Work.AI nun auch ein, um HR-Prozesse abzuwickeln und die Produktivität im Unternehmen zu steigern.

Work.AI habe sie als Mitglied einer statistischen Gruppe identifiziert, die über eine **tiefere Produktivität** verfüge als andere Gruppen. Aus diesem Grund sei **automatisch eine Kündigung** ausgesprochen worden und könne auch nicht mehr rückgängig gemacht werden.



KI-Tools können die in historischen Daten verbreiteten Vorurteile wiedergeben.

Das Verwenden solcher Vorurteile kann zu Diskriminierung führen und so Haftungsrisiken begründen.

Die Modelle von KI-Tools sind nur so gut wie die ihnen zugrundeliegenden Trainingsdaten. Vorurteile (*bias*) in den Trainingsdaten schlagen sich im Output der KI-Tools nieder, sofern die Entwickler dieser Tools nicht spezielle Vorsichtsmassnahmen oder Filter eingebaut haben.

Bei der Verwendung von KI-Tools muss deshalb ein **Bewusstsein für potenzielle Vorurteile** im Output der KI-Tools vorhanden sein und die Resultate und Empfehlungen müssen **von Menschen kritisch überprüft** werden.

Wer die von KI-Tools generierten Informationen oder Empfehlungen unkritisch verwendet, kann Menschen **diskriminieren**. Dies kann z.B. eine Haftung für den Verstoss gegen Grundrechte oder arbeitsrechtliche Pflichten auslösen.

Werden KI-Tools für **automatisierte Einzelentscheidungen nach Art. 21 DSG** eingesetzt, müssen die betroffenen Personen informiert werden und der Entscheid muss unter Umständen auf Antrag einer betroffenen Person von einem Menschen überprüft werden.

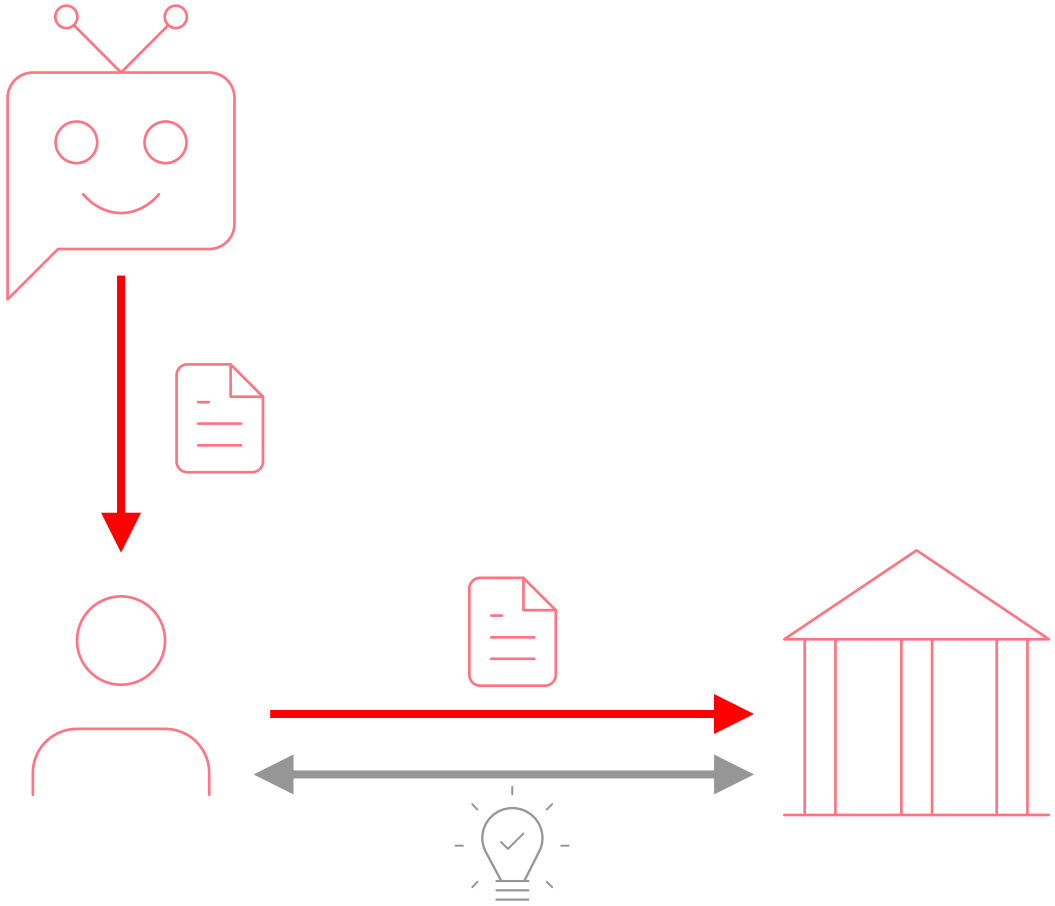
Szenario 5 – «Fehlende Rechte»

Homburger

Schliesslich lässt Max Work.AI einen **Artikel für die Website** des Unternehmens generieren und übergibt diesen an das Unternehmen.

Kurze Zeit später taucht ein **fast identischer Text** auf der Website des Konkurrenten auf.

Der **Beratervertrag** zwischen Max und dem Unternehmen sieht vor, dass das Unternehmen allein an allen Arbeitserzeugnissen berechtigt ist und Max sämtliche Rechte daran an das Unternehmen zu übertragen hat.



Von KI-Tools generierte Inhalte geniessen praktisch keinen immaterialgüter-rechtlichen Schutz.

Bei Pflichten zur Rechte-übertragung kann dies zum Problem werden.

Nach herrschender Lehre geniessen von KI-Tools generierte Inhalte grundsätzlich **keinen Schutz durch das Urheberrecht**, da es an einer geistigen (menschlichen) Schöpfung fehlt. Dieses Problem besteht auch in vielen anderen Ländern.

Ein Schutz von durch KI-Tools generierte «Erfindungen» durch das **Patentrecht ist ebenfalls ausgeschlossen**, da es an einem menschlichen Erfinder fehlt (je nach Land umstritten).

Enthalten Verträge eine **Pflicht zur Übertragung alleiniger Rechte** an den Ergebnissen der Dienstleistungen, kann die Verwendung von KI-Tools die Erfüllung dieser Pflicht effektiv verunmöglichen und so eine vertragliche Haftung auslösen.

Gerade im Zusammenhang mit Forschungs-, Entwicklungs- und Beratungsverträgen ist deshalb Vorsicht geboten beim Einsatz von KI-Tools zur Generierung von Inhalten.

3. Key Takeaways

Homburger

«Die ich rief, die Geister, werd ich nun nicht los.»
(Goethe, Der Zauberlehrling, 1797)

Beim Einsatz von KI-Tools sind wir in rechtlicher Hinsicht oft noch Zauberlehrlinge.

KI-Tools wie Chatbots können enorm nützlich sein

— KI-Tools haben das Potenzial, die Arbeit stark zu beschleunigen und repetitive Aufgaben zu minimieren

— Zur Zeit kommen fast im Monatsrhythmus neue Entwicklungen dazu

Beim Einsatz von KI-Tools wie Chatbots ist im Einzelfall Vorsicht geboten

— Im Normalfall nur solche Informationen an ein KI-Tool preisgeben, die bereits öffentlich sind oder es werden dürfen

— Output von KI-Tools nicht ungeprüft einsetzen, sondern kritisch hinterfragen

Erwägen, eine interne Richtlinie zum Einsatz von KI-Tools zu erlassen

— Ausdrücklich regeln, welche Nutzungen zulässig sind und welche nicht

— Zur Verminderung von externen Haftungsrisiken wie auch von Verantwortlichkeitsrisiken

Besten Dank für die Aufmerksamkeit!

Homburger AG
Prime Tower
Hardstrasse 201
CH-8005 Zürich

Luca Dal Molin
luca.dalmolin@homburger.ch
T +41 43 222 12 97

Philippe Baumann
philippe.baumann@homburger.ch
T +41 43 222 16 83

Luca Dal Molin ist Co-Leiter der TechGroup und der Datenschutzpraxis von Homburger und auf das Technologie-, Datenschutz- und Immaterialgüterrecht spezialisiert. Regelmässig unterstützt er Klienten bei der Einführung innovativer Technologie und der Umsetzung von Digitalisierungsstrategien.

2020	Partner bei Homburger
2015	Stanford Law School (LL.M. in Law, Science und Technology)
2011	Associate bei Homburger
2011	Anwaltspatent
2010	Rechtspraktikant am Bezirksgericht Bremgarten
2008	Praktikum bei Homburger
2008	Universität Zürich (lic. iur.)

T +41 43 222 12 97
luca.dalmolin@homburger.ch

Eingetragen im Anwaltsregister
Deutsch, Englisch, Französisch, Italienisch

Assistenz
lea.kelemen@homburger.ch

Philippe Baumann konzentriert sich auf transaktionale IP- und IT-Angelegenheiten. Er berät Klienten in den Bereichen Services (inkl. IT und Outsourcing), Lizenzierung, Forschung und Entwicklung sowie bei Akquisitionen mit Technologiebezug. In seiner Beratungspraxis kann er auf fundierte IT-Kenntnisse zurückgreifen.

2019	Associate bei Homburger
2018	Anwaltspatent
2017	Universität Zürich (MLaw)
2016	Praktikant bei Homburger
2015	Universität Hong Kong (LL.M.)
2013	Universität Zürich (BLaw)

T +41 43 222 16 83
philippe.baumann@homburger.ch

Eingetragen im Anwaltsregister
Deutsch, Englisch