smoca

Datenschutzkonformer Einsatz von KI-Modellen

Interdisziplinäre Projektarbeit
Informatikmittelschule Frauenfeld

Bundesgesetz über das Urheberrecht

Bundesgesetz gegen den unlauteren Wettbewerb

Bundesgesetz über den Datenschutz

Fach:
Wirtschaft & Recht
Abgabetermin:
23.01.2026
Verfassende Person:
Lukas Zürcher
Betreuende Lehrperson:
Roger Stöcker

Inhaltsverzeichnis

Abstract

Der rasante Anstieg generativer KI-Modelle in der Softwareentwicklung birgt grosse Effizienzpotenziale, stellt Unternehmen jedoch auch vor komplexe datenschutzrechtliche Herausforderungen. In der vorliegenden interdisziplinären Projektarbeit wird am Beispiel der Smoca AG untersucht, wie externe und interne KI-Systeme unter Einhaltung des Schweizer Datenschutzgesetzes (DSG), des Urheberrechtsgesetzes (URG) sowie des Gesetzes gegen den unlauteren Wettbewerb (UWG) eingesetzt werden können.

Zur Beantwortung dieser Frage wurden die Nutzungsbedingungen und Datenverarbeitungsprozesse führender Cloud-Anbieter (OpenAI, Google, Anthropic) analysiert und mit selbst gehosteten Open-Source-Modellen (z. B. Qwen, Ollama) verglichen. Die rechtliche Bewertung zeigte, dass die Nutzung von Consumer-Cloud-Diensten insbesondere das Risiko ungewollten Datenabflusses und der Verwendung vertraulicher Inhalte zu Trainingszwecken birgt. Eine Analyse der Unternehmensstruktur der Smoca AG ergab jedoch, dass aufgrund der technischen Kompetenz der Mitarbeitenden und der leistungsfähigen Hardware-Infrastruktur ideale Voraussetzungen für den Betrieb lokaler KI-Modelle bestehen.

Als zentrales Ergebnis wurde ein praxisnahes Klassifizierungssystem («Ampel-System») entwickelt, welches Datenkategorien definiert und diesen zulässige KI-Tools zuordnet. Die Arbeit schliesst mit der Empfehlung einer «Local-First»-Strategie: Sensible Personen- und Kundendaten sollen primär auf internen Modellen verarbeitet werden, während für unkritische Aufgaben Cloud-Dienste unter strikter Deaktivierung der Trainingsoptionen («Opt-Out») genutzt werden dürfen.

1 Einleitung[1]

1.1 Einführung in das Thema KI und Datenschutz

Mit ihrem rasanten Aufstieg hat künstliche Intelligenz einen Wandel in der Arbeitswelt ausgelöst. Bei der Textproduktion, der Auswertung komplexer Daten oder der Generierung von Programmcode bieten diese Technologien ein enormes Potenzial zur Steigerung der Effizienz. Allerdings nehmen mit der immer stärkeren Einbindung dieser Hilfsmittel in die Unternehmensroutinen auch die Sorgen um die Datensicherheit zu.

In diesem Spannungsfeld stehen der Schutz der Privatsphäre, die Wahrung von Geschäftsgeheimnissen und der Schutz des geistigen Eigentums im Mittelpunkt. KI-Modelle benötigen Daten als «Treibstoff» und es ist für Nutzer oft nicht transparent, ob die eingegebenen Informationen nur verarbeitet oder dauerhaft gespeichert werden, um zukünftige Modelle zu trainieren.

Unternehmen stehen angesichts des seit September 2023 in Kraft getretenen Schweizer Datenschutzgesetzes (DSG) sowie der Bestimmungen des Urheberrechts (URG) und des Wettbewerbsrechts (UWG) vor der Herausforderung, ihre Innovationskraft mit der Einhaltung von Vorschriften in Einklang zu bringen. Die Herausforderung besteht darin, die Vorzüge der KI auszuschöpfen, ohne dabei unabsichtlich sensible Daten offenzulegen oder gegen rechtliche Bestimmungen zu verstossen.

1.2 Bedeutung für Unternehmen wie Smoca

Dies ist für die Softwareagentur Smoca AG von hoher Relevanz. Entwickler nutzen KI-Tools zunehmend als «Co-Piloten», um Code schneller zu schreiben, Fehler zu finden oder Dokumentationen zu erstellen. Hierbei entsteht jedoch ein Risiko. Werden personenbezogene Daten, vertrauliche Projektinhalte oder geschützte Werke unbedacht an externe KI-Dienste übermittelt, kann dies als ungewollte Datenbekanntgabe oder als Verletzung von Geschäftsgeheimnissen gewertet werden. Ein Datenleck könnte nicht nur rechtliche Konsequenzen nach sich ziehen, sondern auch den Ruf der Agentur nachhaltig schädigen. Es gilt daher, einen Weg zu finden, der den technologischen Fortschritt integriert und gleichzeitig höchste Sicherheitsstandards für interne und kundenseitige Daten garantiert.

1.3 Unternehmensstruktur und technisches Umfeld der Smoca AG

Die Smoca AG ist eine Agentur für App-Entwicklung. Das Unternehmen ist mit rund 20 Mitarbeitenden überschaubar und setzt auf flache Hierarchien. Zwar leiten die vier Gründer die Firma, in den einzelnen Projekten übernehmen die Teams jedoch viel Verantwortung selbst.

[1] Für die sprachliche Überarbeitung, Strukturierung und formale Optimierung dieser Arbeit wurden verschiedene KI-basierte Hilfsmittel punktuell eingesetzt, darunter Gemini (Version 3 Pro) und DeepL Write. Die inhaltliche Erarbeitung und Analyse erfolgten hingegen vollständig eigenständig. Beispiel-Prompt: «Überarbeite Abschnitt 2.3.2 gemäss APA-Richtlinien». Verwendet am 04.12.2025.

Die 20 Mitarbeitenden entwickeln auf leistungsstarken lokalen Maschinen (Apple Silicon), was den Einsatz lokaler KI-Modelle begünstigt. Ausserdem betreibt Smoca eigene Server, auf denen interne Dienste und KI-Modelle laufen.

Das Angebot der Smoca AG ist vielfältig und reicht von mobilen Apps über Web-Plattformen bis hin zu IoT und Virtual Reality. Genauso unterschiedlich sind die Kunden: Vom Start-up bis zum Grosskonzern oder zu Behörden ist alles dabei. Diese Mischung erfordert flexible Arbeitsweisen, die aber trotzdem sicher sein müssen.

1.4 Zentrale Fragestellung und Unterfragen

Wie kann die Smoca AG externe sowie interne KI-Modelle datenschutzkonform einsetzen und sensible Informationen dabei wirksam schützen?

1.5 Zielsetzung und Methodik der Arbeit

Das Ziel dieser Arbeit besteht darin, praxisnahe und rechtlich fundierte Richtlinien für den sicheren Einsatz von KI-Systemen bei der Smoca AG zu entwickeln. Die Methodik umfasst eine Kombination aus Literatur- und Rechtsanalyse, dem Vergleich von Datenschutzrichtlinien führender KI-Anbieter sowie der Bewertung selbst gehosteter Modelle. Auf dieser Grundlage werden Handlungsempfehlungen abgeleitet, die eine datenschutzkonforme Nutzung gewährleisten.

1.6 Aufbau der Arbeit

Die Arbeit gliedert sich in drei Bereiche. Nach dieser Einleitung folgt im Hauptteil eine detaillierte Untersuchung der rechtlichen, technischen und organisatorischen Aspekte des KI-Einsatzes. Aufbauend darauf fasst der Schlussteil die gewonnenen Erkenntnisse zusammen und definiert konkrete Handlungsempfehlungen für die Smoca AG.

2 Hauptteil

2.1 Prinzipien, die immer beachtet werden müssen

Die nachfolgend aufgeführten Prinzipien stützen sich auf die allgemeinen Bearbeitungsgrundsätze des Schweizer Datenschutzgesetzes (DSG, 2025, Art. 6). Sie bilden das rechtliche Fundament für jede Datenverarbeitung sind technologieneutral und somit sind sie auch beim Einsatz von künstlicher Intelligenz zwingend einzuhalten. Werden diese Grundsätze, wie beispielsweise Verhältnismässigkeit oder Zweckbindung missachtet, ist der Einsatz von KI-Tools – unabhängig von der genutzten Software – unzulässig.

2.1.1 Transparenz gegenüber Kunden und Mitarbeitenden

Es muss jederzeit nachvollziehbar und kommunizierbar sein, ob und in welchem Umfang KI-Systeme zur Bearbeitung von Aufgaben eingesetzt werden. Das schafft Vertrauen und verhindert, dass Kunden oder Mitarbeitende unwissentlich Teil einer automatisierten Datenverarbeitung werden.

2.1.2 Datenminimierung: Nur notwendige Daten weitergeben

Es gilt der Grundsatz der Datensparsamkeit. An ein KI-System dürfen nur die Informationen übergeben werden, die zur Lösung einer spezifischen Aufgabe zwingend erforderlich sind. Um das Risiko eines ungewollten Informationsabflusses bereits an der Quelle zu minimieren, sind ganze Datensätze oder unnötige Metadaten vor der Eingabe zu entfernen.

2.1.3 Zweckbindung: Nutzung nur für klar definierte Zwecke

Daten, die für einen bestimmten Zweck – beispielsweise Support oder Fehleranalyse – erhoben wurden, dürfen nicht ohne Weiteres für andere Zwecke, etwa das Training einer KI, verwendet werden. Die Nutzung muss sich strikt im Rahmen dessen bewegen, was ursprünglich vereinbart oder vorgesehen war.

2.1.4 Schutz besonders sensibler Daten durch erhöhte Sicherheitsvorkehrungen

Besonders vertrauliche Informationen wie Gesundheitsdaten, biometrische Merkmale oder strategisch kritische Geschäftsinformationen erfordern ein erhöhtes Schutzniveau. Solche Daten sollten standardmässig nicht in offenen oder externen KI-Systemen verarbeitet werden, da das Schadenspotenzial im Falle eines Verlusts hoch ist.

2.2 Technische und organisatorische Massnahmen

Die Einhaltung der oben genannten Prinzipien erfordert nicht nur theoretische Richtlinien, sondern muss auch durch konkrete Vorkehrungen im Betriebsalltag abgesichert werden. Das Datenschutzgesetz verlangt, dass die Sicherheit der Datenverarbeitung durch technische und organisatorische Massnahmen gewährleistet wird. Technisch bedeutet dies, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten durch geeignete Systemarchitekturen und Sicherheitsstandards geschützt werden müssen. Organisatorisch muss sichergestellt werden, dass Handlungs-

anweisungen, Verantwortlichkeiten und Kontrollprozesse etabliert sind, um menschliches Fehlverhalten zu minimieren.

2.3 Schweizer rechtlicher Rahmen

Der rechtliche Rahmen für den Einsatz von KI-Systemen in der Schweiz stützt sich nicht allein auf den Datenschutz. Von zentraler Bedeutung ist das am 1. September 2023 in Kraft getretene Datenschutzgesetz (DSG), das den Schutz der Persönlichkeit regelt. Ergänzend dazu sind jedoch zwei weitere Gesetze von entscheidender Bedeutung: das Urheberrechtsgesetz (URG), das den Schutz von Software und Werken sicherstellt, sowie das Bundesgesetz gegen den unlauteren Wettbewerb (UWG), das den Schutz von Geschäftsgeheimnissen definiert.

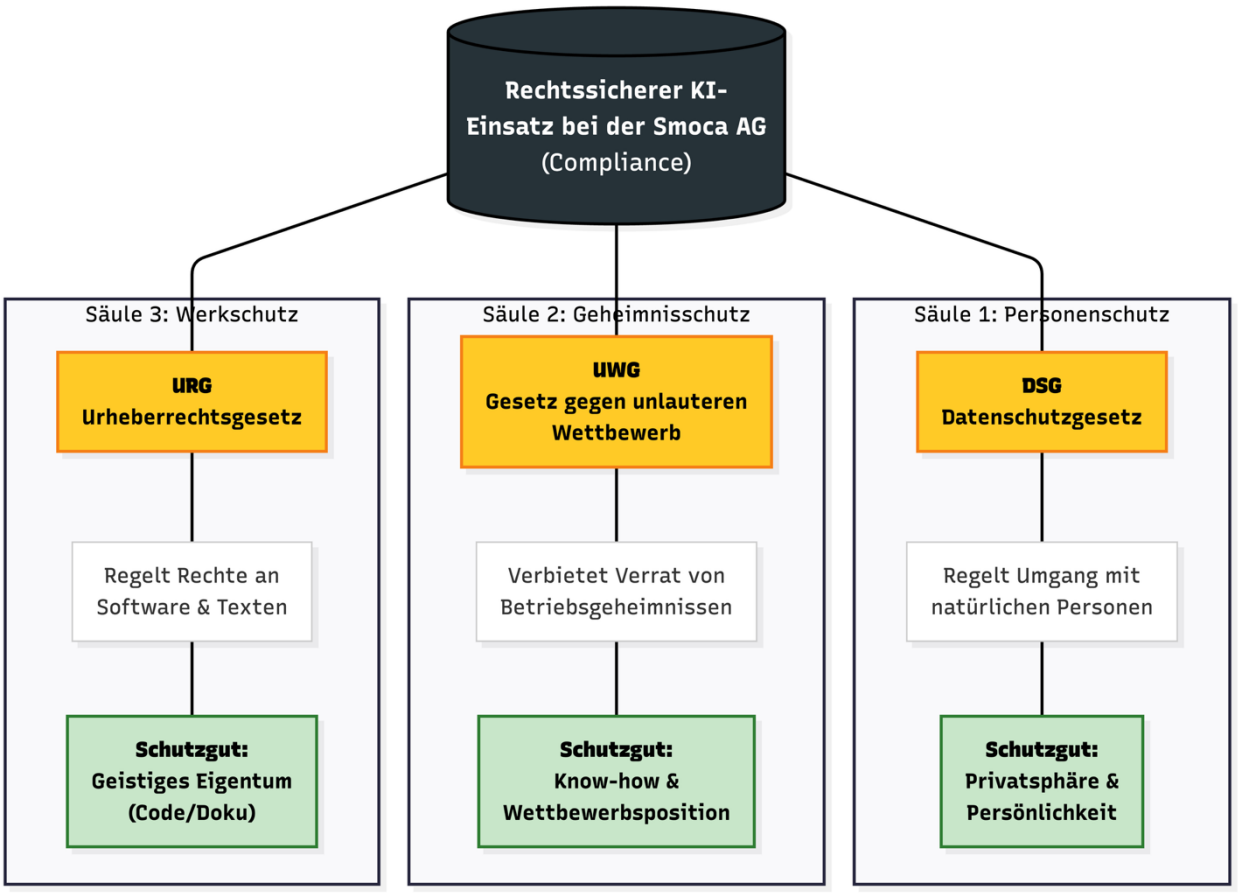


Abbildung 1: Das Drei-Säulen-Modell der rechtlichen Rahmenbedingungen für den KI-Einsatz (eigene Darstellung)

2.3.1 Überblick über das Datenschutzgesetz

Das Datenschutzgesetz bildet die Grundlage für den Schutz der Persönlichkeit und der Grundrechte natürlicher Personen, deren Daten in der Schweiz verarbeitet werden. Gemäss DSG (2025, Art. 1) sichert es die Privatsphäre und die informationelle Selbstbestimmung. Es legt fest, unter welchen Bedingungen Daten bearbeitet werden dürfen, welche Anforderungen an Unternehmen gelten und welche Rechte betroffene Personen besitzen. Es gilt für jede Bearbeitung von Personendaten durch private Unternehmen und Bundesorgane (DSG, 2025, Art. 2).

2.3.2 Begriffsbestimmungen

Die Begriffsbestimmungen des DSG (2025, Art. 5) legen fest, welche Daten dem Gesetz unterstehen.

2.3.2.1 Personendaten

Personendaten sind laut DSG (2025, Art. 5 lit. a) alle Angaben zu einer bestimmten oder bestimmbaren natürlichen Person. Dazu gehören sowohl direkte Identifikatoren wie Name und Kontaktangaben als auch indirekte wie Kundennummern oder IP-Adressen.

2.3.2.2 Besonders schützenswerte Personendaten

Hierzu zählen beispielsweise Daten zur Gesundheit, zur Intimsphäre, zur ethnischen Zugehörigkeit, zu religiösen oder politischen Ansichten sowie genetische und biometrische Daten (DSG, 2025, Art. 5 lit. c). Ihre Bearbeitung unterliegt erhöhten Sicherheitsanforderungen.

2.3.2.3 Anonymisierte Daten

Der Begriff der «Anonymisierten Daten» wird im Datenschutzgesetz nicht explizit definiert. Aus der Systematik des Gesetzes folgt jedoch, dass Daten, die nicht mehr einer bestimmten Person zugeordnet werden können, nicht als Personendaten gelten (DSG, Art. 2 Abs. 1; Art. 5 lit. a). Damit eine Anonymisierung wirksam ist, muss eine Re-Identifizierung dauerhaft ausgeschlossen sein.

2.3.3 Rechtliche Risiken der Datenweitergabe

Um die rechtlichen Risiken einer Datenweitergabe beurteilen zu können, müssen die Bestimmungen des Datenschutzgesetzes (DSG) mit den Schutzmechanismen des Urheberrechts und des Wettbewerbsrechts verknüpft werden. Die nachfolgende Tabelle 1 bietet eine Übersicht der zentralen Artikel aus allen drei Gesetzen (DSG, URG, UWG) und zeigt, welche Normen bei der Übermittlung von Daten, Werken oder Geschäftsgeheimnissen an KI-Systeme betroffen sind.

Tabelle 1: Zusammenfassung der zentralen Bestimmungen (eigene Darstellung)

Gesetz	DSG-Artikel	Inhalt/Bedeutung	Relevanz für KI-Datenweitergabe
DSG	Art. 5	Begriffsbestimmungen	Definitionen für relevante Begriffe des DSG
DSG	Art. 6	Grundsätze der Bearbeitung	Zweckbindung, Verhältnismässigkeit
DSG	Art. 8	Datensicherheit	Risiko bei Übermittlung an externe KI
DSG	Art. 16-17	Bekanntgabe ins Ausland	KI-Server ausserhalb CH/EU
DSG	Art. 19	Informationspflicht bei Beschaffung von Personendaten	relevant, wenn Betroffene bei Datenerhebung nicht über spätere KI-Verwendung informiert wurden
DSG	Art. 31	Rechtfertigung der Bearbeitung	Rechtsgrundlage oder Einwilligung für Weitergabe erforderlich
URG	Art. 2	Schutz von Werken (zum Beispiel Software, Dokumentationen)	Risiko unzulässiger Werkoffenlegung an KI

UWG	Art. 6	Schutz von Geschäfts- und Betriebsgeheimnissen	Verbot unbefugter Weitergabe vertraulicher Daten

2.3.4 Rechtfertigungsgründe und Datensicherheit

Die in Kapitel 2.1 beschriebenen Grundsätze (DSG, 2025, Art. 6) müssen stets eingehalten werden. Für die Weitergabe von Personendaten an externe KI-Systeme ist jedoch oft eine zusätzliche Rechtfertigung erforderlich. Dies ist der Fall, wenn die Bearbeitung gegen Persönlichkeitsrechte verstossen könnte. Eine solche Rechtfertigung kann durch eine explizite Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch eine gesetzliche Vorschrift erfolgen (DSG, 2025, Art. 31). Zudem verpflichtet das Gesetz Unternehmen explizit dazu, die Datensicherheit zu gewährleisten (DSG, 2025, Art. 8). Das bedeutet, dass die in Kapitel 2.2 beschriebenen technischen und organisatorischen Massnahmen nicht nur "Best Practice", sondern gesetzlich vorgeschrieben sind, um die Daten vor unbefugtem Zugriff durch Dritte oder KI-Anbieter zu schützen.

2.3.5 Umgang mit geistigem Eigentum und Geschäftsgeheimnissen

Das URG schützt Werke wie Software oder technische Dokumentationen, sofern sie eine individuelle geistige Schöpfung darstellen (URG, 2025, Art. 2). Werden sie unberechtigt an eine KI übermittelt, kann dies als unzulässiges Zugänglichmachen gegenüber Dritten gelten und somit eine Urheberrechtsverletzung darstellen.

Das UWG schützt vertrauliche Geschäfts- und Betriebsgeheimnisse. Ihre Weitergabe an Dritte ist unzulässig (UWG, 2025, Art. 6). Zu den Geschäftsgeheimnissen zählen insbesondere interne Abläufe, Kundenlisten, technische Prozesse und nicht öffentlicher Quellcode. In der Praxis wird dieser gesetzliche Schutz häufig durch privatrechtliche Geheimhaltungsvereinbarungen (Non-Disclosure Agreements, NDAs) verstärkt. Solche Verträge untersagen oft explizit jegliche Weitergabe von Informationen an Dritte, was die Nutzung cloudbasierter KI-Dienste für entsprechende Projektdaten faktisch ausschliesst.

2.4 Analyse von KI-Modellen und deren Umgang mit Daten

Um die Datensicherheit bei der Nutzung externer KI-Dienste bewerten zu können, müssen die Vertragsbedingungen und technischen Abläufe genau untersucht werden. In diesem Kapitel werden die Marktführer OpenAI, Google und Anthropic untersucht, da sie die aktuell leistungsfähigsten Modelle bereitstellen und im Unternehmensumfeld am häufigsten anzutreffen sind.

2.4.1 Überblick über aktuelle KI-Systeme

In diesem Kapitel werden die Nutzungsbedingungen der Marktführer OpenAI, Google und Anthropic analysiert. Alle drei Anbieter unterscheiden bei der Datenverarbeitung technisch und vertraglich zwischen Produkten für Endverbraucher und Unternehmenslösungen. Die Tabelle 2 fasst die wesentlichen Unterschiede bezüglich des Modelltrainings zusammen.

Tabelle 2: Umgang mit Daten für das Modelltraining nach Kundensegment (eigene Darstellung)

Anbieter	Endverbraucher	Unternehmenskunden
OpenAI	Daten werden standardmässig genutzt	Standardmässig kein Training
Google		
Anthropic	Nutzung nur nach Zustimmung	

2.4.1.1 ChatGPT – OpenAI

OpenAI stellt ChatGPT über Weboberflächen und APIs bereit. Die europäische Datenschutzerklärung beschreibt die Erhebung von Nutzerinhalten und technischen Protokolldaten (OpenAI, 2024b). Für Geschäftskunden und die API-Nutzung gelten gesonderte Vereinbarungen, die festlegen, dass Kundendaten standardmässig nicht zum Training der Modelle verwendet werden (OpenAI, 2024a).

2.4.1.2 Gemini – Google

Google stellt Gemini als App sowie in Google Workspace integriert bereit. Über die «Gemini App Aktivitäten» können Nutzende steuern, ob Chats gespeichert und zur Verbesserung der Technologien genutzt werden (Google, 2025b). Workspace-Inhalte unterliegen den dortigen Sicherheitskontrollen und werden nicht ohne Einwilligung für das Training externer Modelle genutzt (Google, o. D.).

2.4.1.3 Claude – Anthropic

Anthropic unterscheidet zwischen Konsumentenprodukten und kommerziellen Angeboten wie «Claude for Work» (Anthropic, 2025a). Bei Konsumentenkonten hängt die Nutzung für das Training von der Zustimmung der Nutzenden ab und wird standardmässig nicht verwendet (Anthropic, 2025b). Für kommerzielle Produkte wird hingegen festgelegt, dass Eingaben standardmässig nicht zum Modelltraining verwendet werden (Anthropic, 2025c).

2.4.2 Verarbeitung von Eingabedaten

Nach der Vorstellung der Anbieter untersucht der folgende Abschnitt die konkreten technischen Verarbeitungsprozesse. Für die rechtliche Bewertung ist es entscheidend, zwischen der blossen Speicherung von Chatverläufen und der tiefergehenden Nutzung der Daten zur Weiterentwicklung der Modelle zu differenzieren.

2.4.2.1 Speicherung und Weiterverarbeitung von Chats

OpenAI erhebt Inhalte und Metadaten zur Bereitstellung, Sicherheit und Missbrauchserkennung. Dabei unterliegen Unternehmensprodukte nicht denselben Regeln wie Consumer-Produkte (OpenAI, 2024b). Google speichert Eingaben der Gemini-Apps zur Produktverbesserung, während Inhalte von Workspace ausschliesslich in der Kundendomäne verarbeitet werden (Google, 2025a). Anthropic wiederum speichert Daten zur Missbrauchserkennung, löscht API-Eingaben jedoch nach kurzer Zeit und nutzt diese nicht für andere interne Zwecke (Anthropic, 2025a).

2.4.2.2 Nutzung von Daten für das Modelltraining

OpenAI und Google nutzen die Eingaben aus den Consumer-Versionen grundsätzlich zur Verbesserung der Modelle, bieten jedoch über die Einstellungen Opt-out-Möglichkeiten an (OpenAI, 2024a; Google, 2025b). Anthropic nutzt Inhalte von Konsumenten dagegen nur nach expliziter Zustimmung (Anthropic, 2025b). Unternehmens- und API-Produkte aller drei Anbieter sind vertraglich vom Training ausgeschlossen (OpenAI, 2024a; Google, o. D.; Anthropic, 2025c).

2.4.2.3 Unterschiede zwischen einzelnen Anbietern

Der wesentliche Unterschied liegt in der Standardeinstellung für Konsumenten. Während OpenAI und Google auf ein Opt-out-Verfahren setzen, erfordert Anthropic teilweise eine Zustimmung. Nur Unternehmenslösungen und API-Produkte bieten bei allen Anbietern einen garantierten Ausschluss der Trainingsnutzung und strengere Verarbeitungsregeln.

2.4.3 Risikobewertung externer Modelle

Die Analyse der Datenschutzrichtlinien und gesetzlichen Vorgaben zeigt, dass beim Einsatz externer KI-Systeme bestimmte Handlungen erhebliche datenschutz-, geheimnisschutz- und urheberrechtliche Risiken erzeugen. Tabelle 3 gibt einen Überblick über die zentralen Risikokategorien.

Tabelle 3: Überblick über rechtliche Risiken beim Einsatz externer KI-Modelle (eigene Darstellung)

Risikotyp	Auslöser	Rechtsnormen	Konsequenzen
Unzulässige Weitergabe von Personen Daten	Eingabe personenbezogener daten in externe KI (alle Versionen).	Art. 6, Art. 16–17, Art. 31	Unzulässige Datenbekanntgabe; fehlende Rechtsgrundlage.
Nutzung für Modelltraining	Eingabe personenbezogener Daten in KI-Produkte mit Trainingsnutzung (Consumer).	DSG Art. 6, 31	Zweckentfremdung; irreversible Weitergabe.
Verlust von Geschäfts- und Betriebsgeheimnissen	Eingabe vertraulicher Informationen (Code, Prozesse, Kundenlisten) in Systeme ohne vertragliche Geheimhaltung.	UWG Art. 6	Verletzung von Geschäftsgeheimnissen.
Urheberrechtsverletzungen	Übermittlung geschützter Werke an externe KI-Anbieter.	URG Art. 2	Unbefugtes Zugänglichmachen eines Werkes.

2.4.3.1 Risiken aufgrund unzulässiger Weitergabe von Personendaten

Werden personenbezogene Kundendaten in ChatGPT, Gemini oder Claude eingegeben, so werden sie zur Antwortgenerierung verarbeitet und je nach Produktversion gespeichert oder intern weiterverarbeitet. Dies kann gegen die Zweckbindung und Verhältnismässigkeit verstossen (DSG, 2025, Art. 6), insbesondere wenn keine Rechtsgrundlage besteht oder die Betroffenen nicht informiert wurden.

Auch die Übermittlung ins Ausland ist nur zulässig, wenn ein angemessenes Schutzniveau besteht (DSG, 2025, Art. 16–17).

Fehlt eine Rechtsgrundlage, stellt bereits die Eingabe personenbezogener Daten eine unzulässige Datenbekanntgabe dar, unabhängig von der verwendeten Version (Consumer, Enterprise oder API). Eine Rechtfertigung wäre nur über die Einwilligung oder andere Gründe gemäss DSG (2025, Art. 31) möglich.

2.4.3.2 Risiken durch Nutzung für Modelltraining

Während Consumerprodukte zur Modellverbesserung genutzt werden können, schliessen Unternehmens- und API-Angebote dies aus. Werden Inhalte dennoch in Systeme eingegeben, die eine Trainingsnutzung erlauben, liegt ein Verstoss gegen die Zweckbindung (DSG, 2025, Art. 6) und die Rechtfertigungspflicht (DSG, 2025, Art. 31) vor. Zudem kann eine irreversible Weitergabe entstehen, wenn die Inhalte ins Modelltraining einfliessen. Unternehmen dürfen deshalb nur Systeme nutzen, bei denen eine Trainingsnutzung ausgeschlossen oder deaktivierbar ist. Eine gültige Rechtsgrundlage ist dennoch immer erforderlich.

2.4.3.3 Risiken bezüglich Geschäfts- und Betriebsgeheimnisse

Die Weitergabe vertraulicher Informationen wie beispielsweise Quellcode, Abläufe oder Kundenlisten an externe KI-Systeme kann gemäss UWG (2025, Art. 6) eine Verletzung von Geschäftsgeheimnissen darstellen. Dies gilt insbesondere für KIs ohne vertragliche Geheimhaltungspflichten. Auch Enterprise- oder API-Versionen bleiben riskant, wenn Mitarbeitende Informationen unkontrolliert eingeben.

2.4.3.4 Risiken hinsichtlich des Urheberrechts

Das URG schützt Software, Dokumentationen und technische Zeichnungen (URG, 2025, Art. 2). Werden solche Inhalte einer KI zugänglich gemacht, kann dies eine Urheberrechtsverletzung darstellen – insbesondere, wenn die Eingebenden nicht die Rechteinhaber sind oder die Inhalte in das Modelltraining einfliessen.

2.4.3.5 Gesamtschlussfolgerung

Die Analyse zeigt, dass der Einsatz externer KI-Modelle in den Bereichen Datenschutz, Geschäftsgeheimnisse und Urheberrecht erhebliche Risiken birgt. Die Eingabe personenbezogener oder vertraulicher Informationen in ein externes KI-System gilt als Datenbekanntgabe an einen Dritten und erfordert eine Rechtsgrundlage. Fehlt diese, liegt bereits mit der Eingabe ein Verstoss vor.

Zusätzlich wird das Risiko durch Consumer-KIs erhöht, da Eingaben dort für Trainingszwecke genutzt oder gespeichert werden können. Auch bei Enterprise- oder API-Produkten bleibt die Verantwortung beim Unternehmen. Ohne klaren Zweck, Einwilligung oder gesetzliche Grundlage ist jede Weitergabe unzulässig.

2.5 Umgang mit Code und Datensätzen

In diesem Kapitel wird erörtert, welche Arten von Code, JSON-Dateien und Datensätzen an externe KI-Systeme weitergegeben werden dürfen und welche rechtlichen Grenzen dabei gelten. Grundlage hierfür sind das Datenschutzgesetz (DSG), das Urheberrechtsgesetz (URG), das

Gesetz gegen den unlauteren Wettbewerb (UWG) sowie die vertraglichen Regelungen der KI-Anbieter.

2.5.1 Zulässigkeit der Datenweitergabe

Bei der Weitergabe von Informationen an externe KI-Anbieter muss rechtlich differenziert werden, um welche Art von Daten es sich handelt. Während das DSG ausschliesslich den Schutz natürlicher Personen regelt, schützen das UWG und das URG das geistige Eigentum sowie betriebliche Werte des Unternehmens. Dabei sind drei Kategorien zu unterscheiden:

2.5.1.1 Personendaten im Quellcode

Wie in Kapitel 2.3.2.1 dargelegt, reicht bereits eine theoretische Identifizierbarkeit aus. In Datensätzen und Code betrifft dies oft übersehene Details, wie etwa Namen in Kommentaren, Autorentags, E-Mail-Adressen in Testdaten oder hardcodierte User-IDs.

Die Eingabe solcher Daten in ein KI-System gilt als Bekanntgabe an Dritte. Dies ist nur zulässig, wenn eine explizite Rechtfertigung vorliegt (DSG, 2025, Art. 31 Abs. 1).

2.5.1.2 Besonders schützenswerte Daten

Hierzu zählen beispielsweise Gesundheitsdaten, Angaben zur Religionszugehörigkeit oder biometrische Daten (DSG, 2025, Art. 5 lit. c). Die Weitergabe an externe KI-Systeme ist aufgrund des hohen Risikos für die Persönlichkeit ohne ausdrückliche Einwilligung grundsätzlich unzulässig (DSG, 2025, Art. 31 Abs. 2 lit. a).

2.5.1.3 Nicht-personenbezogene Daten

Zu dieser Kategorie zählen Informationen ohne direkten Personenbezug wie beispielsweise technische Daten, Systemkonfigurationen oder abstrakte Logik. Diese Daten unterstehen nicht dem Datenschutzgesetz. Sie dürfen weitergegeben werden, sofern kein Geschäftsgeheimnis (UWG, 2025, Art. 6) oder Urheberrecht (URG, 2025, Art. 2) verletzt wird.

Da Programmiercode und technische Dokumentationen unter Umständen Geschäftsgeheimnisse darstellen, sind viele Formen von Unternehmenscode rechtlich wie vertrauliche Daten zu behandeln, auch wenn sie keinen Personenbezug aufweisen.

2.5.2 JSON-Dateien und strukturierte Datensätze

Strukturierte Datensätze, wie sie häufig im JSON-Format vorliegen, sind in der Softwareentwicklung allgegenwärtig. Sie enthalten oft nicht nur personenbezogene Daten, sondern auch sicherheitskritische Zugangsdaten, die beispielsweise in Test-Dumps oder Konfigurationsdateien vergessen wurden.

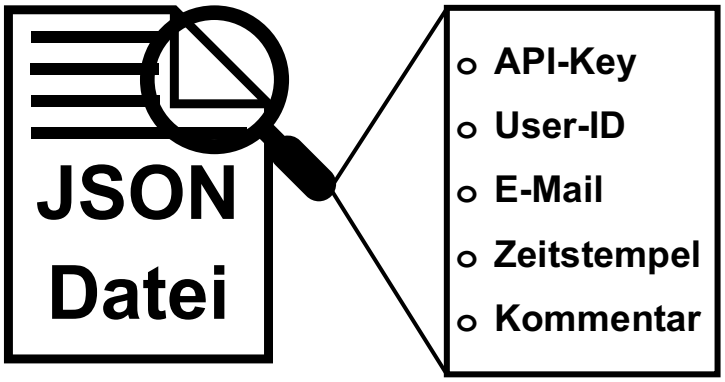


Abbildung 2: Visualisierung versteckter Personenbezüge und Sicherheitsrisiken in technischen Datensätze (eigene Darstellung)

2.5.2.1 Versteckte Personenbezüge in technischen Strukturen

Technische Identifikatoren in JSON-Objekten können fälschlicherweise als unkritisch eingestuft werden. Wie jedoch in Kapitel 2.3.2.1 dargelegt, genügt für den Personenbezug bereits die theoretische Möglichkeit der Zuordnung. In strukturierten Datensätzen betrifft dies häufig:

- Kundennummern oder interne User-IDs (Pseudonyme).
- Zeitstempel von Nutzeraktionen.
- Nutzungsmuster und Verhaltensdaten.
- Kombinationen mehrerer Merkmale, die eine Re-Identifikation ermöglichen.

Solche Daten fallen somit trotz ihres technischen Charakters in den Schutzbereich des DSG, da sie jederzeit einer konkreten Person zugeordnet werden können.

2.5.2.2 Sicherheitskritische Daten

Ein technisches Sicherheitsrisiko stellen Authentifizierungsdaten dar, die häufig in Konfigurationsdateien, Datenbank-Dumps oder API-Antworten enthalten sind. Die Weitergabe der folgenden Daten an externe Systeme stellt ein massives Sicherheitsrisiko dar:

- API-Keys: Zugangsschlüssel zu Drittdiensten oder internen APIs.
- Bearer-Tokens: temporäre Zugriffsberechtigungen für Nutzersitzungen.
- Passwörter: Klartext- oder Hash-Werte von Nutzer- oder Systemkonten.
- Private Keys: Kryptografische Schlüssel für Verschlüsselung oder Signatur.

Diese Daten können Dritten direkten Zugriff auf interne Infrastrukturen oder Kunden-Accounts gewähren und müssen daher unabhängig vom Datenschutzgesetz geschützt werden.

2.5.2.3 Anonymisierung und Bereinigung als Voraussetzung

Eine Weitergabe strukturierter Datensätze an externe KI ist nur unter folgenden Bedingungen zulässig:

- Es liegt eine echte Anonymisierung gemäss DSG (2025, Art. 2 Abs. 1) vor, bei der eine Re-Identifikation irreversibel ausgeschlossen ist.
- Sicherheitskritische Daten müssen vor der Eingabe restlos entfernt werden.

Da die Eingabe pseudonymisierter Daten in ein KI-Modell weiterhin eine Datenbekanntgabe an Dritte darstellt, ist Vorsicht geboten. Nur vollständig anonymisierte Daten dürfen frei an KI-Systeme übermittelt werden.

2.5.3 Programmiercode

Programmiercode kann sowohl personenbezogene Informationen wie beispielsweise hardcodierte IDs oder Kommentare mit Namen, als auch geschützte Geschäftsgeheimnisse enthalten. Daher muss zwischen sensibler und unsensibler Logik unterschieden werden.

2.5.3.1 Sensible Logik

Zu diesem Begriff zählen insbesondere Geschäftsgeheimnisse, sicherheitsrelevante Logik sowie proprietäre Algorithmen. Folgende Codearten dürfen nicht an externe KI-Systeme weitergegeben werden:

- Sicherheitsrelevante Funktionen (Authentifizierung, Autorisierung, Verschlüsselung)
- Interne Geschäftslogik, die einen Wettbewerbsvorteil darstellt
- Proprietäre oder patentfähige Algorithmen
- Nicht öffentlich zugängliche Softwarekomponenten und Bibliotheken
- Konfigurationsdaten (Secrets, API-Keys), die interne Systeme offenlegen

Diese Inhalte erfüllen die Kriterien eines Geschäftsgeheimnisses gemäss UWG (2025, Art. 6). Ihre unbefugte Weitergabe kann zudem eine Urheberrechtsverletzung darstellen (URG, 2025, Art. 2).

2.5.3.2 Unsensible Logik

In diese Kategorie fallen allgemeiner Hilfscode und unkritische Funktionen, die kein spezifisches Unternehmenswissen offenbaren. Folgende Codearten können an externe KI-Systeme weitergegeben werden:

- Einfache Utility- oder Helper-Funktionen
- Allgemein bekannte Entwurfsmuster
- Öffentlich dokumentierte oder standardisierte Algorithmen
- Beispielcode ohne Bezug zu internen Systemen
- Codebestandteile ohne geschäftsrelevante Logik oder interne Abläufe
- Code, der keine personenbezogenen Daten verarbeitet
- Nicht urheberrechtlich geschützte oder frei verfügbare Komponenten

Diese Arten von Code lassen keine Rückschlüsse auf interne Systeme zu, berühren keine Geschäftsgeheimnisse und weisen keinen Personenbezug auf.

2.6 Selbst gehostete Modelle (Qwen, Ollama)

Selbst gehostete KI-Modelle, wie sie beispielsweise von Alibaba mit Qwen angeboten werden oder lokal ausgeführte Modelle, wie sie mit Ollama möglich sind, unterscheiden sich grundlegend von cloudbasierten Systemen wie ChatGPT, Gemini oder Claude. Während bei Cloud-Modellen Daten an externe Anbieter übermittelt werden, verbleiben die Eingaben bei lokalen Modellen vollständig im Unternehmen.

Um die Sicherheitsimplikationen dieser beiden Architekturansätze zu verdeutlichen, werden die Datenflüsse in der folgenden Grafik gegenübergestellt. Szenario B zeigt das Risiko des Kontrollverlusts bei der Nutzung externer Server, insbesondere was die Speicherung und das Modelltraining in Drittstaaten betrifft. Szenario A zeigt dagegen, dass sensible Informationen beim Einsatz lokaler Modelle zu keinem Zeitpunkt den geschützten Netzwerkperimeter der Smoca AG verlassen.

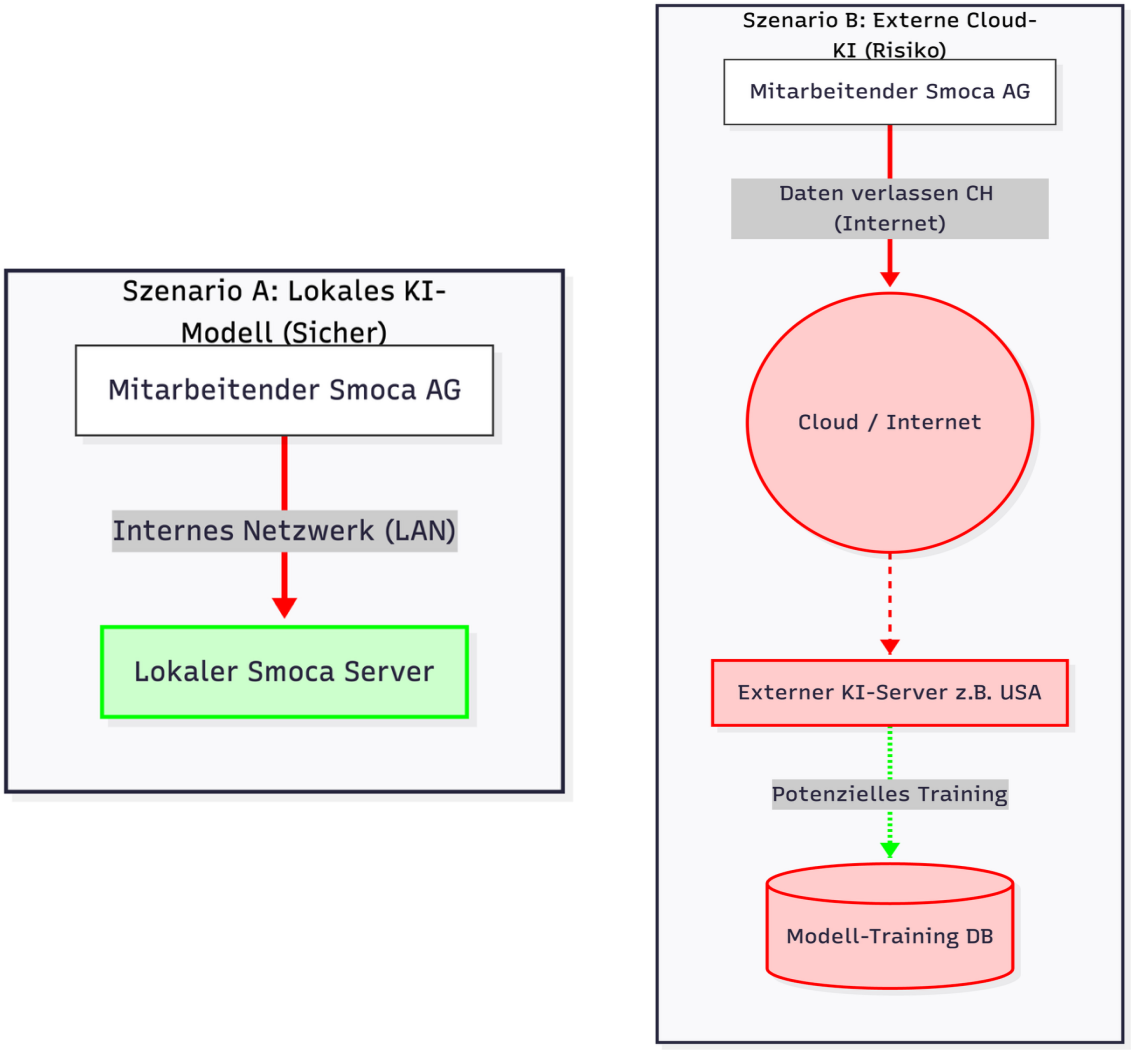


Abbildung 3: Vergleich der Datenflüsse und Sicherheitsrisiken zwischen lokalen Modellen (Szenario A) und externer Cloud-KI (Szenario B) (eigene Darstellung)

2.6.1 Vergleich: Cloud vs. lokale Modelle

Der wesentliche Unterschied betrifft die Datenflüsse und die rechtlichen Anforderungen.

2.6.1.1 Cloud-Modelle (OpenAI, Google, Anthropic)

Bei Cloud-Modellen werden Eingaben an externe Anbieter übermittelt. Dies stellt eine Bekanntgabe dar, wobei der Anbieter je nach Vertragsverhältnis als Dritter oder als Auftragsbearbeiter fungiert (DSG, 2025, Art. 9). Eine solche Übermittlung ist nur zulässig, wenn sie durch eine Rechtsgrundlage, einen klar definierten Zweck oder eine Einwilligung gedeckt ist (DSG, 2025, Art. 6, Art. 31). Zusätzlich müssen Betroffene darüber informiert werden, dass ihre Daten extern verarbeitet werden (DSG, 2025, Art. 19). Werden Daten an Server im Ausland übermittelt, gelten zudem die Anforderungen zur Auslandsbekanntgabe (DSG, 2025, Art. 16–17), insbesondere das Erfordernis eines angemessenen Schutzniveaus oder geeigneter Garantien.

Unternehmen haben dabei nur begrenzte Kontrolle über die Speicherung, Verarbeitung und Sicherheit der Daten.

2.6.1.2 Selbst gehostete Modelle (Qwen, Ollama, lokale LLMs)

Im Gegensatz dazu verbleiben die Daten bei selbst gehosteten Modellen vollständig im Unternehmen. Das bedeutet, dass keine Bekanntgabe an Dritte erfolgt. Die Verarbeitung, zum Beispiel die Antwortgenerierung, ist zwar trotzdem eine Datenverarbeitung nach DSG, findet jedoch innerhalb derselben verantwortlichen Stelle statt. Dadurch sind die Anforderungen reduziert. Es erfolgt keine Auslandsübermittlung, das Unternehmen behält die volle Kontrolle über Speicherung, Löschung und Sicherheit, und es findet keine Weitergabe von Geschäftsgeheimnissen an Dritte statt. Selbst gehostete Modelle erleichtern somit die Einhaltung der Datenschutz-, Zweckbindungs- und Geheimhaltungspflichten erheblich.

2.6.2 Vorteile und Nachteile selbst gehosteter Modelle

Der Einsatz lokaler KI-Modellen unterscheidet sich grundlegend von der Nutzung externer Cloud-Dienste. Im Folgenden werden die spezifischen Vor- und Nachteile in Bezug auf Datenschutz, Kontrolle und Ressourcenaufwand analysiert.

2.6.2.1 Vorteile

Die Hauptargumente für den Eigenbetrieb sind die vollständige Datenhoheit und die Minimierung rechtlicher Risiken. Insbesondere im Kontext strenger Datenschutzvorgaben bieten lokale Systeme folgende entscheidende Mehrwerte:

2.6.2.1.1 Höhere Datensicherheit

Da sämtliche Verarbeitung lokal erfolgt, findet keine Bekanntgabe an Dritte statt (DSG, 2025, Art. 5 lit. e). Somit entfallen die Anforderungen an eine Auslandsbekanntgabe (DSG, 2025, Art. 16–17). Unternehmen behalten zudem die vollständige Kontrolle über die Umsetzung technischer und organisatorischer Massnahmen (DSG, 2025, Art. 8).

2.6.2.1.2 Volle Kontrolle über gespeicherte Informationen

Das Unternehmen legt Speicherfristen, Zugriffsberechtigungen und Verschlüsselung selbst fest. Dadurch werden Know-how-Verlust und die ungewollte Offenlegung von Geschäftsgeheimnissen verhindert (UWG, 2025, Art. 6).

2.6.2.1.3 Unabhängigkeit von Dritten

Es besteht keine Abhängigkeit von externen AGB-Änderungen, Verfügbarkeitsproblemen oder intransparenten Modell-Updates. Dadurch werden stabile Ergebnisse sichergestellt und Compliance-Risiken minimiert.

2.6.2.2 Nachteile

Dem Gewinn an Sicherheit stehen jedoch erhöhte Anforderungen an die betrieblichen Ressourcen gegenüber. Verzichtet ein Unternehmen auf externe Cloud-Lösungen, so trägt es die

vollständige Verantwortung für Betrieb und Stabilität. Dies bringt die folgenden Herausforderungen mit sich:

2.6.2.2.1 Hoher technischer Aufwand

Der Aufwand für die Integration lokaler KI-Modelle hängt stark von der gewählten Implementierungsstrategie ab. Wenn ein zentraler Dienst für viele Mitarbeitende bereitgestellt werden soll, ist je nach Anforderungsprofil eine leistungsfähige Server-Infrastruktur erforderlich. Alternativ können die Modelle dezentral direkt auf den Endgeräten der Nutzenden ausgeführt werden. Dies setzt jedoch leistungsstarke Hardware voraus und kann zu längeren Antwortzeiten führen. Zudem erfordert dieser Ansatz entweder entsprechendes technisches Know-how bei den Anwendenden selbst oder einen erheblichen Administrationsaufwand für die Verteilung und Konfiguration der Software auf allen Geräten.

2.6.2.2.2 Laufende Wartung

Neben der initialen Einrichtung erfordert der Betrieb eine kontinuierliche Wartung von Hardware und Software. Das Unternehmen muss sicherstellen, dass stets Personal mit dem erforderlichen Fachwissen verfügbar ist, um die Infrastruktur zu betreuen. Häufig kommt die Pflege von Zusatzsoftware, wie Web-Interfaces oder API-Gateways hinzu. Dies ist notwendig, um den Mitarbeitenden einen benutzerfreundlichen und sicheren Zugriff auf die Modelle zu ermöglichen. Dies erhöht die Komplexität und bindet langfristig interne Ressourcen.

2.6.2.2.3 Kosten für Hardware und Updates

Im Gegensatz zu Cloud-Diensten, die meist nutzungsbasiert abgerechnet werden, ist beim Eigenbetrieb eine anfängliche Investition in Hardware erforderlich. Selbst bei der Nutzung kosteneffizienter Endgeräte anstelle von Hochleistungsservern entstehen Anschaffungskosten, die amortisiert werden müssen. Hinzu kommen laufende Betriebsausgaben für Energie sowie der personelle Aufwand für regelmässige Updates. Da sich der Markt für Open-Source-Modelle dynamisch entwickelt, müssen kontinuierlich Ressourcen bereitgestellt werden, um die Modelle zu aktualisieren und die Kompatibilität der Systeme sicherzustellen. Dies stellt langfristig oft den grössten Kostenfaktor dar.

2.6.3 Einsatz von Kundendaten für das Training betriebsinterner Modelle

Das Training interner Modelle gilt als Datenverarbeitung (DSG, 2025, Art. 5 lit. d). Auch ohne Datenabfluss gelten folgende Restriktionen:

2.6.3.1 Personenbezogene Daten

Die Nutzung dieser Daten für das Training erfordert eine Rechtsgrundlage (Einwilligung oder überwiegendes Interesse gemäss Art. 31 DSG), sofern dieser Zweck nicht bereits bei der Erhebung transparent kommuniziert wurde (Zweckbindung, Art. 6 Abs. 3 DSG).

2.6.3.2 Anonymisierte Daten

Anonymisierte Daten dürfen frei verwendet werden, sofern eine Re-Identifizierung faktisch ausgeschlossen ist.

2.6.3.3 Quellcode

Quellcode kann urheberrechtlich (URG, 2025, Art. 2) oder als Geschäftsgeheimnis (UWG, 2025, Art. 6) geschützt sein. Um eine unzulässige Verwertung fremder Arbeitsergebnisse zu vermeiden, ist für die Nutzung zum Training eine vertragliche Erlaubnis des Kunden erforderlich.

2.6.4 Rechtliche Voraussetzungen

Für die Nutzung von Kundendaten zum Training interner Modelle ist eine Rechtsgrundlage erforderlich. Gemäss DSG (2025, Art. 6) gelten die Grundsätze der Zweckbindung und Transparenz. Ein Training ist nur zulässig, wenn es mit dem ursprünglichen Erhebungszweck vereinbar ist (Art. 6 Abs. 3), eine Einwilligung vorliegt oder ein überwiegendes Interesse geltend gemacht werden kann (DSG, 2025, Art. 31). Lediglich vollständig anonymisierte Daten können uneingeschränkt verwendet werden. Die Betroffenen sind über diese Bearbeitung zu informieren (DSG, 2025, Art. 19). Besondere Vorsicht ist bei Quellcode geboten, da dieser oft urheberrechtlich geschützt ist (URG, 2025, Art. 2) oder ein Geschäftsgeheimnis darstellt (UWG, 2025, Art. 6). Ohne vertragliche Erlaubnis ist die Nutzung für Trainingszwecke unzulässig.

2.6.5 Interne technische und organisatorische Massnahmen

Unternehmen sind verpflichtet, die Datensicherheit durch geeignete Massnahmen zu gewährleisten (DSG, 2025, Art. 8). Die nachfolgenden Beispiele zeigen mögliche Massnahmen auf.

2.6.5.1 Technische Massnahmen

- Zugriffskontrolle: Beschränkung des Zugriffs auf Modelle und Trainingsdaten.
- Datentrennung: Logische oder physische Trennung von Trainings- und Produktivdaten.
- Sicherheit: Verschlüsselung der Daten im Ruhezustand und während des Transfers sowie Protokollierung aller Zugriffe.

2.6.5.2 Organisatorische Massnahmen

- Richtlinien: Klare Vorgaben zur Datenklassifizierung und Freigabe für das KI-Training.
- Schulung: Sensibilisierung der Mitarbeitenden zum Schutz von Geschäftsgeheimnissen (UWG, 2025, Art. 6).
- Audits: Regelmässige Überprüfung der Modelle auf Schwachstellen und Datenlecks.

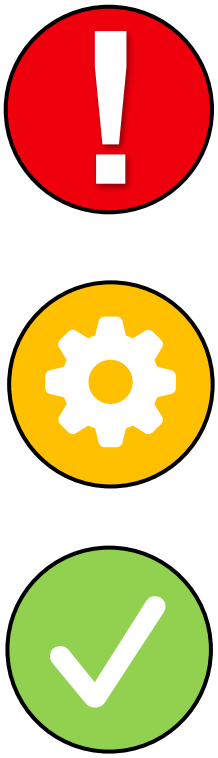
2.7 Entwicklung von Smoca-internen KI-Richtlinien

Die Smoca AG ist technisch hervorragend aufgestellt, um KI sicher zu nutzen. Da die Mitarbeitenden über technisches Know-how verfügen und bereits leistungsfähige Hardware (MacBooks mit Apple Silicon) sowie eine intern gehostete Modell-Infrastruktur nutzen, ist es nicht notwendig, in den Richtlinien technische Grundlagen zu erklären. Stattdessen müssen die Richtlinien den rechtlichen Rahmen für den Umgang mit Daten definieren.

Da in der Smoca AG flache Hierarchien herrschen und es keine zentrale Compliance-Abteilung gibt, setzen die Richtlinien auf die Eigenverantwortung der Entwicklerinnen und Entwickler. Ziel ist es, das Bewusstsein für Datenkategorien zu schärfen.

2.7.1 Ampel-System

Als Ergebnis dieser Arbeit wird ein Klassifizierungssystem in Form eines «Ampel-Systems» vorgeschlagen, das sich nahtlos in den Alltag der Entwicklerinnen und Entwickler integrieren lässt.



2.7.1.1 ROT - Verbot externer KI

In diese Kategorie fallen alle hochsensiblen Informationen, deren Abfluss einen erheblichen Schaden verursachen würde. Dazu gehören Personendaten, Zugangsdaten (API-Keys, Passwörter), Produktionsdatenbanken sowie Code, der strikten Geheimhaltungsverträgen (NDAs) unterliegt. Solche Daten dürfen niemals an externe Cloud-Anbieter gesendet werden. Die Lösung liegt hier zwingend in der Nutzung interner oder lokaler Modelle.

2.7.1.2 GELB - Bedingte Nutzung

Hierzu zählen interner Programmcode ohne kritische Business-Logik, anonymisierte Fehlermeldungen und generische Texte. Die Nutzung von Cloud-Diensten ist unter der strikten technischen Voraussetzung erlaubt, dass das Training mit diesen Daten in den Einstellungen deaktiviert ist.

2.7.1.3 GRÜN - Freie Nutzung

In diese Kategorie fallen öffentliche Informationen, Open-Source-Code oder Marketingtexte ohne Personenbezug. Hier können sämtliche verfügbaren KI-Tools zur Effizienzsteigerung uneingeschränkt genutzt werden.

Abbildung 4: Die drei Stufen des Ampelsystems (eigene Darstellung

Die nachfolgende Tabelle 3 fasst dieses System übersichtlich zusammen und dient als Entscheidungshilfe für die Wahl des korrekten Tools.

Tabelle 4: Übersicht der Datenkategorien und zulässigen KI-Lösungen (eigene Darstellung)

ROT	GELB	GRÜN
Sensible Daten:	**Interner Code:**	**Public Info:**
Personendaten	Abstrakte Logik	Open Source
Credentials / Keys	Anon. Logs	Docs
NDA-Code	Generische Mails	Marketing
Lösung:	**Lösung:**	**Lösung:**
Localhost only Ollama, Firmeninternes Modell	Cloud Training: OFF	Alle Tools (ChatGPT, Claude etc.)

2.7.2 Flow Chart

Während die vorangegangene Tabelle als schnelles Nachschlagewerk dient, visualisiert Abbildung 1 den konkreten Entscheidungsprozess im Arbeitsalltag.

Der Algorithmus beginnt stets mit der Prüfung auf die höchste Risikostufe. Nur wenn keine sensiblen Daten vorliegen, erfolgt die Prüfung auf interne Daten. Dies stellt sicher, dass kritische Informationen wie Credentials oder Personendaten bereits im ersten Schritt abgefangen und zwingend auf lokale Modelle umgeleitet werden.

Abbildung 5: Entscheidungsbaum zur Ermittlung der korrekten Datenkategorie und KI-Lösung (eigene Darstellung)

2.7.3 Ableitung praxisnaher KI-Vorgaben

Das Ziel dieser Richtlinien besteht darin, die bestehende technische Kompetenz der Mitarbeitenden mit rechtlicher Sicherheit zu untermauern. Da die Hardware (lokale Server und M-Chip-Laptops) bereits vorhanden ist, dienen die Vorgaben primär dazu, Flüchtigkeitsfehler im Umgang mit sensiblen Kundendaten zu vermeiden (DSG, 2025, Art. 6). Die Richtlinien sollen so schlank gestaltet sein, dass sie vom Team ohne bürokratischen Aufwand umgesetzt werden können.

3 Schlussteil

3.1 Zusammenfassung der Ergebnisse

In der vorliegenden Arbeit wurden die datenschutzrechtlichen Anforderungen an den Einsatz von KI-Modellen in der Softwareentwicklung untersucht. Die rechtliche Analyse bestätigte, dass die Eingabe von Kundendaten in externe Cloud-Systeme häufig eine genehmigungspflichtige Datenbekanntgabe darstellt. Insbesondere die Nutzung von Daten zum Training externer Modelle ohne explizite Einwilligung der Betroffenen stellt eine Zweckentfremdung dar (DSG, Art. 6 Abs. 3).

Die technische Analyse der Smoca AG ergab jedoch eine vorteilhafte Ausgangslage: Da die Belegschaft überwiegend aus IT-Fachkräften besteht und die Arbeitsgeräte über leistungsstarke Prozessoren verfügen, ist die Abhängigkeit von Cloud-KI geringer als in anderen Unternehmen. Zudem existiert bereits eine interne Infrastruktur für das Hosting eigener Modelle. Das Hauptrisiko liegt somit nicht in der technischen Machbarkeit, sondern in der korrekten Klassifizierung der Daten im Arbeitsalltag. Als Lösung hierfür wurde das «Ampel-System» entwickelt, welches juristische Komplexität in einfache Handlungsanweisungen übersetzt.

3.2 Schlussfolgerungen und Empfehlungen

Aufgrund der hohen technischen Reife der Smoca AG werden folgende Handlungsempfehlungen ausgesprochen:

3.2.1 Priorisierung von «Local-First»

Da die Entwicklerinnen und Entwickler über das notwendige Know-how sowie leistungsfähige Hardware verfügen, sollte bei Coding-Aufgaben standardmässig auf lokale Modelle (auf dem eigenen MacBook oder dem internen Server) gesetzt werden. Dies eliminiert das Datenschutzrisiko fast vollständig.

3.2.2 Verbindliche «Opt-Out»-Regelung bei Subscriptions

Für sämtliche genutzten Accounts muss zwingend sichergestellt werden, dass die Option zur Verwendung der Daten für das Modelltraining in den Einstellungen explizit deaktiviert ist.

3.2.3 Implementierung des Ampel-Systems

Die in Kapitel 2.7 erarbeitete Datenklassifizierung sollte als einfaches Merkblatt etabliert werden, um im hektischen Projektalltag schnelle Entscheidungen zu ermöglichen.

3.2.4 Nutzung des internen Modells für NDA-Projekte

Bei Kundenprojekten mit strengen Geheimhaltungsanforderungen ist die Nutzung externer Cloud-Dienste proaktiv zu untersagen und auf die bereits vorhandene interne Instanz zu verweisen.

3.2.5 Beurteilung der Allgemeingültigkeit

Es ist kritisch anzumerken, dass diese Ergebnisse spezifisch auf die Ressourcen der Smoca AG zugeschnitten sind. Für Unternehmen ohne eine vergleichbare IT-Infrastruktur oder technisches

Fachpersonal wäre die hier empfohlene «Local-First»-Strategie aufgrund des hohen Wartungsaufwands kaum umsetzbar. Die Ergebnisse sind daher nicht universell auf alle KMU übertragbar, sondern setzen eine hohe technische Reife voraus.

3.3 Reflexion und Ausblick

Die Erarbeitung dieser interdisziplinären Projektarbeit erfolgte in einem dynamischen Umfeld. Zwar aktualisierten Anbieter wie OpenAI oder Google während der Schreibphase ihre Datenschutzerklärungen, jedoch zeigte die Analyse, dass die grundlegenden Prinzipien der Datenverarbeitung konstant blieben. Die Aktualisierungen änderten somit nichts am rechtlichen Rahmen, bestätigten jedoch die Notwendigkeit einer vom Anbieter unabhängigen Strategie.

Die zentrale Herausforderung im Arbeitsprozess lag in der interdisziplinären Verknüpfung der Fachbereiche Wirtschaft und Recht mit der Informatik. Während die juristische Analyse oft theoretische Grenzen aufzeigte («Verbot der Bekanntgabe»), mussten aus technischer Sicht pragmatische Lösungen gefunden werden («lokales Hosting»), die den Arbeitsfluss nicht behinderten. Persönlich konnte ich durch diese Auseinandersetzung mein Verständnis dafür vertiefen, dass Datenschutz in der Softwareentwicklung kein Hindernis, sondern ein Qualitätsmerkmal ist. Das entwickelte «Ampel-System» hat sich dabei als zielführendes Instrument erwiesen, um diese Qualitätssicherung ohne bürokratischen Aufwand sicherzustellen.

Mit Blick auf die Zukunft und den kommenden EU AI Act ist die Smoca AG mit der in dieser Arbeit definierten Strategie gut aufgestellt. Da die Datenhoheit durch lokale Modelle im Unternehmen verbleibt, ist die Agentur auch gegen strengere zukünftige Regulierungen gewappnet.

Selbstständigkeitserklärung

Ich habe die vorliegende Arbeit selbstständig verfasst und keine anderen als die erlaubten und angegebenen Quellen, Fachtexte und Hilfsmittel verwendet.

Name: **Zürcher** Vorname: **Lukas**

Ort: Winterthur Datum: 22.01.2026

Unterschrift: 

Tabellenverzeichnis

Abbildungsverzeichnis

Hilfsmittelverzeichnis

Gemini, Version 3 Pro.

DeepL Write.

Literaturverzeichnis

Anthropic. (2025a, 8. Oktober). *Datenschutzerklärung*. https://www.anthropic.com/legal/privacy

Anthropic. (2025b). *Datennutzung bei Konsumenten-Produkten für Model Training*. https://privacy.claude.com/en/articles/10023580-is-my-data-used-for-model-training

Anthropic. (2025c). *Datennutzung bei Kommerzielle-Produkten für Model Training*. https://privacy.claude.com/en/articles/7996868-is-my-data-used-for-model-training#h_8bd735aa4e

DSG. (2025, 7. Juli). https://www.fedlex.admin.ch/eli/cc/2022/491/de

Google. (2025a, 1. Juli). *Datenschutzerklärung*. https://policies.google.com/privacy?hl=de

Google. (2025b, 1. Dezember). *Gemini FAQ*. https://support.google.com/gemini/answer/13594961?hl=de

Google. (o. D.). *Gemini for Workspace – Datenschutzhinweise*. https://workspace.google.com/intl/de_ch/security/ai-privacy/

OpenAI. (2024a, 24. Juni). *Datenschutz für Endverbraucher*. https://openai.com/consumer-privacy/

OpenAI. (2024b, 4. November). *Datenschutzerklärung*. https://openai.com/de-DE/policies/eu-privacy-policy/

URG. (2025, 1. Juli). https://www.fedlex.admin.ch/eli/cc/1993/1798_1798_1798/de

UWG. (2025, 1. Januar). https://www.fedlex.admin.ch/eli/cc/1988/223_223_223/de