Das Potenzial von Open Source KI im Kontext von Datenschutz und Berufsgeheimnis

Studie des Instituts Public Sector Transformation (IPST)
am Departement Wirtschaft der Berner Fachhochschule (BFH)

In Zusammenarbeit mit der ERFA-Gruppe
«KI-Tool für kleine(re) Anwaltskanzleien»
des Bernischen Anwaltsverbands (BAV)

Bern, 3. März 2026

Lara Burkhalter, Luca Rolshoven, Marcel Gygli, Matthias Stürmer

Inhaltsverzeichnis

Executive Summary

Die vorliegende Studie untersucht, wie kleine und mittlere Unternehmen (KMU), deren Mitarbeitende dem Berufsgeheimnis unterliegen, künstliche Intelligenz (KI) rechtskonform in ihre Arbeitsprozesse integrieren können. Analysiert werden vier auf Open-Source-KI-Modellen basierende Lösungsansätze: Lokale (Laptop) Open-Source-KI-Lösung, serverbasierte Eigenlösungen, externe Hosting-Lösung (IaaS) sowie der Bezug von KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS).

Zunächst wurden die einschlägigen rechtlichen Rahmenbedingungen analysiert, insbesondere das Datenschutzgesetz (DSG), das strafrechtliche Berufsgeheimnis gemäss Art. 321 StGB sowie das anwaltsrechtliche Berufsgeheimnis nach Art. 13 BGFA. Darauf aufbauend wurden exemplarische Anwendungsfälle entwickelt, anhand derer ein Open-Source-KI-Prototyp der Berner Fachhochschule (BFH) entwickelt wurde. Der Quellcode davon ist auf GitHub veröffentlicht.[1]

Die Ergebnisse zeigen, dass der Einsatz von KI-Tools bei Berufsgeheimnisträgern unter Einhaltung der rechtlichen Vorgaben grundsätzlich möglich ist. Basierend auf den dargestellten Ergebnissen hat sich insbesondere die Nutzung des BFH-KI-Prototyps entweder auf einem eigenen Server oder auf einem Server einer vertrauenswürdigen Cloud-Anbieterin (IaaS) als beste Lösung erwiesen. Dies gilt sowohl aus Kostensicht als auch aus rechtlicher Sicht, da die Informationen (Personendaten und Geheimnisse) entweder kanzleiintern bearbeitet oder verschlüsselt bei der Cloud-Anbieterin gespeichert werden.

Die Studie wurde im Auftrag der ERFA-Gruppe «KI-Tool für kleine(re) Anwaltskanzleien» des Bernischen Anwaltsverbands (BAV) durchgeführt und im Rahmen des Innovationsscheck 127.305 INNO-ICT finanziert. Während des gesamten Projektverlaufs bestand ein regelmässiger fachlicher Austausch mit dieser ERFA-Gruppe, wodurch praxisrelevante Bedürfnisse und Fragestellungen direkt in die Untersuchung einfliessen konnten.

[1] Fiducia (Public PoC) auf GitHub <https://github.com/digital-sustainability/fiducia>

1 Einleitung

Wie viele andere Unternehmen erhoffen sich auch kleine und mittlere Anwaltskanzleien und Notariate sowie Arztpraxen durch den Einsatz von KI-Tools ihre Arbeitsprozesse effizienter gestalten zu können. Ein zentrales Problem, mit dem diese Branchen im Vergleich zu anderen konfrontiert sind, betrifft die Wahrung des Berufsgeheimnisses. Gemäss Art. 321 des Schweizerischen Strafgesetzbuches (StGB)[2] können sich unter anderem Rechtsanwältinnen[3], Notarinnen oder Ärztinnen dadurch strafbar machen, dass sie ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist, oder das sie in dessen Ausübung wahrgenommen haben. Die Offenbarung eines Geheimnisses liegt bereits vor, wenn beispielsweise eine unzureichende Aufbewahrung der Akten besteht und die Täterin in Kauf nimmt, dass sich eine Aussenstehende Einsicht verschaffen kann.[4] Gegenwärtige Studien weisen darauf hin, dass bei der Verwendung von im Internet zur Verfügung gestellten KI-Lösungen Verletzungen des Berufsgeheimnisses vorliegen können.[5] Vor allem dem Berufsgeheimnis unterstehenden kleine und mittlere Unternehmen (KMU), die nicht über die gleichen finanziellen Möglichkeiten wie Grossunternehmen verfügen, sind bei einer gesetzlich konformen Nutzung von KI-Lösungen weitgehend eingeschränkt.

2 Ziel und Aufbau der Studie

Im Rahmen dieser Studie des Institut Public Sector Transformation der Berner Fachhochschule (BFH) werden vier Lösungsvorschläge dargelegt, anhand deren aufgezeigt wird, wie Anwalts-, Notariats- und Arzt-KMUs KI-Tools unter Wahrung der geltenden rechtlichen Bestimmungen, insbesondere des Berufsgeheimnisses, in ihre Prozesse integrieren können. Besonderes Augenmerk wird auch auf die finanziellen Möglichkeiten und die technische Umsetzbarkeit gelegt.

Die erarbeiteten Lösungsvorschläge sollen dabei eine digital souveräne und von US-Technologieanbietern unabhängige Lösung darstellen. In diesem Zusammenhang ist der Bereich "Open-Source-AI" von grosser Bedeutung, da mit den frei zugänglichen KI-Modellen Lösungen auf persönlichen Computer, auf eigenen Servern oder auf zur Verfügung gestellten Infrastrukturen von Drittanbietern betrieben werden können.[6]

Die vier möglichen Lösungsansätze, die allesamt auf Open-Source-KI-Modellen basieren, unterscheiden sich wie folgt:

1. Lokale Open-Source-KI-Lösung: Der Betrieb eines Open-Source-KI-Modelles erfolgt vollständig auf einem lokalen Endgerät (z.B. auf dem eigenen Arbeitslaptop).[7]
2. Serverbasierte Eigenlösung: Das Open-Source-KI-Modell wird auf einem unternehmenseigenen Server betrieben.
3. Externe Hosting-Lösung (IaaS): Das Open-Source-KI-Modell wird auf einem externen Server einer Schweizer[8] Cloud-Anbieterin (Infrastructure-as-a-Service, IaaS) betrieben.
4. KI-Dienstleistungen von einer Schweizer[9] Cloud-Anbieterin (SaaS): Die KI-Applikation sowie die Datenhaltung werden auf einem unternehmenseigenen Server betrieben und die KI-Dienstleistung wird von einer Cloud-Anbieterin bezogen (Software-as-a-Service, SaaS).

---

[2] SR 311.0 Schweizerisches Strafgesetzbuch (StGB).

[3] Zur besseren Lesbarkeit wird das generische Femininum verwendet. Die Bezeichnungen gelten für alle Geschlechter.

[4] BSK StGB-OBERHOLZER, Art. 321 N 19

[5] Siehe beispielsweise: KOHLMEIER, Der Einsatz von KI: Was wir juristisch wissen und was nicht; KOHLMEIER, KI-Einsatz in Anwaltskanzleien und Unternehmen; FÖRSTER, Keine Garantien: Microsoft muss EU-Daten an USA übermitteln; KÖCHLI ROLAND, SS. 372-379.

[6] Siehe auch http://bfh.ch/ipst/public-sector-ai

[7] Da die notwendige Rechenleistung für den zuverlässigen Einsatz solcher Anwendungen oftmals die Möglichkeiten eines normalen Laptops übersteigen, wird dieser Lösungsvorschlag zwar genannt, aber schlussendlich nicht empfohlen.

[8] Da die notwendige Rechenleistung für den zuverlässigen Einsatz solcher Anwendungen oftmals die Möglichkeiten eines für den üblichen Geschäftseinsatz verwendeten Laptops übersteigen, wird dieser Lösungsvorschlag zwar genannt, aber nicht empfohlen.

[9] Die Studie beschränkt sich ausdrücklich auf den Bezug einer KI-Dienstleistung eine Schweizer Cloud-Anbieterin. Bei der Nutzung einer ausländischen Dienstleisterin wäre der rechtliche Rahmen gesondert zu analysieren.

Mit dem Begriff «Cloud» wird eine Vielzahl von Online-Diensten bezeichnet, die über ein Netzwerk ortsunabhängig genutzt werden können.[10] Zu den Online-Diensten zählen das Anbieten von Rechner- und Speicherkapazität, Plattformdienste oder Anwendungsdienste.

Die Studie richtet sich grundsätzlich an sämtliche KMUs, die dem Berufsgeheimnis unterstehen. Die Ausführungen und Bewertungen dieser Studie erfolgen jedoch exemplarisch anhand von kleinen und mittleren Anwaltskanzleien.

Zu Beginn der Studie werden die rechtlich relevanten Rahmenbedingungen dargelegt. Im Fokus stehen dabei das Berufsgeheimnis, die datenschutzrechtlichen Vorgaben sowie die für Rechtsanwältinnen spezifische Pflichten aus dem Anwaltsgesetz. Im Anschluss wird der funktionale Umfang eines potenziellen KI-Tools für kleine Anwaltskanzleien anhand exemplarischer Anwendungsfälle (Use Cases) definiert. Auf dieser Grundlage wird ein Prototyp eines geeigneten Open-Source-KI-Modells intern an der BFH entwickelt und im Rahmen dieser Studie vorgestellt.

Basierend auf den zuvor beschriebenen Lösungsansätzen erfolgt abschliessend eine Gegenüberstellung verschiedener Betriebsvarianten des BFH-KI-Prototypen unter Berücksichtigung technischer, rechtlicher und wirtschaftlicher Kriterien.

Die vorliegende Studie stellt eine Momentaufnahme dar, die den Stand der Technik zum Zeitpunkt ihrer Erstellung widerspiegelt. Angesichts der raschen technologischen Entwicklungen ist zu beachten, dass die hierin enthaltenen Einschätzungen und Empfehlungen einer fortlaufenden Überprüfung und Aktualisierung bedürfen.

3 Rechtlicher Rahmen

Bei der Nutzung bereitgestellter KI-Anwendungen oder der für den Betrieb von KI-Applikationen eingesetzten Cloud-Lösungen ist aus rechtlicher Sicht im Vorfeld zu klären, wie mit den eingegebenen Daten (Prompting-Daten) sowie mit den Daten umgegangen wird, auf die ein KI-Modell im Rahmen seiner Funktionalität zugreift (etwa im Fall von *Retrieval-Augmenten-Generation* (RAG)– Lösungen). Dabei ist massgeblich zu prüfen, wer Zugriff auf diese Daten hat und wo sie (zwischen-)gespeichert werden.[11]

In diesem Zusammenhang sind insbesondere die strafrechtliche Berufsgeheimnispflicht, die datenschutzrechtlichen Bestimmungen sowie das anwaltliche Berufsgeheimnis zu beachten, auf die nachfolgend näher eingegangen wird.

3.1 Datenschutzrecht

Das Bearbeiten von Personendaten durch Private in der Schweiz oder mit Auswirkung in der Schweiz unterliegt den Bestimmungen des schweizerischen Datenschutzgesetzes (DSG).[12]

Personendaten sind nach Art. 5 lit. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Unterschieden wird zwischen Personendaten und besonders schützenswerten Personendaten. Letztere umfassen Daten zu religiösen oder politischen Ansichten, Gesundheitsinformationen, Informationen zur Intimsphäre oder zur Zugehörigkeit zu einer Rasse oder Ethnie, genetische und biometrische Daten, Daten zu verwaltungs- und strafrechtlichen Verfolgungen oder Sanktionen sowie zu Massnahmen der sozialen Hilfe (Art. 5 lit. c DSG). Dabei ist die Liste in Art. 5 lit. c DSG abschliessend.[13]

Das Bearbeiten von Personendaten umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren,

[10] SCHWARZENEGGER/THOUVENIN /STILLER/GEORGE, S. 25.

[11] Vgl. auch SAV-Wegleitung für den Umgang mit künstlicher Intelligenz.

[12] SR 235.1 Bundesgesetz über den Datenschutz (DSG). Die Anwendung der Datenschutz-Grundverordnung (DSGVO) wird im Rahmen dieser Studie nicht berücksichtigt.

[13] BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, Art. 5 Rz. 55.

Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (Art. 5 lit. d DSG). Die Bearbeitung von Personendaten darf nur nach den allgemeinen Grundsätzen nach Art. 6 DSG erfolgen. Dabei müssen die Personendaten rechtmässig, verhältnismässig und nach Treu und Glauben bearbeitet werden (Art. 6 Abs. 1 und 2 DSG). Die Personendaten dürfen nur zu einem bestimmten und erkennbaren Zweck beschafft werden und nur in Übereinstimmung mit diesem Zweck bearbeitet werden (Art. 6 Abs. 3 DSG). Aus Art. 6 Abs. 3 DSG ergibt sich, obwohl nicht ausdrücklich erwähnt, der Grundsatz der Transparenz, nach welchem die Erkennbarkeit des Zweckes nur durch eine transparente Datenbearbeitung gewährleistet werden kann.[14] Wer Personendaten bearbeitet, muss die Richtigkeit dieser Personendaten sicherstellen (Art. 6 Abs. 5 DSG) und die Personendaten vernichten oder anonymisieren, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4 DSG).

Die Einwilligung wird in Art. 6 DSG (Art. 6 Abs. 6 und 7 DSG) behandelt, stellt aber keinen Bearbeitungsgrundsatz dar. Für die Bearbeitung von besonders schützenswerten Personendaten, beim Profiling mit hohem Risiko durch eine private Person oder bei einem Profiling durch ein Bundesorgan, wird eine ausdrückliche Einwilligung seitens der betroffenen Person verlangt (Art. 6 Abs. 7 DSG). Eine Einwilligung gilt dann als ausdrücklich, «wenn sie durch geschriebene oder gesprochene Worte oder ein Zeichen erfolgt und der geäusserte Willen aus den verwendeten Worten oder dem Zeichen unmittelbar hervorgeht».[15]

Bei der Bearbeitung von Personendaten muss nach Art. 8 DSG zudem die Datensicherheit gewährleistet werden. Dazu muss durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Sicherheit garantiert werden (Art. 8 Abs. 1 DSG). Die Massnahmen sollen Verletzungen der Datensicherheit verhindern und die Integrität, Verfügbarkeit sowie Vertraulichkeit der bearbeiteten Personendaten sicherstellen (Art. 8 Abs. 2 DSG).[16] Die Mindestanforderungen an die Datensicherheit werden in Art. 3 DSV[17] konkretisiert.

Personendaten werden grundsätzlich durch die Verantwortliche selbst bearbeitet, d.h. durch die private Person oder das Bundesorgan, die bzw. das allein oder zusammen mit anderen über Zweck und Mittel der Bearbeitung entscheidet (Art. 5 lit. j DSG). Eine Übertragung der Datenbearbeitung auf eine Auftragsbearbeiterin (Art. 5 lit. k DSG) ist zulässig, sofern die in Art. 9 DSG genannten Voraussetzungen eingehalten werden.[18]

Die Übertragung der Bearbeitung durch eine Auftragsbearbeiterin hat regelmässig aufgrund eines Vertrags (sog. *Data Processing Agreement*, DPA) [19] oder dann ausnahmsweise durch Gesetzgebung zu erfolgen.[20] Die Verantwortliche muss sicherstellen, dass die Auftragsbearbeiterin die Daten nur so bearbeitet, wie die Verantwortliche es selbst tun dürfte (Art. 9 Abs. 1 lit. a DSG). Eine Übertragung ist dann unzulässig, wenn ihr gesetzliche oder vertragliche Geheimhaltungspflichten entgegenstehen (Art. 9 Abs. 1 lit. b DSG). Eine gesetzliche Geheimhaltungspflicht stellt beispielsweise das Berufsgeheimnis nach Art. 321 StGB dar. Wird die Auftragsbearbeiterin aber als Hilfsperson im Sinne von Art. 321 Ziff. 1 StGB qualifiziert, dann besteht zwischen Hilfsperson und Hauptgeheimnisträgerin keine Geheimhaltungspflicht, und die Weitergabe bzw. Bearbeitung der Personendaten durch die Auftragsbearbeiterin stellt keine strafrechtliche Offenbarung dar.[21]

Zudem muss sich die Verantwortliche vergewissern, dass die Auftragsbearbeiterin in der Lage ist, die Datensicherheit zu gewährleisten (Art. 9 Abs. 2 DSG).

---

[14] HUSI-STÄMPFLI/MORAND, Rz. 159.

[15] BSK DSG-BÜHLMANN/REINLE, Art. 6 Rz. 322.

[16] HÜRLIMANN/STEIGER, S. 201.

[17] SR 235.1 Verordnung über den Datenschutz (Datenschutzverordnung, DSV)

[18] BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 3.

[19] Siehe zum Mindestinhalt eines DPAs: BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 31.

[20] BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 4.

[21] BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 37; siehe Kapitel 3.2.1.3 und 3.2.1.4.

Die Auftragsbearbeiterin ist weisungsgebunden (vgl. Art. 9 Abs. 1 lit. a DSG) und bearbeitet die Daten nur gemäss den Weisungen der Verantwortlichen.[22] Deshalb steht ihr keine Entscheidungsbefugnis betreffend Zweck und Mittel zu.[23] Bei der Abgrenzung zwischen Verantwortlicher und Auftragsbearbeiterin ist also entscheidend, wem die Entscheidungsgewalt über Zweck und Mittel zukommt, nicht ausschlaggebend ist, ob sich die Verantwortliche selbst an der Bearbeitung beteiligt.[24]

Für die Auftragsbearbeitung ist grundsätzlich keine Einwilligung der betroffenen Personen erforderlich; die Auftragsbearbeiterin wird datenschutzrechtlich der Verantwortlichen zugeordnet, wodurch keine Bekanntgabe an Dritte erfolgt.[25]

Ein typisches Beispiel einer Auftragsbearbeiterin ist eine Cloud-Anbieterin, die einem Unternehmen ihre Computer und Software zur Bearbeitung von Daten zur Verfügung stellt.[26] Hingegen ist bei IT-Supportleistungen die Rollenzuteilung schwieriger: Bei einem bloss punktuellen Zugriff auf Personendaten durch die IT-Supportleistung, ist die IT-Dienstleisterin keine Auftragsbearbeiterin und auch keine Verantwortliche, sondern schlichtweg eine Dritte.[27] Die Prüfung und Wartung von IT-Systemen, bei welchen eine IT-Dienstleisterin zufällig mit Personendaten in Kontakt kommt, stellt grundsätzlich ebenfalls keine Auftragsbearbeitung dar.[28] Hat die IT-Dienstleisterin jedoch einen systematischen Zugriff auf Personendaten, weil es die Art der IT-Supportleistung verlangt, ist die Dienstleisterin als Auftragsbearbeiterin anzusehen.[29]

3.2 Strafrecht

3.2.1 Berufsgeheimnis Art. 321 StGB

Der Kern des Tatbestandes des Berufsgeheimnisses liegt im Interesse der Geheimnisherrin («Inhaberin des Geheimnisses»), die Kontrolle über die Offenbarung ihres Geheimnisses gegenüber Dritten zu behalten.[30] Gemäss Art. 321 Ziff. 1 StGB macht sich eine Täterin strafbar, wenn sie ein Geheimnis offenbart, das ihr infolge ihres Berufes anvertraut wurde oder das sie im Rahmen der Berufsausübung wahrgenommen hat. Art. 321 StGB ist sowohl ein Antrags- als auch ein Erfolgsdelikt. Voraussetzung für die Strafbarkeit bei einem Erfolgsdelikt ist, dass eine unberechtigte Person tatsächlich Kenntnis vom Geheimnis erlangt hat, die blosse Möglichkeit zur Kenntnisnahme genügt nicht.[31]

3.2.1.1 Geheimnis

Ein Geheimnis im Sinne von Art. 321 Ziff. 1 StGB liegt vor, wenn eine Tatsache oder Information nur einem beschränkten Personenkreis bekannt ist und die Geheimnisherrin ein berechtigtes Interesse an der Geheimhaltung der entsprechenden Tatsache hat.[32] Dabei wird der Begriff des Geheimnisses weit verstanden.[33] So definiert auch das Bundesgericht weit: «Geheimnis im Sinne dieser Bestimmung ist alles, was der Patient dem Arzt zwecks Ausführung des Auftrags anvertraut oder was der Arzt in Ausübung seines Berufes wahrnimmt».[34]

---

[22] BSK DSG-Bühler/Rampini, Art. 9 Rz. 8.

[23] BSK DSG-Bühler/Rampini, Art. 9 Rz. 8.

[24] BSK DSG-Bühler/Rampini, Art. 9 Rz. 8; vgl. auch Husi-Stämpfli/Morand, Rz. 148.

[25] Hürlimann/Steiger, S. 201; Sury /Gogniat, S. 204.

[26] Husi-Stämpfli/Morand, Rz. 147; Hürlimann/Steiger, S. 201.

[27] Husi-Stämpfli/Morand, Rz. 153.

[28] Husi-Stämpfli/Morand, Rz. 153.

[29] Husi-Stämpfli/Morand, Rz. 153.

[30] Schwarzenegger/Thouvenin /Stiller, S. 20.

[31] Hürlimann/Steiger, S. 203.

[32] BSK StGB-Oberholzer, Art. 321 Rz. 14.

[33] PK StGB-Trechsel/Vest, Art. 321 Rz. 20.

[34] BGE 101 Ia 10, E. 5c.

Dem Berufsgeheimnis unterstehen somit nicht bloss solche Tatsachen, die für die berufliche Erfüllung der Schweigepflichtigen von Bedeutung sind,[35] sondern auch persönliche und berufliche Informationen über sich und ihre Nächsten.[36] Die Geheimnishaltung erstreckt sich darüber hinaus bereits auf die Tatsache der Mandatsführung und die Art des Auftrages.[37]

Erforderlich ist, dass das Geheimnis der Geheimnisträgerin («Trägerin des Geheimnisses der Geheimnisherrin» z.B. Anwältin oder Ärztin) infolge ihres Berufes anvertraut wurde oder dass sie es in Ausübung ihres Berufes wahrgenommen hat, unabhängig davon, ob sie es direkt von der Geheimnisherrin oder von einer Dritten in Erfahrung gebracht hat.[38] Die Informationen müssen der Geheimnisträgerin somit nicht bewusst mitgeteilt oder übergeben worden sein.[39] Entscheidend ist der kausale Zusammenhang zwischen Kenntnisnahme und Berufsausübung.[40]

Abgrenzungsschwierigkeiten ergeben sich dann, wenn Anwältinnen Aufgaben erfüllen, die über den berufsspezifischen Tätigkeitsbereich einer Anwältin hinausgehen. Dies ist zum Beispiel dann der Fall, wenn eine Anwältin als Verwaltungsrätin oder Vermögensverwalterin tätig ist.[41] In diesen Fällen gilt das Berufsgeheimnis nur, wenn das Geheimnis der Anwältin in Erfüllung einer Aufgabe anvertraut wurde oder sie dieses im Rahmen der Aufgabenerfüllung wahrgenommen hat, die zu den typischen Aufgaben einer Anwältin zählen.[42] Überwiegt das kaufmännische Element, sodass die Tätigkeit nicht mehr der Ausübung des Anwaltsberufes zugeordnet werden kann, fallen die dabei erworbenen Kenntnisse nicht unter das Berufsgeheimnis.[43]

Auch Tatsachen, die die Berufsangehörige privat erfahren hat, werden nicht als Geheimnisse im Sinne von Art. 321 Ziff. 1 StGB qualifiziert.[44] Dasselbe gilt für Tatsachen, die allgemein bekannt sind, sodass die Geheimnisherrin von vornherein kein Interesse daran haben kann, sie gegenüber Dritten geheim zu halten.[45]

Nicht tatbestandsmässig ist das Weitergeben von anonymisierten Informationen, bei denen die Geheimnisherrin nicht mehr identifiziert werden kann.[46]

3.2.1.2 Täter

Der Straftatbestand der Verletzung des Berufsgeheimnisses ist ein sogenanntes echtes Sonderdelikt.[47] Täterin dieses Deliktes kann nur diejenige Person sein, die einen der in Art. 321 Ziff. 1 StGB abschliessend aufgezählten Berufe ausübt.[48]

Sie umfasst folgende Berufsangehörige: Geistliche, Rechtsanwältinnen, Verteidigerinnen, Notarinnen, Patentanwältinnen, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisorinnen, Ärztinnen, Zahnärztinnen, Chiropraktikerinnen, Apothekerinnen, Hebammen, Psychologinnen, Pflegefachpersonen, Physiotherapeutinnen, Ergotherapeutinnen, Ernährungsberaterinnen, Optometristinnen, Osteopathinnen sowie ihre Hilfspersonen.[49]

---

[35] DONATSCH/THOMMEN/WOHLERS, S. 591.

[36] PK StGB-TRECHSEL/VEST, Art. 321 Rz. 20.

[37] WALTERS, Rz. 546.

[38] BSK StGB-OBERHOLZER, Art. 321 Rz. 16.

[39] SCHWARZENEGGER/THOUVENIN /STILLER, S. 22.

[40] Vgl. BGE 115 Ia 197, E 3c.

[41] WALTERS, Rz. 548.

[42] WALTERS, Rz. 548.

[43] WALTERS, Rz. 548, vgl. auch BSK StGB-OBERHOLZER, Art. 321 Rz. 17.

[44] BSK StGB-OBERHOLZER, Art. 321 Rz. 15.

[45] BSK StGB-OBERHOLZER, Art. 321 Rz. 15.

[46] HK- StGB- WOHLERS, Rz. 13.

[47] BSK StGB-OBERHOLZER, Art. 321 Rz. 4.

[48] BSK StGB-OBERHOLZER, Art. 321 Rz. 4.

[49] Zu den einzelnen Berufsgruppen siehe BSK StGB-OBERHOLZER, Art. 321 Rz. 5 ff.

Ihnen gleichgestellt werden nach Art. 321 Ziff. 1 Abs. 2 StGB Studierende, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrgenommen haben.

Zur Kategorie der Rechtsanwältinnen zählen Inhaberinnen eines kantonalen schweizerischen oder ausländischen Fähigkeitsausweises, unabhängig davon, ob sie im anwaltlichen Monopolbereich tätig oder in einem kantonalen Anwaltsregister eingetragen sind.[50] Es ist umstritten, ob Art. 321 StGB nur für selbständige Anwältinnen im Sinne von Art. 12 Bst. b BGFA oder auch für Unternehmensjuristen mit Anwaltspatent (unselbständige Anwältinnen) anwendbar ist.[51]

3.2.1.3 Hilfsperson

Hilfspersonen unterstehen der Geheimhaltungspflicht wie die Geheimnisträgerin selbst (Art. 321 Ziff. 1 StGB), sofern sie unter deren Leitung und Aufsicht tätig werden.[52] Eine Hilfsperson ist «wer bei der Berufstätigkeit eines der genannten (Haupt-)Geheimnisträgers in der Weise mitwirkt, dass er grundsätzlich von den dabei wahrgenommenen Tatsachen ebenfalls Kenntnis erhält».[53]

Hilfspersonen müssen nicht notwendigerweise in einem Arbeitsverhältnis mit der Geheimnisträgerin stehen, sie können ihre Unterstützungstätigkeiten auch ausserhalb der Büroräumlichkeiten der Geheimnisträgerin erbringen.[54] Somit ist nicht ihre Stellung entscheidend, sondern dass die Hilfsperson die Geheimnisträgerin bei der Erfüllung ihrer Tätigkeiten unterstützt und dabei Kenntnis von Geheimnissen einer betreuten Person erlangt.[55]

Lehre und Rechtsprechung zählen unter anderem folgende Personen zu den Hilfspersonen: Sekretariatspersonal, Buchhalterinnen, Praktikantinnen, Assistenz- und Pflegepersonal, medizinische Fachangestellte, Laborangestellte,[56] IT-Techniker[57] sowie Mitarbeitende im Reinigungsdienst oder in der Telefonzentrale und weiteres Kanzleipersonal, sofern sie unter Leitung der zur Geheimhaltung verpflichteten Berufsangehörigen tätig werden.[58]

Auch das Wartungspersonal für technische Einrichtungen kann als Hilfsperson qualifiziert werden.[59] Entscheidend ist hierbei, ob das Wartungspersonal in dieser Funktion Kenntnis von Informationen über die Geheimnisherrin erhalten kann.[60] Heutzutage stellt auch in Anwaltskanzleien der IT-Support eine zentrale Hilfsfunktion bei der digitalen Informationsverarbeitung und Dokumentenverwaltung dar.[61] IT-Spezialistinnen (im Auftrags- oder Anstellungsverhältnis) sowie Mitarbeitende einer IT-Providerin, die eine Anwältin bei der Dokumentenverwaltung und -archivierung sowie bei der Softwarebedienung unterstützen, gelangen zwangsläufig in Kenntnis von Geheimnissen.[62]

Nach der grammatikalischen Auslegung sind Hilfspersonen Personen, die eine andere Person bei der Ausführung einer Aufgabe unterstützen.[63] Unter diesen Begriff können somit auch IT-Dienstleisterinnen, die für die Geheimnisträgerin Daten bearbeiten, gefasst werden.[64]

---

[50] BSK StGB-Oberholzer, Art. 321 Rz. 6.

[51] BSK StGB-Oberholzer, Art. 321 Rz. 6.

[52] BSK StGB-Oberholzer, Art. 321 Rz. 10.

[53] PK StGB-Trechsel/Vest, Art. 321 Rz. 13.

[54] Schwarzenegger/Thouvenin /Stiller, S. 40.

[55] BSK StGB-Oberholzer, Art. 321 Rz. 10.

[56] BSK StGB-Oberholzer, Art. 321 Rz. 10 m.w.N.

[57] Graf/Vonwill, StGB Annotierter Kommentar, Art. 321 Rz. 12.

[58] PK StGB-Trechsel/Vest, Art. 321 Rz. 13.

[59] Schwarzenegger/Thouvenin /Stiller, S. 23; HK StGB- Wohlers, Art. 321 Rz. 7; PK StGB-Trechsel/Vest, Art. 321 Rz. 13.

[60] Schwarzenegger/Thouvenin /Stiller, S. 23.

[61] Schwarzenegger/Thouvenin /Stiller, S. 23.

[62] Schwarzenegger/Thouvenin /Stiller, S. 23.

[63] Schwarzenegger/Thouvenin/Stiller/George, S. 28.

[64] Schwarzenegger/Thouvenin/Stiller/George, S. 28; Schwarzenegger/Thouvenin /Stiller, S. 39-40.

Zudem ergibt sich sowohl aus der systematischen als auch aus der historischen und teleologischen Auslegung, dass der Begriff der Hilfsperson weit zu verstehen ist.[65]

Folglich werden IT-Spezialistinnen (im Auftrags- oder Anstellungsverhältnis) sowie Mitarbeitende einer Cloud-Providerin, die IT-Infrastrukturen oder Applikationen als Dienstleistungen anbieten, mehrheitlich als Hilfspersonen von Anwältinnen im Sinne von Art. 321 Ziff. 1 StGB qualifiziert.[66]

3.2.1.4 Offenbarung

Die Tathandlung bei der Verletzung des Berufsgeheimnisses liegt in der Offenbarung des Geheimnisses. Dies ist dann der Fall, wenn die Geheimnisträgerin das Geheimnis einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht.[67]

Keine Offenbarung des Geheimnisses liegt hingegen vor, wenn diese zur Erfüllung des erteilten Auftrages sachlich gerechtfertigt ist.[68] Dies ist insbesondere der Fall bei arbeitsteiligen Organisationsstrukturen.[69] Dementsprechend gelten Hilfspersonen nicht als Drittpersonen, sondern gehören zum inneren Kreis der arbeitsteiligen Organisation der Geheimnisträgerin, womit gegenüber Hilfspersonen keine Geheimnisse offenbart werden können,[70] da sie Teil der gleichen Verantwortungssphäre der Geheimnisträgerin werden.[71]

Innerhalb des Verhältnisses zwischen der primären Geheimnisträgerin und der Hilfsperson dürfen geschützte Daten somit ungehindert fliessen, ohne dass dabei eine Verletzung von Art. 321 StGB anzunehmen ist, zumal Hilfspersonen ebenso von der Geheimhaltungspflicht erfasst sind wie die Geheimnisträgerin selbst.[72]

Unbeachtlich ist, auf welchem Weg die Offenbarung geschieht, dabei kann es sich um eine direkte Weiterleitung von geheimhaltungspflichtigen Unterlagen oder Informationen handeln, es genügt jedoch auch eine unzureichende Aufbewahrung von Akten, wenn die Täterin hierbei zumindest in Kauf nimmt, dass eine Aussenstehende sich Einsicht verschaffen kann.[73]

Ein Geheimnis wird auch dann offenbart, wenn die Empfängerin dieses bereits kennt oder vermutet, da dadurch ihre unsicheren oder unvollständigen Kenntnisse ergänzt oder verstärkt werden.[74]

Sind die Daten hingegen anonymisiert oder verschlüsselt und deren Inhalt nicht feststellbar, liegt keine Offenbarung vor, auch dann nicht, wenn aussenstehende Dritte die Daten zur Kenntnis nehmen können.[75]

Anderer Meinung ist WOHLERS, der die Ansicht vertritt, dass aus der Tatsache, dass Hilfspersonen als taugliche Täter aufgelistet werden, nicht gefolgert werden kann, dass auch die Weitergabe an sie für die primäre Geheimnisträgerin straflos sein soll.[76] Die Einstufung einer Person als Hilfsperson ändert nach WOHLERS somit nichts daran, dass die Weitergabe der Daten an diese als Offenbarung eines Geheimnisses einzustufen ist.[77]

---

[65] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 28.

[66] SCHWARZENEGGER/THOUVENIN /STILLER, S. 23 und 40; SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 29; CASANOVA, S. 49; HÜRLIMANN/STEIGER, S. 203; SURY /GOGNIAT, S. 203; A.M. WOHLERS, Outsourcing durch Berufsgeheimnisträger, S. 117.

[67] BSK StGB-OBERHOLZER, Art. 321 Rz. 19.

[68] BSK StGB-OBERHOLZER, Art. 321 Rz. 20; BGE 75 IV 71, S. 74; vgl. PK-StGB, TRECHSEL/VEST, Art. 321 Rz 23.

[69] BSK StGB-OBERHOLZER, Art. 321 Rz. 20.

[70] SCHWARZENEGGER/THOUVENIN /STILLER, S. 29; SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 29; BSK StGB-OBERHOLZER, Art. 321 Rz. 20.

[71] SCHWARZENEGGER/THOUVENIN /STILLER, S. 29; vgl. PK-StGB, TRECHSEL/VEST, Art. 321 Rz 23.

[72] BezGer Zürich, Urteil vom 18. November 2015, GG 150233, E. II.2.5.3.

[73] BSK StGB-OBERHOLZER, Art. 321 Rz. 19.

[74] BGE 75 IV 71, E. 2.

[75] PK-StGB, TRECHSEL/VEST, Art. 321 Rz 23.

[76] WOHLERS, Auslegung einer Datenbearbeitung und Berufsgeheimnis, S. 25.

[77] WOHLERS, Auslegung einer Datenbearbeitung und Berufsgeheimnis, S. 25.

3.2.1.5 Zeitliche Komponente

Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung der Berufsausübung oder des Studiums strafbar (Art. 321 Abs. 1 Ziff. 3 StGB). Die Pflicht zur Wahrung des Berufsgeheimnisses endet somit nicht mit der Beendigung des Mandats, sondern bleibt bis zum Tod der Geheimnisträgerin bestehen.[78]

3.2.1.6 Subjektiver Tatbestand

Strafbar ist, wer mit Vorsatz handelt, dabei genügt Eventualvorsatz. Die Täterin muss also in Kenntnis des Geheimnischarakters und im Wissen um ihre Schweigepflicht die Tatsache offenbaren oder dies zumindest in Kauf nehmen.[79]

Der subjektive Tatbestand ist vor allem dann von Relevanz, falls eine Hilfsperson ein Geheimnis offenbart, da sich dann die Frage stellt, ob auch die (Haupt-)Geheimnisträgerin strafbar sein kann.[80] Die Strafbarkeit wäre zu bejahen, wenn der (Haupt-)Geheimnisträgerin von Anfang an bekannt ist, oder es ihr für möglich erscheint, dass es zu einer Offenbarung durch die Hilfsperson kommen wird und der Erfolg in Kauf genommen wurde.[81] Meist wird dies jedoch nicht der Fall sein, sodass nur die Hilfsperson strafrechtlich zu Rechenschaft gezogen wird; die (Haupt-)Geheimnisträgerin kann aber allenfalls zivilrechtlich nach Art. 101 OR belangt werden.[82]

3.2.1.7 Rechtswidrigkeit

Gemäss Art. 321 Ziff. 2 StGB ist die Täterin nicht strafbar, wenn sie das Geheimnis auf Grund einer Einwilligung der Berechtigten oder einer auf Gesuch der Täterin erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat (sog. Gesuch um Entbindung).

Mit einer Einwilligung kann die Berechtigte auf den Schutz des Berufsgeheimnisses verzichten.[83] Die Berechtigte kann dabei die Informationen selbst verbreiten oder der Berufsträgerin erlauben, die Geheimnisse mit Dritten zu teilen.[84] Die auf Gesuch hin erteilte schriftliche Bewilligung der vorgesetzten Behörden oder Aufsichtsbehörden kann nur von der Geheimnisträgerin selbst gestellt werden und nicht von der Geheimnisherrin oder einer Drittperson.[85]

Vorbehalten bleiben auch die eidgenössischen und kantonalen Bestimmungen über die Melde- und Mitwirkungsrechte, über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde (Art. 321 Ziff. 3 StGB).

3.2.2 Verletzung der beruflichen Schweigepflicht nach Art. 62 DSG

Gemäss Art. 62 Abs. 1 DSG macht sich strafbar, wer vorsätzlich geheime Personendaten offenbart, die sie bei der Ausübung ihres Berufes erfahren hat, der die Kenntnis solcher Daten erfordert. Ebenfalls strafbar macht sich, wer vorsätzlich geheime Personendaten offenbart, die sie während der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser erfahren hat (Art. 62 Abs. 2 DSG). Dabei ist das Offenbaren geheimer Personendaten auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar (Art. 62 Abs. 3 DSG).

Gegenüber dem Berufsgeheimnis nach Art. 321 StGB wird das Datengeheimnis nach Art. 62 DSG in der Literatur auch als «Berufsgeheimnis für jedermann» bezeichnet.[86] Durch Art. 62 DSG sollen Lücken geschlossen werden, die durch den eingeschränkten Täterinnenkreis des Berufsgeheimnisses nach Art. 321 StGB bestehen, und die Schweigepflicht auch in weiteren Berufsbereichen statuieren, in denen der

---

[78] BGE 123 IV 75, E. 2a.

[79] BSK StGB-OBERHOLZER, Art. 321 Rz. 21.

[80] SCHWARZENEGGER/THOUVENIN /STILLER, S. 43.

[81] SCHWARZENEGGER/THOUVENIN /STILLER, S. 43.

[82] SCHWARZENEGGER/THOUVENIN /STILLER, S. 43.

[83] MICHLIG/WYLER, StGB Annotierter Kommentar, Art. 321 Rz. 19.

[84] BGE 131 I 223, E. 4.5.6.

[85] BSK StGB-OBERHOLZER, Art. 321 Rz. 23.

[86] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 1.

Schutz der Vertraulichkeit genauso unerlässlich ist.[87] Anders als bei der Berufsgeheimnispflicht nach Art. 321 StGB wird bei Art. 62 DSG nämlich keine bestimmte Berufszugehörigkeit für die Tätereigenschaft gefordert, sondern es genügt, dass die Täterin die betreffende Tatsache im Rahmen der Berufsausübung erfahren hat.[88] Täterin ist nach Art. 62 DSG die Berufsausübende selbst sowie ihre Hilfspersonen,[89] zu welchen auch die Auftragsbearbeiterin nach Art. 9 DSG zählt.[90] Art. 62 DSG beschränkt sich nicht nur auf Privatpersonen, sondern umfasst auch Bundesorgane.[91]

Strafbar ist gemäss Art. 62 DSG das Offenbaren geheimer Personendaten. Der Begriff des Offenbarens entspricht demjenigen nach Art. 321 StGB.[92] Somit wird ein Geheimnis offenbart, wenn die Geheimhaltungspflichtige es einer dazu nicht ermächtigten Dritten zur Kenntnis bringt oder ihr die Kenntnisnahme ermöglicht.[93] Auf den Weg der Offenbarung kommt es nicht an.[94] Auch Art. 62 DSG setzt voraus, dass die unberechtigte Dritte vom Geheimnis Kenntnis erlangt hat, um die Tat zu vollenden.[95] Hilfspersonen, darunter auch die Auftragsbearbeiterin, gelten nicht als unberechtigte Dritte,[96] da sie Teil der arbeitsteiligen Organisation der Geheimnisträgerin sind und gemäss Art. 62 DSG der gleichen Strafdrohung wie die (Haupt-)Geheimnisträgerin unterstehen, für die sie tätig sind.[97]

Das Tatobjekt nach Art. 62 DSG sind Personendaten gemäss Art. 5 lit. a DSG.[98] Keine Personendaten sind anonymisierte Daten.[99] Strafbar ist jedoch nur das Offenbaren *geheimer* Personendaten. Tatsachen sind dann geheim, wenn sie nicht allgemein bekannt oder zugänglich sind, wenn die Geheimnisträgerin objektiv ein schutzwürdiges Interesse an der beschränkten Bekanntheit hat und wenn sie die Daten subjektiv geheim halten will.[100] Dies entspricht den Vorgaben von Art. 321 StGB.[101]

Sodann setzt Art. 62 DSG einen zweifachen Zusammenhang mit der Berufsausübung voraus:[102] Erstens macht sich nur strafbar, wer von den geheimen Personendaten «bei der Ausübung ihres Berufes … Kenntnis erlangt hat»; zweitens muss «die Kenntnisnahme solcher Daten» vom betreffenden Beruf «erfordert» sein. Somit werden Vertrauensbrüche ausserhalb dieser Berufssphäre nicht erfasst.[103] Art. 62 DSG ist aber nicht auf besonders vertrauenswürdige Berufe beschränkt.[104]

Zu berücksichtigen ist, dass das Offenbaren geheimer Personendaten auch nach Beendigung der Berufsausübung oder Ausbildung strafbar ist (Art. 62 Abs. 3 DSG).

Zuletzt kann Art. 62 DSG nur durch vorsätzliches Handeln verletzt werden, wobei Eventualvorsatz genügt.[105] Auch bei der Verletzung von Art. 62 DSG können Rechtfertigungsgründe wie die Einwilligung des Betroffenen vorliegen.[106]

---

[87] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 2.

[88] PK-StGB, TRECHSEL/VEST, Art. 321 Rz. 16.

[89] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 14.

[90] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 15.

[91] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 17.

[92] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[93] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[94] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[95] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 20.

[96] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 22.

[97] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 22.

[98] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 24.

[99] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 24.

[100] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 26.

[101] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 26.

[102] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 32.

[103] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 32.

[104] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 34.

[105] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 39.

[106] Vgl. dazu BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 42 ff.

3.3 Das Berufsgeheimnis nach Art. 13 BGFA

Gemäss Art. 13 des Bundesgesetzes über die Freizügigkeit der Anwältinnen und Anwälte (BGFA)[107] unterstehen Anwältinnen zeitlich unbegrenzt und gegenüber jedermann dem Berufsgeheimnis über alles, was ihnen infolge ihres Berufes von ihrer Klientschaft anvertraut worden ist. Der Begriff des Berufsgeheimnisses nach Art. 13 BGFA deckt sich mit dem Geheimnisbegriff von Art. 321 StGB.[108] Erforderlich ist demnach, dass die Tatsache weder offenkundig noch allgemein zugänglich ist und dass ein berechtigtes Geheimhaltungsinteresse der Geheimnisherrin sowie deren Geheimniswillen vorliegt.[109] Art. 13 BGFA umfasst Geheimnisse, die die Klientin der Anwältin infolge ihres Berufes anvertraut sowie Geheimnisse, die die Anwältin infolge ihres Berufes wahrnimmt.[110] Des Weiteren wird auf die Ausführungen in Kapitel 4.2.1.1 verwiesen.

Das BGFA und somit die Bestimmung zum Berufsgeheimnis nach Art. 13 BGFA gilt für Personen, die über ein Anwaltspatent verfügen und in der Schweiz im Rahmen des Anwaltsmonopols Parteien vor Gericht vertreten (Art. 2 Abs. 1 BGFA).[111] Entgegen dem Wortlaut von Art. 2 Abs. 1 BGFA werden auch Anwältinnen von diesem Gesetz erfasst, die im Anwaltsregister eingetragen sind und nur beratend tätig sind.[112] Hingegen findet das BGFA, unter Vorbehalt kantonaler Regelungen, auf schweizerische Anwältinnen und Anwälte, die lediglich beratend tätig sind und nicht im Anwaltsregister eingetragen sind, keine Anwendung.[113]

Zu beachten ist, dass der Adressatenkreis von Art. 13 BGFA und Art. 321 StGB nicht deckungsgleich ist.[114] Wobei es umstritten ist, ob Art. 321 StGB auch für sogenannte Unternehmensjuristinnen anwendbar ist.[115]

Anwältinnen haben zudem für die Wahrung des Berufsgeheimnisses durch ihre Hilfspersonen zu sorgen, was sich aus Art. 13 Abs. 2 BGFA sowie Art. 101 OR ergibt.[116] Nach Art. 101 OR haften Anwältinnen für alle in Erfüllung der Schuldpflicht durch die Hilfsperson verursachten Schäden, soweit ihnen diese hypothetisch vorwerfbar wären,[117] das heisst, wenn ihnen bei gleichem Verhalten wie der Hilfsperson eine Pflichtverletzung vorgeworfen werden könnte.[118] Von der Schadenersatzpflicht kann sich nur befreien, wer nachweist, dass ihr bei gleichem Handeln kein Verschulden vorgeworfen werden kann und die Hilfsperson somit die Sorgfalt ausgeübt hat, zu welcher sie selbst verpflichtet war.[119] Daher ist bereits bei der Auswahl der Hilfsperson eine gewisse Sorgfalt zu wahren.[120]

Im Gegensatz zu Art. 321 StGB, der auch Hilfspersonen selbst als Normadressatinnen erfasst, richtet sich Art. 13 BGFA ausschliesslich an Anwältinnen; die Hilfspersonen können somit nicht aufsichtsrechtlich diszipliniert werden.[121] Beim Begriff der Hilfsperson nach Art. 13 Abs. 2 BGFA ist von einem weit

---

[107] SR 935.61 Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (BGFA).

[108] WALTER, Rz. 614.

[109] WALTER, Rz. 614.

[110] WALTER, Rz. 615.

[111] Faktisch setzt dies einen Eintrag in ein kantonales Anwaltsregister voraus, da nur in seltenen Fällen Personen Parteien vor Gerichtsbehörden vertreten, die nicht in einem Anwaltsregister eingetragen sind, siehe hierzu: NATER, Kommentar zum Anwaltsgesetz, Art. 2 Rz. 2.

[112] WALTER, Rz. 105.

[113] WALTER, Rz. 104.

[114] NATER/ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 29.

[115] Siehe hierzu Kapitel 4.2.1.2 «Täter».

[116] SURY /GOGNIAT, S. 203; BBl 1999 6013, 6056; Vgl. SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 29.

[117] SCHWARZENEGGER/THOUVENIN /STILLER, S. 36; SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 29; BBl 1999 6013, 6056, SURY /GOGNIAT, S. 203.

[118] TARKAN, Präjudizienbuch OR, Art. 101, Rz. 3.m.w.H.

[119] TARKAN, Präjudizienbuch OR, Art. 101, Rz. 3.m.w.H.

[120] SCHWARZENEGGER/THOUVENIN /STILLER, S. 38; SAV-Wegleitung für IT-Outsourcing und Cloud-Computing, S. 3.

[121] NATER/ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 49.

gefassten Verständnis der Hilfsperson auszugehen.[122] Hilfspersonen nach Art. 13 Abs. 2 BGFA sind nicht nur Hilfskräfte, die unmittelbar bei der Mandatserfüllung unterstützen und deren Tätigkeit in einem direkten Zusammenhang mit der Berufsausübung der Anwältin steht,[123] sondern beispielsweise auch Personen die zur Aufrechterhaltung der Infrastruktur des Dienstleistungsbetriebs beigezogen wurden.[124] Somit sind Hilfspersonen nach Art. 13 Abs. 2 BGFA alle Personen, die die Anwältin zur Unterstützung ihrer Berufstätigkeit beizieht und die im Zusammenhang mit dieser Tätigkeit einen Zugang zu Mandatsinformationen haben.[125] Dabei muss kein direkter Sachzusammenhang zur eigentlichen Berufstätigkeit bestehen, massgebend ist vielmehr, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu Mandatsinformationen einschliesst.[126]

Die Pflicht der Anwältinnen für die Wahrung des Berufsgeheimnisses durch ihre Hilfspersonen zu sorgen, verlangt auch, die Kanzlei so zu organisieren, dass die dem Berufsgeheimnis unterstehenden Informationen kanzleiweit geschützt sind.[127] Dazu gehören unter anderem die Instruktion, mandatsbezogene Informationen strikt geheim zu halten, und von den Hilfspersonen, vor der Aufnahme ihrer Tätigkeit, eine Verschwiegenheitspflicht vertraglich zu vereinbaren.[128] Je nach Grösse und Tätigkeit der Kanzlei kann aber auch ein eigentliches Sicherheitsdispositiv erforderlich sein.[129] Beispielsweise durch das Schlüsselmanagement, das bei IaaS Service-Modellen grundsätzlich in der Verantwortung der Kanzlei bleibt oder Zugangskontrollen bei IaaS und Saas Service-Modellen.[130] Zudem muss die Anwältin die Einhaltung der angeordneten Massnahmen überwachen.[131]

Das Berufsgeheimnis nach Art. 13 BGFA wird bereits verletzt, wenn eine Anwältin die Wahrung des Berufsgeheimnisses ernsthaft gefährdet (im Gegensatz zu Art. 321 StGB, bei welchem eine Offenbarung benötigt wird).[132] Dies ergibt sich aus Art. 13 Abs. 2 BGFA, wonach Anwältinnen präventiv für die Wahrung des Berufsgeheimnisses durch ihre Hilfspersonen zu sorgen haben.[133]

Das Berufsgeheimnis nach Art. 13 BGFA kann im Gegensatz zu Art. 321 StGB fahrlässig verletzt werden.[134] Eine Fahrlässigkeit liegt in Anlehnung an Art. 12 Abs. 3 StGB demnach vor, wenn eine Anwältin die Folgen ihres Verhaltens aus pflichtwidriger Unvorsichtigkeit nicht bedacht oder darauf keine Rücksicht genommen hat.[135] Dabei ist eine Unvorsichtigkeit pflichtwidrig, wenn die Anwältin die gebotene Sorgfalt nicht beachtet hat, zu der sie nach den Umständen und nach ihrer Stellung als Anwältin verpflichtet war.[136] Anders als beim Fahrlässigkeitsmassstab nach Art. 12 Abs. 3 StGB gilt im Disziplinarrecht ein objektiver Massstab womit diejenige fahrlässig handelt, die die durchschnittliche Sorgfalt missachtet, welche von jeder Anwältin in guten Treuen verlangt werden darf und muss.[137]

Das Berufsgeheimnis nach Art. 13 BGFA bleibt, wie das Berufsgeheimnis nach Art. 321 StGB, auch nach Beendigung des Mandats bestehen. Gemäss dem Wortlaut von Art. 13 BGFA unterstehen Anwältinnen

---

[122] NATER/ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[123] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[124] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[125] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[126] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 53.

[127] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56.

[128] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56; BGE 145 II 229, E. 7.6; SCHILLER, Rz. 541.

[129] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56.

[130] SCHWARZENEGGER/THOUVENIN /STILLER, S. 36 in Fn. 87.

[131] NATER/GAUDEZ, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 57.

[132] WALTER, Rz. 626; zu beachten ist hier jedoch, dass eine Offenbarung auch gegeben ist, wenn die Geheimnisträgerin das Geheimnis einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht (BSK StGB-OBERHOLZER, Art. 321 Rz. 19).

[133] WALTER, Rz. 627.

[134] WALTER, Rz. 630.

[135] WALTER, Rz. 630.

[136] WALTER, Rz. 630.

[137] WALTER, Rz. 630.

dem Berufsgeheimnis «zeitlich unbegrenzt». Weder der Tod der Klientin noch die Berufsaufgabe der Anwältin hebt dieses auf.[138]

3.4 Systematischer Vergleich von Art. 321 StGB, Art. 62 DSG und Art. 13 BGFA

Dieser Abschnitt vergleicht Art. 321 StGB, Art. 62 DSG und Art. 13 BGFA, um die zentralen Gemeinsamkeiten und Unterschiede der Normen auf einen Blick darzustellen.

Berufsgeheimnis und berufliche Schweigepflicht			
	Art. 321 StGB	**Art. 62 DSG**	**Art. 13 BGFA**
Täterin/ Persönlicher Geltungsbereich	**Täterin**: Wer einen der in Art. 321 Ziff. 1 StGB abschliessend aufgezählten Berufe praktiziert. Dazu zählen Anwältinnen, die Inhaberinnen eines kantonalen schweizerischen oder ausländischen Fähigkeitsausweises sind, unabhängig davon, ob sie im anwaltlichen Monopolbereich tätig oder in einem kantonalen Anwaltsregister eingetragen sind.[139] Auch erfasst werden ihre Hilfspersonen. Umstritten ist, ob Unternehmensjuristinnen mit Anwaltspatent erfasst werden.[140] *(Kapitel 4.2.1.2 und 4.2.1.3)*	**Täterin**: Wer einen Beruf ausübt (Berufsausübende) sowie ihre Hilfspersonen.[141] *(Kapitel 4.2.2)*	**Subjektiver Anwendungsbereich:** Erfasst werden Anwältinnen, also Personen, die über ein Anwaltspatent verfügen und in der Schweiz im Rahmen des Anwaltsmonopols Parteien vor Gericht vertreten oder auch nur beratend tätig sind.[142] Keine Anwendung findet das BGFA auf sog. Unternehmensjuristinnen. Art. 13 BGFA richtet sich nicht an die Hilfspersonen. Anwältinnen müssen aber für die Wahrung des Berufsgeheimnisses durch ihre Hilfspersonen sorgen. *(Kapitel 4.3)*

[138] WALTER, Rz. 625.

[139] BSK StGB-OBERHOLZER, Art. 321 Rz. 6.

[140] BSK StGB-OBERHOLZER, Art. 321 Rz. 6.

[141] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 14.

[142] NATER/ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 26.

Berufsgeheimnis und berufliche Schweigepflicht			
	Art. 321 StGB	**Art. 62 DSG**	**Art. 13 BGFA**
Tatobjekt und Tathandlung/ Sachlicher Geltungsbereich	**Tatobjekt**: Geheimnis, das der Geheimnisträgerin infolge ihres Berufes anvertraut wurde. Ein Geheimnis liegt vor, wenn eine Tatsache nur einem beschränkten Personenkreis bekannt ist und die Geheimnisherrin ein berechtigtes Interesse an der Geheimhaltung der entsprechenden Tatsache hat.[143] *(Kapitel 4.2.1.1)* **Tathandlung**: Offenbarung des Geheimnisses, d.h. wenn die Geheimnisträgerin das Geheimnis einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht.[144] *(Kapitel 4.2.1.4)* **Erfolg**: Kenntnisnahme des Geheimnisses durch unberechtigte Dritte. *(Kapitel 4.2.1)*	**Tatobjekt**: Geheime Personendaten, die nicht allgemein bekannt oder zugänglich sind, bei denen die Geheimnisträgerin objektiv und subjektiv ein schutzwürdiges Interesse an deren Geheimhaltung hat.[145] Die Kenntnisnahme der geheimen Personendaten muss im Rahmen der Berufsausübung stattfinden und muss vom betreffenden Beruf erfordert werden.[146] *(Kapitel 4.2.2)* **Tathandlung**: Offenbarung der geheimen Personendaten. Gleiche Bedeutung wie bei Art. 321 StGB.[147] *(Kapitel 4.2.2)* **Erfolg**: Kenntnisnahme des Geheimnisses durch unberechtigte Dritte.[148] *(Kapitel 4.2.2)*	**Sachlicher Anwendungsbereich:** **Geheimnis**: deckungsgleich mit Art. 321 StGB. **Handlung**: Das Berufsgeheimnis nach Art. 13 BGFA wird bereits verletzt, wenn eine Anwältin die Wahrung des Berufsgeheimnisses ernsthaft gefährdet.[149] **Erfolg:** Es wird kein Erfolg vorausgesetzt. *(Kapitel 4.3)*
Zeitlicher Geltungsbereich	Die Berufsgeheimnispflicht gilt auch nach Beendigung der Berufsausübung (Art. 321 Abs. 1 Ziff. 3 StGB). Also bis zum Tode der Geheimnisträgerin.[150] *(Kapitel 4.2.1.5)*	Die Offenbarung geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder Ausbildung strafbar (Art. 62 Abs. 3 DSG). *(Kapitel 4.2.2)*	Das Berufsgeheimnis bleibt nach Beendigung des Mandats bestehen. Weder Tod der Klientin noch die Berufsaufgabe der Anwältin heben es auf.[151] *(Kapitel 4.3)*
Subjektiver Tatbestand/ **Verschulden**	Strafbar ist, wer mit Vorsatz handelt, dabei genügt Eventualvorsatz. *(Kapitel 4.2.1.6)*	Strafbar ist, wer mit Vorsatz handelt, dabei genügt Eventualvorsatz. *(Kapitel 4.2.2)*	Fahrlässige Verletzung möglich.[152] *(Kapitel 4.3)*

[143] BSK StGB-OBERHOLZER, Art. 321 Rz. 14.

[144] BSK StGB-OBERHOLZER, Art. 321 Rz. 19.

[145] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 26.

[146] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 32.

[147] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[148] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[149] WALTER, Rz. 626.

[150] BGE 123 IV 75, E. 2a.

[151] WALTER, Rz. 625.

[152] NATER/ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 195.

Hilfsperson und Auftragsbearbeiterin			
	Hilfsperson Art. 321 StGB	**Hilfsperson Art. 13 BGFA**	**Auftragsbearbeiterin Art. 9 DSG**
Persönlicher und sachlicher Geltungsbereich	Eine Hilfsperson ist, «wer bei der Berufstätigkeit eines der genannten (Haupt-) Geheimnisträgers in der Weise mitwirkt, dass er grundsätzlich von den dabei wahrgenommenen Tatsachen ebenfalls Kenntnis erhält».[153] Somit genügt es, wenn die Hilfsperson die Geheimnisträgerin bei der Erfüllung ihrer Tätigkeiten unterstützt und dabei Kenntnis von Geheimnissen einer betreuten Person erlangt.[154] *(Kapitel 4.2.1.3)*	Hilfspersonen sind alle Personen, die die Anwältin zur Unterstützung ihrer Berufstätigkeit beizieht und die im Zusammenhang mit dieser Tätigkeit einen Zugang zu Mandatsinformationen haben.[155] Es muss keinen direkten Sachzusammenhang zur eigentlichen Berufstätigkeit bestehen, massgebend ist, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu Mandatsinformationen einschliesst.[156] *(Kapitel 4.3)*	Auftragsbearbeiterin ist eine private Person oder ein Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet (Art. 5 Bst. k DSG) *(Kapitel 4.1)*
Voraussetzungen	Die Hilfsperson muss die Berufsgeheimnisträgerin bei der Erfüllung ihrer Tätigkeit unterstützen und dabei Kenntnis von Geheimnissen einer betreuten Person erlangen.[157] Ein Arbeitsverhältnis zwischen der Geheimnisträgerin und der Hilfsperson ist nicht vorausgesetzt.[158] *(Kapitel 4.2.1.3)*	Anwältinnen müssen für die Wahrung des Berufsgeheimnisses durch ihre Hilfspersonen sorgen.[159] Dies erfasst auch die Instruktion, mandatsbezogene Informationen strikt geheim zu halten, dabei empfiehlt es sich mit den Hilfspersonen eine Verschwiegenheitspflicht vertraglich zu vereinbaren.[160] *(Kapitel 4.3)*	Die Voraussetzungen von Art. 9 Abs. 1 und 2 DSG müssen erfüllt werden. *(Kapitel 4.1)*
Strafbarkeit bzw. Haftung	Falls eine Hilfsperson ein Geheimnis offenbart, ist (Haupt-) Geheimnisträgerin nur dann strafbar, wenn ihr von Anfang an bekannt ist, oder es ihr für möglich erscheint, dass es zu einer Offenbarung durch die Hilfsperson kommen wird und der Erfolg in Kauf genommen wurde.[161] Meist wird dies jedoch nicht der Fall sein, so dass nur die Hilfsperson strafrechtlich zu Rechenschaft gezogen wird; die (Haupt-)Geheimnisträgerin kann aber allenfalls nach Art. 101 OR zivilrechtlich belangt werden.[162] *(Kapitel 4.2.1.6)*	Anwältinnen haben für die Wahrung des Berufsgeheimnisses durch ihre Hilfspersonen zu sorgen.[163] Nach Art. 101 OR haften Anwältinnen für alle in Erfüllung der Schuldpflicht durch die Hilfsperson verursachten Schäden, soweit ihnen diese hypothetisch vorwerfbar sind.[164] Bereits bei der Auswahl der Hilfsperson ist eine gewisse Sorgfalt zu wahren.[165] Im Gegensatz zu Art. 321 StGB, richtet sich Art. 13 BGFA ausschliesslich an Anwältinnen. Hilfspersonen können nicht aufsichtsrechtlich diszipliniert werden.[166] *(Kapitel 4.3)*	Die Auftragsbearbeiterin wird datenschutzrechtlich der Verantwortlichen zugeordnet.[167] Die Verantwortliche muss sicherstellen, dass die Auftragsbearbeiterin die Daten nur so bearbeitet, wie die Verantwortliche es selbst tun dürfte (Art. 9 Abs. 1 lit. a DSG). *(Kapitel 4.1)*
Zeitlicher Geltungsbereich	Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung der Berufsausübung strafbar (Art. 321 Abs. 1 Ziff. 3 StGB). Die Pflicht zur Wahrung des Berufsgeheimnisses bleibt bis zum Tod der Geheimnisträgerin bestehen.[168] *(Kapitel 4.2.1.5)*	Gemäss Art. 13 BGFA unterstehen Anwältinnen dem Berufsgeheimnis «zeitlich unbegrenzt», somit auch nach Beendigung des Mandats. Weder der Tod des Klienten noch die Berufsaufgabe der Anwältin hebt dieses auf.[169] *(Kapitel 4.3)*	Gemäss gesetzlichen Bestimmungen oder Vertrag *(Kapitel 4.1)*

[153] PK StGB-Trechsel/Vest, Art. 321 Rz. 13.

[154] BSK StGB-Oberholzer, Art. 321 Rz. 10.

[155] Nater/ Zindel, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[156] Nater/ Zindel, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 53.

[157] BSK StGB-Oberholzer, Art. 321 Rz. 10.

[158] Schwarzenegger/Thouvenin /Stiller, S. 40.

[159] Nater/ Zindel, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56.

[160] Nater/ Zindel, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56; BGE 145 II 229, E. 7.6; Schiller, Rz. 541.

[161] Schwarzenegger/Thouvenin /Stiller, S. 43.

[162] Schwarzenegger/Thouvenin /Stiller, S. 43.

[163] Sury /Gogniat, S. 203; BBl 1999 6013, 6056; Vgl. Schwarzenegger/Thouvenin/Stiller/George, S. 29.

[164] Schwarzenegger/Thouvenin /Stiller, S. 36; Schwarzenegger/Thouvenin/Stiller/George, S. 29; BBl 1999 6013, 6056.

[165] Schwarzenegger/Thouvenin /Stiller, S. 38; SAV-Wegleitung für IT-Outsourcing und Cloud-Computing, S. 3.

[166] Nater/Zindel, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 49.

[167] Hürlimann/Steiger, S. 201; Sury/Gogniat, S. 204.

[168] BGE 123 IV 75, E. 2a.

[169] Walter, Rz. 625.

4 Umfang des KI-Prototyps

Dieses Kapitel erläutert den potenziellen Einsatz eines KI-Tools in einem KMU, das dem Berufsgeheimnis unterliegt. Die Anwendungsmöglichkeiten werden anhand von drei exemplarischen Anwendungsfällen (sog. Use Cases) dargestellt. Bei der Ausarbeitung der Use Cases lag der Fokus auf Einsatzmöglichkeiten in kleinen und mittleren Anwaltskanzleien.

Die Anwendungsfälle dienen als Grundlage für die Entwicklung des BFH-KI-Prototyps, einschliesslich der zusätzlichen Funktionen, die für die Umsetzung der Use Cases erforderlich sind (vgl. Kapitel 6).

Die Use Cases wurden in Zusammenarbeit mit der ERFA-Gruppe «KI-Tool für kleine(re) Anwaltskanzleien» des Bernischen Anwaltsverbands erstellt.

4.1 Use Cases

Der erste Anwendungsfall betrifft das Studium von Verfahrensakten im Rahmen der Akteneinsicht und damit verschiedene Fragestellungen und Aufgaben im Zusammenhang mit einem bestimmten Verfahren. Der zweite Anwendungsfall bezieht sich auf die Möglichkeit, in einer Dokumentenablage Fragen zu bestehenden Unterlagen zu stellen und mithilfe dieser Dokumente neue Dokumente zu erstellen. Der Dritte ausgearbeitet Anwendungsfall betrifft den Abgleich von Rechtsschriften.

Die drei ausgearbeiteten Use Cases wurden entsprechend ihrer Relevanz in drei Prioritätsstufen eingeteilt. Bei der Entwicklung des BFH-Prototyps konnte aufgrund der im Rahmen dieser Studie verfügbaren Ressourcen nur der Use Case mit Priorität 1 berücksichtigt werden.

4.1.1 Studium der Verfahrensakten (Priorität 1)

Als erste Priorität wurde das Studium der Verfahrensakten identifiziert.

Dabei soll das KI-Modell dazu dienen eine Übersicht über ein bestimmtes Verfahren zu erstellen sowie Verfahrensakten effizienter zu studieren. Die KI-Lösung sollte in der Lage sein, den Sachverhalt eines bestimmten Verfahrens zu erläutern und eine Zusammenfassung der Geschehnisse zu erstellen. Zudem sollte die KI-Lösung imstande sein, eine inhaltliche zeitliche Abfolge des bisherigen prozessualen Verfahrens zu erstellen. Auch soll es möglich sein, nach bestimmten Informationen in den Verfahrensakten zu suchen, oder die erbachten Beweismittel der jeweiligen Parteien aufzuzeigen.

Zudem soll die KI-Lösung die verschiedenen Verfahrensunterlagen nach deren Inhalte klassifizieren (beispielsweise: Rechtsschriften, Beweismittel usw.). Dabei soll das KI-Modell bei den generierten Antworten die verwendeten Quellen (Dokumente der Verfahrensakte) angeben.

4.1.2 Unterlagen- und Vorlagensammlung (Priorität 2)

Als zweite Priorität wurde die Suchfunktion innerhalb von Unterlagen- und Vorlagensammlungen festgelegt. Der Nutzerin soll es dabei möglich sein, Suchfragen zu verschiedenen Unterlagensammlungen zu stellen. Beispielsweise die Suche nach konkreten Vertragsklauseln. Auch hier soll das KI-Tool bei den generierten Antworten die verwendeten Quellen angeben.

Zudem soll die KI-Lösung, basierend auf den bestehenden Unterlagen- und Vorlagensammlungen, im Stande sein, neue Unterlagen zu generieren. Beispielsweise die Vorlage für einen neuen Erbvertrag oder Arbeitsvertrag.

4.1.3 Abgleich Rechtsschriften (Priorität 3)

Als dritte Priorität wurde der Abgleich von Rechtsschriften identifiziert. Dabei soll die KI-Lösung Klageschriften, Klageantworten, Repliken oder Dupliken miteinander vergleichen und aufzeigen, ob in der Klageantwort oder Duplik auf alles Bezug genommen wurde, was in der Klageschrift erläutert wurde und ob auf neue Tatsachen Bezug genommen wurde.

Dies ist vor allem im Hinblick auf das Novenrecht von Relevanz.

4.2 Benutzte Unterlagen

Für die Entwicklung des BFH-KI-Prototyps wurde darauf geachtet, Unterlagen unter Wahrung des Berufsgeheimnisses und unter Einhaltung datenschutzrechtlicher Vorschriften zu suchen und zu verwenden.

Um den jeweiligen Bestimmungen des Strafrechts, des Anwaltsrechts sowie des Datenschutzrechts gerecht zu werden, wurden für die jeweiligen Use Cases Unterlagen verwendet, die öffentlich zugänglich sind oder die keine Geheimnisse im Sinne von Art. 321 StGB oder Personendaten enthalten.

4.2.1 Studium der Verfahrensakten

Für den ersten Use Case, «Studium der Verfahrensakten», wurden Verfahrensunterlagen (Test-Datensätze) verwendet, die aus dem Gesamtband des Schweizerischen Bundesarchiv (1798-) stammen.[170]

Der erste «Test-Datensatz» besteht aus den Verfahrensunterlagen des Verfahrensdossier in der «Anklage gegen Max Leo Keller: Vorbereitungen zur Hauptverhandlung, Anklageschrift, Verteidigungsschrift, Vortrag, Urteil». Die Verfahrensunterlagen stammen aus dem Zeitraum 1941-1948 und sind im Gesamtband des Schweizerischen Bundesarchiv öffentlich einsehbar.[171]

Die einzelnen Dokumente wurden mit Titeln, die ihrem jeweiligen Inhalt entsprechen, versehen. Zudem wurden leere Seiten aus dem Dokumentensatz entfernt, um eine korrekte Seitenzählung sicherzustellen. Nicht entzifferbare oder handgeschriebene Dokumente wurden entsprechend gekennzeichnet.

Der zweite «Test-Datensatz» besteht ebenfalls aus Unterlagen aus dem Gesamtband des Schweizerischen Bundesarchiv mit dem Titel «Gefährdung der verfassungsmässigen Ordnung / Bändlistrasse, diverse einvernommene Personen / (0)202/199(Dossier)». Diese Unterlagen stammen aus dem Zeitraum 1972-1974 und sind ebenfalls öffentlich einsehbar.[172]

Als dritter «Test-Datensatz» wurde ein anonymisierter Musterfall aus der Praxis verwendet.

4.2.2 Unterlagen- und Vorlagensammlung

Für den zweiten Use Case «Unterlagen- und Vorlagensammlung» wurden für die Erstellung des «Test-Datensatzes» die Schlussberichte und Empfehlungen in Sachen Datenschutz[173] und Öffentlichkeitsgesetz (BGÖ)[174] des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB); sowie die Stellungnahmen zum Vernehmlassungsverfahren des Bundesgesetzes über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ)[175] zusammengetragen. Die zuletzt genannten Dokumente wurden zusätzlich mit einer Texterkennung (OCR) bearbeitet.

4.2.3 Abgleich Rechtsschriften

Für den dritten Use Case wurde das Rechtsschriftendossier zum Fall «Kernkraftwerk Graben AG» angedacht. Die Verfahrensunterlagen stammen aus dem Zeitraum 1990-1991 und sind im Gesamtband des Schweizerischen Bundesarchiv öffentlich einsehbar.[176]

---

[170] https://www.recherche.bar.admin.ch/recherche/recherche/#/de/archiv/einheit/1

[171] https://www.recherche.bar.admin.ch/recherche/recherche/#/de/archiv/einheit/1.

[172] https://www.recherche.bar.admin.ch/recherche/recherche/#/de/archiv/einheit/3595564

[173] https://www.edoeb.admin.ch/de/schlussberichte-empfehlungen-bis-31082023

[174] https://www.edoeb.admin.ch/de/empfehlungen-nach-bgo

[175] https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-kommunikation.html

[176] https://www.recherche.bar.admin.ch/recherche/recherche/#/de/archiv/einheit/30828001

5 KI-Tool: Open Source Prototyp

Dieses Kapitel erläutert, welche Technologien bei der Umsetzung des BFH-KI-Prototyps verwendet wurden, wie der Chatbot aufgebaut ist und über welche Features der Prototyp verfügt.

5.1 Verwendete Technologie

5.1.1 Software

Für die Benutzeroberfläche wurde das Python-Framework Chainlit[177] verwendet. Damit der Chatbot nur authentifizierten Benutzerinnen und Benutzern zur Verfügung steht, wurde ein Login-Mechanismus via OAuth mittels eines Authentik[178]-Servers, der auf einem Server des Digital Sustainability Labs (DSL) des IPST aufgesetzt wurde.

Die Logik, insbesondere für die Retrieval Augmented Generation (RAG), wurde grösstenteils in der Form von Haystack[179] Pipelines implementiert. Dabei wurde die Vektordatenbank Qdrant[180] verwendet, um die Textpassagen der einzelnen Dokumente und die entsprechenden Vektoren, welche die semantische Bedeutung dieser Passagen repräsentieren, zu speichern. Die Vektordatenbank wurde ebenfalls selbst auf einem Server des DSL betrieben. Für die Verarbeitung der Dokumente und die Unterteilung in einzelne Textpassagen wurde Docling[181] verwendet.

5.1.2 Sprachmodelle

Als Large Language Model (LLM), welches für die Generierung von Text zuständig ist, wurde das Modell `meta-llama/Llama-3.3-70B-Instruct-Turbo`[182] via Together AI[183] verwendet. Als Embedding-Modell diente `Qwen3-Embedding-0.6B`[184] ausgeführt über die DeepInfra-API[185]. Ausserdem wurde das Modell `Qwen3-Reranker-4B`[186] verwendet, um die Rangliste der gefundenen Textpassagen zu verfeinern. Dieses Modell wurde ebenfalls über die DeepInfra-API ausgeführt. Der Grund, warum die Modelle nicht lokal ausgeführt wurden, war die Auslastung unseres Servers mit anderen Experimenten. In der Praxis müssten diese Modelle selbst betrieben werden, was aber durchaus möglich ist, da wir nur offene Modelle verwendet haben, die wir bei Kapazität auch jederzeit auf unseren eigenen Servern betreiben können.

5.2 Architektur

In diesem Abschnitt gehen wir auf die Kernelemente der Architektur des Prototyps ein.

5.2.1 Ablauf einer Chatbot-Anfrage

Sobald die Benutzerin oder der Benutzer eingeloggt ist, kann der Chatbot direkt verwendet werden. Es kann entweder direkt eine Frage zu einer bestehenden Dokumentensammlung via Nachrichtenfeld gestellt werden, oder man kann einen der verfügbaren Befehle ausführen, mehr dazu in Abschnitt 6.3.

Im Falle einer Frage wird die RAG-Pipeline gestartet. Anhand der passendsten fünf Textpassagen, welche vom Chatbot gefunden wurden, generiert der Chatbot daraufhin eine Antwort auf die Frage. Es obliegt in der Verantwortung des LLMs, die verwendeten Quellen an den richtigen Stellen zu zitieren. Diese

---

[177] https://docs.chainlit.io/get-started/overview

[178] https://goauthentik.io/

[179] https://haystack.deepset.ai/

[180] https://qdrant.tech/

[181] https://docling-project.github.io/docling/

[182] https://huggingface.co/meta-llama/Llama-3.3-70B-Instruct

[183] https://www.together.ai/models/llama-3-70b-instruct-turbo

[184] https://huggingface.co/Qwen/Qwen3-Embedding-0.6B

[185] https://deepinfra.com/Qwen/Qwen3-Embedding-0.6B/api?example=openai-emb-py

[186] https://huggingface.co/Qwen/Qwen3-Reranker-4B

Zitate sind in der Benutzeroberfläche ersichtlich und mit einem Klick auf den Dateinamen öffnet sich eine Seitenleiste, in der sich das entsprechende PDF-Dokument betrachten lässt.

Standardmässig wird eine Frage anhand aller verfügbaren Dokumentensammlungen beantwortet. Sollte es sich um eine spezifische Frage zu einem Fall handeln, so muss die entsprechende Dokumentensammlung zuerst in den Einstellungen des Chatbots ausgewählt werden.

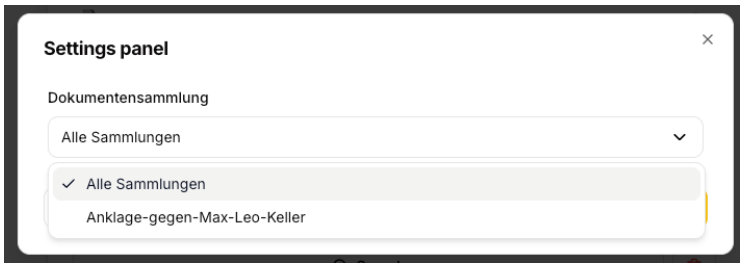

Abbildung 1: Auswahl der Dokumentensammlung, zu der Fragen beantwortet werden sollen. Die zu durchsuchende Dokumentensammlung kann in den Einstellungen angepasst werden.

5.2.2 Technische Implementierung

Die RAG-Pipeline funktioniert folgendermassen: Der Chatbot wandelt die Frage in ein Vektor-Embedding um und sucht die 30 ähnlichsten Textpassagen aus der Vektordatenbank. Ausserdem werden die 10 ähnlichsten Textpassagen mittels der Qdrant-Implementierung[187] des BM25-Algorithmus[188] gesucht und mit den 30 anderen Suchresultaten kombiniert. Danach wird das oben erwähnte Reranker-Modell verwendet, um die Relevanz der gefundenen Textpassagen für die Frage neu zu bewerten. Anhand dieser optimierten Rangliste werden dann die fünf passendsten Textpassagen dem LLM zusammen mit der Frage übergeben, damit dieses eine Antwort generieren kann.

5.3 Features und Umsetzung

Im Folgenden werden die einzelnen Features des Chatbots erläutert.

5.3.1 Contextual Retrieval

Manchmal können einzelne Textpassagen aus dem Kontext herausgerissen falsch interpretiert werden. Um dem entgegenzuwirken, verwenden wir eine adaptierte Version von Contextual Retrieval[189]. Dabei wird eine Textpassage im gesamten Dokument *situiert*, d.h. es wird geschaut, wie diese Textpassage in dem Dokument eingebettet ist, und die Textpassage wird um die entsprechende Kontextualisierung ergänzt. Das führt einerseits dazu, dass diese Zusatzinformationen bei der Generierung des Embeddings berücksichtigt werden, und andererseits dient es dem LLM als Stütze bei der Generierung der Antwort, da es weniger interpretieren muss.

Die Anpassung, die wir vorgenommen haben, dient dazu, dieses Verfahren auch bei langen Dokumenten durchführen zu können. Sprachmodelle erlauben in der Regel nur eine limitierte Anzahl an Zeichen pro Anfrage, was bei längeren Dokumenten und insbesondere bei selbst betriebenen LLMs zu Problemen führen kann. Deshalb basiert unsere Situierung nicht auf dem gesamten Dokument, sondern lediglich aus den ersten 10 Textpassagen sowie den drei Textpassagen vor und nach der zu situierenden Textpassage. Nebst dieser Situierung verwenden wir das LLM auch zur Extraktion von gewissen Restriktionen, die für das Verständnis der Textpassage wichtig sind, zum Beispiel wenn eine Aussage sich nur auf einen gewissen Zeitraum oder gewisse Personen bezieht.

5.3.2 Follow-Up Fragen

Es ist praktisch, wenn ohne grossen Aufwand Folgefragen gestellt werden können. Damit dies möglich ist, überprüft der Chatbot jeweils, ob eine Frage neu ist, oder ob sie sich auf ein vorheriges Thema

[187] https://huggingface.co/Qdrant/bm25

[188] https://en.wikipedia.org/wiki/Okapi_BM25

[189] https://www.anthropic.com/news/contextual-retrieval

bezieht. In letzterem Fall wird die Frage so umformuliert, dass sie alle nötigen Informationen enthält, ohne dabei den ganzen Chatverlauf an das Embedding-Modell senden zu müssen. Die umformulierte Frage ist in der Benutzeroberfläche auf Wunsch ersichtlich.

5.3.3 Quellen Anzeigen

Nachdem das LLM die Antwort auf eine Frage generiert hat, wird die Antwort auf Quellenangaben überprüft. Wenn das LLM eine solche Angabe erwähnt hat, wird diese mit einem klickbaren Link mit dem Titel des Dokuments ersetzt, aus dem die Information extrahiert wurde. Die Benutzerin oder der Benutzer kann dann auf diesen Link klicken, um das Dokument anzuzeigen.

5.3.4 Dokumentensammlungen verwalten

Bestehende Dokumentensammlungen können mit dem Befehl «/Show Collection» oder via Klick auf den entsprechenden Button angezeigt werden:

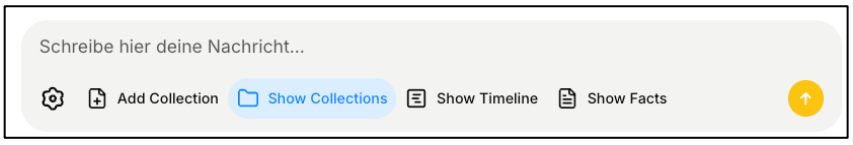

Abbildung 2: Mit dem Button "Show Collections" können vorhandene Dokumentensammlungen aufgelistet werden.

Um eine neue Dokumentensammlung, z.B. Unterlagen zu einem neuen Fall, hinzuzufügen, kann der Befehl «/Add Collection» oder der entsprechende Button verwendet werden. Es öffnet sich ein Formular, in dem man der neuen Dokumentensammlung einen Namen geben und einen Ordner auswählen kann. Der Ordner wird dann auf Dokumente gescannt, welche im nächsten Schritt zur Dokumentensammlung hochgeladen werden können. Sobald dies geschieht, befinden sich die Dokumente auf dem Chatbot-Server. Diese können zusammen mit der Dokumentensammlung über die Ansicht des «Show Collections» Befehl wieder gelöscht werden.

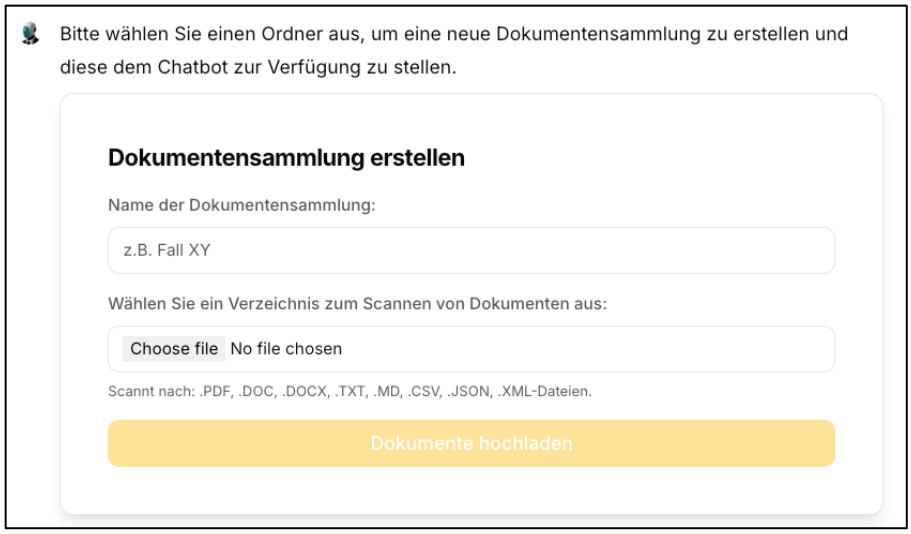

Abbildung 3: Formular, das zum Erstellen einer neuen Dokumentensammlung dient. Es wird durch den Befehl "Add Collection" geöffnet.

5.3.5 Timeline anzeigen

Jede Dokumentensammlung verfügt über eine Timeline. Diese wird bei der Erstellung einer neuen Dokumentensammlung automatisch von einem LLM generiert, indem jede Textpassage auf Ereignisse gescannt wird. Über den Befehl «Show Timeline» oder den entsprechenden Button kann eine Timeline angezeigt werden. Zusätzlich zu dem Befehl muss der Name der Dokumentensammlung in der Nachricht angegeben werden, damit die Timeline geladen wird. Ein Beispiel einer solchen Pipeline ist in Abbildung 4 ersichtlich.

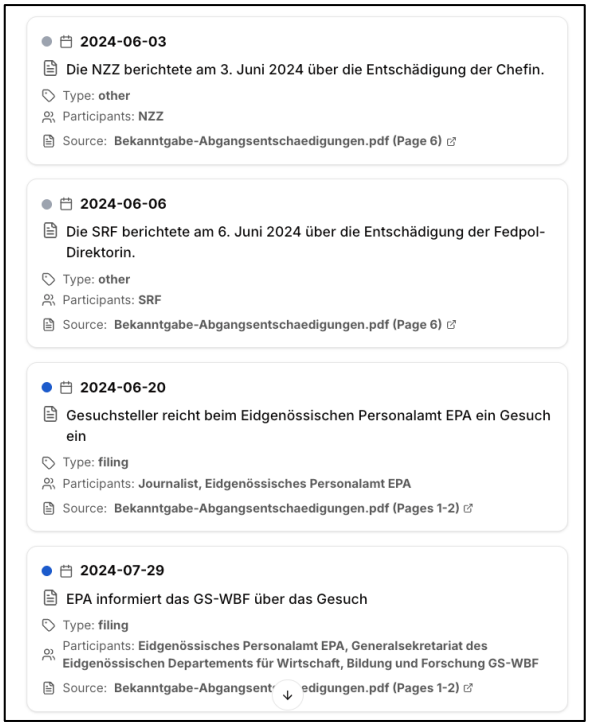

Abbildung 4: Ausschnitt aus einer exemplarischen Timeline.

5.3.6 Sachverhalt anzeigen

Mit dem Befehl «Show Facts», oder durch Klick auf den entsprechenden Button, kann der Sachverhalt des Falls, der in der entsprechenden Dokumentensammlung beschrieben wird, angezeigt werden. Dieser Sachverhalt wird durch ein LLM generiert, welches alle Textpassagen analysiert und den Sachverhalt inkrementell erweitert und am Ende noch einmal zusammenfasst. Falls der Sachverhalt für eine Dokumentensammlung bereits generiert wurde, so wird dieser aus einer Datenbank geladen. Falls der Sachverhalt noch nicht extrahiert wurde, wird mit dem Befehl die Extraktion in Gang gesetzt. Dies kann je nach Anzahl Dokumente und Seiten in der Dokumentensammlung einige Zeit in Anspruch nehmen.

5.4 Herausforderungen für den produktiven Betrieb

Der Prototyp zeigt auf, dass ein Chatbot oder allgemeiner ein KI-Tool für Anwaltskanzleien aus technischer Sicht durchaus mit Open-Source Technologien und KI-Modellen umsetzbar ist. Der Umfang der Features und die Effizienz eines solchen Tools hängt jedoch stark von der verfügbaren Hardware ab. Je besser die Hardware, umso längere Text können von einem LLM auf einmal verarbeitet werden. Ausserdem kann die Hardware einen Einfluss auf die Geschwindigkeit des Tools haben: momentan dauert die Erstellung einer neuen Dokumentensammlung mit ca. 60 Dokumenten mehrere Stunden, was vor allem an der umfangreichen Vorverarbeitung der Dokumente mittels Docling und der Erstellung der Timeline via LLM zusammenhängt. Es sei an dieser Stelle erwähnt, dass unser Server, auf dem wir den Chatbot laufen lassen, über wenig Leistung und keine Grafikprozessoren verfügt, was das Ganze verlangsamt.

Um diesen Prototypen produktiv im Einsatz zu haben, müsste ausserdem mehr Zeit in die Entwicklung des Tools investiert werden. Für eine möglichst robuste und benutzerfreundliche Erfahrung braucht es ein Team von Softwareentwicklern, die sowohl das Frontend als auch das Backend weiterentwickeln und verfeinern. Im Falle einer Weiterentwicklung des Prototyps empfiehlt es sich, das Tool hochgradig konfigurativ zu gestalten, so dass dieses von unterschiedlichen Parteien mit unterschiedlichen Bedürfnissen und Budgets eingesetzt werden kann. Insbesondere sollte sich die Verarbeitung der Dokumente und die Bereicherung der Textpassagen mit Metadaten, welche von einem LLM extrahiert werden, an die Hardware, die im Rahmen des Budgets einer einzelnen Partei gemietet oder beschafft wurde, anpassen.

5.5 Verfügbarkeit des Prototyps

Der Prototyp lässt sich mit den bereits genannten Einschränkungen testen. Der vollständige Quellcode ist auf GitHub unter der Open Source MIT Lizenz veröffentlicht. [190] Eine technische Anleitung erläutert, wie der Prototyp installiert und in Betrieb genommen wird.

6 Lösungsvorschläge für Nutzung von Open-Source-KI und Betrieb des BFH-KI-Prototyps

In diesem Kapitel werden die eingangs vorgestellten Lösungsvorschläge zur Nutzung von Open-Source-KI-Modellen besprochen.

Zwei davon beziehen sich auf die Umsetzung und den Betrieb des in Kapitel 6 beschriebenen BFH-KI-Prototyps. Die beiden weiteren Lösungen zeigen alternative Ansätze auf, bei denen bestehenden KI-Open-Source-Anwendungen genutzt werden können.

Der erste Lösungsvorschlag stellt das Herunterladen und Betreiben von bestehenden Open-Source-KI-Applikationen auf dem eigenen Laptop dar. Dabei kann die KI-Lösung offline genutzt werden und ist lokal gespeichert. Die zweite Lösung stellt die serverbasierte Eigenlösung dar, bei der ein kanzleiinterner Server benutzt wird, auf welchem der BFH-KI-Prototyp betrieben werden kann. Die Wartung und das Management des Servers obliegen der Kanzlei. Der dritte Lösungsvorschlag bezieht sich auf eine externe Hosting-Lösung. Im Sinne von Infrastructure-as-a-Service wird von einer Schweizer Cloud-Anbieterin die Infrastruktur zur Verfügung gestellte, auf welcher der BFH-KI-Prototyp betrieben werden kann. Je nach Bedarf können die Infrastrukturanbieterinnen auch Wartungs- und Managementaufgaben wahrnehmen. Der letzte Lösungsvorschlag betrifft das Benutzen einer Open-Source-KI-Dienstleistung einer Schweizer Cloud-Anbieterin. Im Sinne einer Software-as-a-Service, wird in diesem Fall eine webbasierte Dienstleistung zur Verfügung gestellt, wobei die zugrundeliegenden Dienste (Support, Management usw.) bei der Cloud-Anbieterin liegen.

6.1 Lokale-Open-Source KI-Lösung

Es bestehen zurzeit diverse Open-Source-KI-Applikationen, die lokal auf dem eigenen Laptop betrieben werden können. Einige Beispiele hierfür sind: LM Studio,[191] GPT4all[192] oder Ollama.[193] Das sind allesamt Applikationen, mit welchen verschiedene Open-Source-KI-Modelle (z.B. Llama, DeepSeek, Qwen, Gemma usw.) heruntergeladen und lokal betrieben werden können.

Diese Applikationen können «offline» genutzt werden, wodurch, gemäss den Aussagen der Anbieterin, keine privaten Daten ins Internet übertragen werden noch durch diese Anbieterin gesammelt oder gespeichert werden.[194]

GPT4all, beispielsweise, unterstützt die Betriebssysteme Windows, macOS und Linux. Dabei wird für die Applikation einen Arbeitsspeicher von mindestens 8GB RAM benötigt sowie ein aktuelles Betriebssystem (Windows 10 oder neuer, macOS Monterey 12.6 oder neuer, Ubuntu 22.04 LTS oder neuer).[195] Für den lokalen Betrieb der verschiedenen Sprachmodelle, die über die Applikation heruntergeladen und benutzt werden, ist ein ausreichend grosser Arbeitsspeicher erforderlich. Das jeweilige Sprachmodell

[190] Fiducia (Public PoC) auf GitHub <https://github.com/digital-sustainability/fiducia>

[191] LM Studio, <https://lmstudio.ai/>

[192] NOMIC GPT4All, <https://www.nomic.ai/gpt4all>

[193] Ollama, <https://ollama.com/>

[194] LM Studio – Offline Operation,<https://lmstudio.ai/docs/app/offline>, NOMIC GPT4All <https://www.nomic.ai/gpt4all>, GitHub-Ollama, <https://github.com/ollama/ollama/blob/main/docs/faq.md>

[195] GitHub-nomic-ai/gpt4all, <https://github.com/nomic-ai/gpt4all/wiki>

muss vollständig heruntergeladen und lokal gespeichert werden. Je grösser der verfügbare Arbeitsspeicher, desto grössere und leistungsfähigere Sprachmodelle können genutzt werden.

Bei den meisten Open-Source-KI-Anwendungen besteht die Möglichkeit, eine benutzerdefinierte Wissensdatenbank zu erstellen, auf welche das heruntergeladenen und benutzte Sprachmodell bei der Beantwortung einer Frage gezielt Bezug nehmen muss.[196] Die Vektorisierung der Texte (sog. Embedding) wird lokal von der Applikation selbst vorgenommen.

Die für den Betrieb solcher Applikationen erforderliche Rechenleistung übersteigt jedoch in der Regel die Kapazität eines herkömmlichen Laptops, insbesondere wenn sie im Rahmen anwaltlicher Tätigkeiten zuverlässig funktionieren sollen. Daher wird diese Option zwar erwähnt, gilt jedoch als wenig empfehlenswert.

6.2 Serverbasierte Eigenlösung

Der in Kapitel 6 entwickelte BFH-KI-Prototyp kann sowohl auf einem eigenen Server wie auch auf einer Cloud-Infrastruktur betrieben werden. Die Kosten für den Betrieb auf einem internen Server beziehen sich sowohl auf die Anschaffung der Hardware, sowie Kosten für Wartung und Betrieb.

Anschaffungskosten für einen Server belaufen sich auf ca. 7'000 CHF (insbesondere für 2x NVIDIA RTX 5090 für den Betrieb der Sprachmodelle). Der Betrieb und Unterhalt kann relativ kostengünstig organisiert werden. Für das Management des Servers sollten 15-20 Arbeitsstunden pro Jahr ausreichend sein. Bei einem Stundensatz von 160 CHF wären das 2400 – 3200 CHF / Jahr.

6.3 Externe Hosting-Lösung (IaaS)

Analog können die Ressourcen für den Betrieb des BFH-KI-Prototypens auch bei einer Schweizer Cloud-Anbieterin erfolgen.

Infomaniak[197] bietet hier einen nach ISO 27001 zertifizierten Dienst an über welchen KI-Dienstleistungen bezogen werden können.

Dabei fallen folgende Kosten an:[198]

Aufgabe	Modell	Kosten
Sprachmodell	Llama 3.3 70b	Eingehend: CHF 0.01 / 10k Tokens Ausgehend: CHF 0.03 / 10k Tokens
Einbettungen	Bge Multilingual Gemma2	CHF 0.065 CHF / 1M Tokens

Infomaniak gibt an, dass keine Daten auf ihrer Infrastruktur gespeichert werden.[199] Anstelle des Bezugs von KI-Dienstleistungen als Service kann auch direkt eine virtuelle GPU-Infrastruktur bezogen werden. Eine GPU-Infrastruktur kann bei ähnlichen Anbietern bezogen werden[200].

Die Kosten für GPU-Infrastruktur in diesem Rahmen belaufen sich auf ca. 220 CHF / Monat. Ausserdem kann die Kommunikation mit der Infrastruktur über verschlüsselte Verbindungen gemacht werden, wodurch auch eine Überwachung der Kommunikation kaum möglich wäre. Zusätzlich müsste noch ein

[196] Beispielsweise LocalDocs von GPT4all, <https://docs.gpt4all.io/gpt4all_desktop/localdocs.html>

[197] Infomaniak, <https://www.infomaniak.com/de>

[198] Infomaniak-Tarife, <https://www.infomaniak.com/de/hosting/ai-tools/tarife#llm>

[199] Infomaniak unter «Privatsphäre», <https://www.infomaniak.com/de/hosting/ai-tools>

[200] Siehe: https://www.infomaniak.com/de/hosting/public-cloud/tarife#instances

virtueller Server für den Betrieb der Applikation sowie das Speichern der Daten eingerichtet werden. Dieser Server würde jährlich ca. 2'500 kosten.

6.4 KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS)

Die letzte Möglichkeit wäre, die Applikation sowie die Datenhaltung auf einem lokalen Server zu betreiben und nur die KI-Dienstleistungen[201] von einer Cloud-Anbieterin zu beziehen. Die Kosten für die KI-Dienstleistungen würden sich im Vergleich zu Abschnitt 7.3 nicht verändern.

Analog zu Abschnitt 7.2 müsste auch hier ein lokaler Server angeschafft und betrieben werden. Die Kosten für einen Server ohne die entsprechenden KI-Features lägen bei ca. 4'000 - 5'000 CHF. Die Kosten für die jährliche Wartung und den Betrieb lägen ebenfalls bei ca. 2'400 - 3'200 CHF pro Jahr.

Der grosse Vorteil dieser Lösung wäre, dass alle Dokumente und Informationen auf einem lokalen Server gespeichert wären und bei der KI-Verarbeitung in der Cloud sichergestellt ist, dass keine Daten gespeichert werden.[202]

6.5 Rechtliche Auslegeordnung

6.5.1 Datenschutzrecht

Bei allen vier vorgestellten Lösungsvorschlägen (Lokale Open-Source-KI-Lösung; serverbasierte Eigenlösung, externe Hosting-Lösing; Bezug von KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin) werden Personendaten im Sinne von Art. 5 lit. a DSG bearbeitet. Es greifen somit die datenschutzrechtlichen Bestimmungen nach dem DSG insbesondere die Bearbeitungsgrundsätze nach Art. 6 DSG. Klientinnen müssen vor allem darüber informiert werden, zu welchem Zweck ihre Personendaten erhoben und verarbeitet werden, wer darauf Zugriff hat und wie lange diese Daten gespeichert werden.[203] Auch hier gilt es zu berücksichtigen, dass Personendaten die von Anwältinnen bearbeitet werden, häufig besonders schützenswerte Personendaten sind,[204] was wiederum eine ausdrückliche Einwilligung erfordert (Art. 6 Abs. 7 DSG). Diese kann regelmässig durch die Unterzeichnung der Anwaltsvollmacht eingeholt werden.

Zudem muss bei der Bearbeitung von Personendaten die Datensicherheit gewährleistet werden (Art. 8 DSG), und die Integrität, Verfügbarkeit und Vertraulichkeit der bearbeiteten Personendate stets sichergestellt werden.[205] Vor allem Cloud-Anbieterinnen von IaaS- und SaaS-Lösungen müssen somit zwingend sorgfältig ausgewählt werden.[206]

Kanzleiinterner Server

Werden externe IT-Supportleistungen herangezogen, beispielswiese für die Wartung des Servers, dann muss unterschieden werden, ob die IT-Dienstleisterin, im Rahmen ihrer Tätigkeiten, bloss punktuellen oder zufälligen oder dann einen systematischen Zugriff auf Personendaten hat.[207] Im ersten Szenario

---

[201] Siehe beispielsweise: https://www.infomaniak.com/de/hosting/ai-tools

[202] Beachte jedoch Kapitel 7.5; die Daten werden zwar nicht in der Cloud gespeichert, nichtsdestotrotz müssen diese für die Benutzung der Applikation, unverschlüsselt übermittelt werden, was wiederum bedeutet, dass die Cloud-Providern Zugriff auf die Daten hat.

[203] Vgl. Vorlage des Schweizerischen Anwaltsverbandes «Datenschutzerklärung für das Mandatsverhältnis» erstellt von David Schwaninger (Blum & Grob Rechtsanwälte AG) und Rechtsanwalt Thomas Steiner (LAUX LAWYERS AG), abrufbar unter: https://www.sav-fsa.ch/home/-/asset_publisher/nVUlpgxhWiQo/content/datenschutzerkl%25C3%25A4rung-f%25C3%25BCr-das-mandatsverh%25C3%25A4ltnis?refererPlid=1565176&_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_nVUlpgxhWiQo_redirect=https%3A%2F%2Fwww.sav-fsa.ch%2Ffr%2Fhome%3Fp_p_id%3Dcom_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_nVUlpgxhWiQo%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26refererPlid%3D1565176%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_nVUlpgxhWiQo_cur%3D0%26p_r_p_resetCur%3Dfalse%26_com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_nVUlpgxhWiQo_assetEntryId%3D3504741

[204] HÜRLIMANN/STEIGER, S. 201.

[205] HÜRLIMANN/STEIGER, S. 201.

[206] SURY /GOGNIAT, S. 204; SAV-Wegleitung für IT-Outsourcing und Cloud-Computing, S. 3-4.

[207] HUSI-STÄMPFLI/MORAND, Rz. 153.

wird die IT-Dienstleisterin in der Regel nicht als Auftragsbearbeiterin qualifiziert, bei der zweiten Variante hingegen schon.[208]

Wird die IT-Dienstleisterin als Auftragsbearbeiterin qualifiziert, müssen die Voraussetzungen nach Art. 9 DSG erfüllt werden. Ist dies nicht der Fall, dann stellt der Zugriff der IT-Dienstleisterin auf die Personendaten eine neue Datenbearbeitung dar. Diese bedarf eines rechtlichen Rechtfertigungsgrundes (Art. 30 DSG).

Externe Hosting-Lösung (IaaS) und KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS)

Grundsätzlich werden Cloud-Anbieterinnen, die die Infrastruktur zur Verfügung stellen, als Auftragsbearbeiterinnen qualifiziert.[209] Dabei ist entscheidend, ob die Serverbetreiberin systematischen Zugriff auf die Personendaten hat und diese nur gemäss den Weisungen der Kanzlei bearbeitet.[210] Auch beim Bezug von KI-Dienstleistungen über eine Cloud-Anbieterin, im Sinne einer SaaS-Leistung, wird die Cloud-Anbieterin als Auftragsbearbeiterin eingestuft.[211]

Zu berücksichtigen ist, dass bei einem IaaS-Modell die Daten entweder erst bei der Cloud-Providerin oder aber bereits vor der Übertragung über das Internet (unter Verwendung von HTTPS: Hypertext Transmission Protocol Secure) durch die Anwaltskanzlei verschlüsselt werden können.[212] Somit hat nur noch die Anwaltskanzlei Zugang zu den Daten.[213]

Bei SaaS-Modellen, bei welchen die Software in der Cloud zur Verfügung gestellt wird, muss die Softwareapplikation Zugriff auf die unverschlüsselten Dateien haben, was wiederum bedeutet, dass die Daten für die Cloud-Providerin im Klartext sichtbar sind.[214]

Daraus folgt, dass bei IaaS-Angebote die Daten in verschlüsselter Form bei der Cloud-Providerin gespeichert werden und diese somit keinen Zugriff auf den Inhalt der Daten hat. Mangels Bestimmbarkeit der betroffenen natürlichen Person werden die Daten nicht mehr als Personendaten qualifiziert, womit die Bestimmungen des Datenschutzgesetzes nicht zur Anwendung kommen.

Bei SaaS-Modellen, bei welchen die Cloud-Providerin Zugriff auf die unverschlüsselten Daten hat, ist es von Bedeutung, dass die Cloud-Providerin als Auftragsbearbeiterin nach Art. 9 Abs. 1 DSG qualifiziert wird. Hierbei ist zu berücksichtigen, dass die Übertragung der Bearbeitung durch eine Auftragsverarbeiterin regelmässig aufgrund eines Vertrags[215] (sog. Data Processing Agreement, DPA) oder dann ausnahmsweise durch Gesetzgebung zu erfolgen hat.[216] Die Verantwortliche hat dabei sicherzustellen, dass die Daten durch die Auftragsbearbeiterin nur «so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte» (Art. 9 Abs. 1 lit. a DSG). Zudem muss sich die Verantwortliche vergewissern, dass die Auftragsbearbeiterin in der Lage ist, die Datensicherheit zur gewährleisten (Art. 9 Abs. 2 DSG). Die Auftragsbearbeiterin ist weisungsgebunden (vgl. Art. 9 Abs. 1 lit. a DSG), und bearbeitet die Daten nur gemäss den Weisungen der Verantwortlichen.[217] Deshalb steht ihr keine Entscheidungsbefugnis betreffend Zweck und Mittel zu.[218]

Würde die Cloud-Anbieterin, nicht als Auftragsbearbeiterin qualifiziert werden, dann würde die Weitergabe von Personendaten an die Serverbetreiberin eine neue Datenbearbeitung darstellen.

---

[208] HUSI-STÄMPFLI/MORAND, Rz. 153.

[209] HUSI-STÄMPFLI/MORAND, Rz. 147; HÜRLIMANN/STEIGER, S. 201.

[210] HUSI-STÄMPFLI/MORAND, Rz. 153.

[211] HÜRLIMANN/STEIGER, S. 201.

[212] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 26.

[213] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 26; Vgl. auch Infomaniak, Die Sicherheit der kDrive-Daten verstehen, https://www.infomaniak.com/de/support/faq/2462/die-sicherheit-der-kdrive-daten-verstehen.

[214] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 26; Vgl. Infomaniak, Das Verständnis der Nutzung von KI bei Infomaniak, https://www.infomaniak.com/de/support/faq/1369/das-verstandnis-der-nutzung-von-ki-bei-infomaniak

[215] Siehe zum Mindestinhalt: BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 31.

[216] BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 4.

[217] BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 8.

[218] BSK DSG-BÜHLER/RAMPINI, Art. 9 Rz. 8.

6.5.2 Strafrecht

Lokale Open-Source-KI-Lösung

Die Offline-Nutzung der Open-Source-KI-Desktop-Varianten, bei denen sämtliche Daten im lokalen Arbeitsspeicher verbleiben,[219] verletzt die Berufsgeheimnispflicht nach Art. 321 StGB sowie die berufliche Schweigepflicht nach Art. 62 DSG nicht.

Kanzleiinterner Server

Kanzleipersonal sowie Personen, die für die IT-Dienste einer Anwältin zuständig sind, und im Rahmen ihrer unterstützenden Tätigkeit Kenntnis von Geheimnissen erlangen, werden in der Lehre als Hilfspersonen im Sinne von Art. 321 Abs. 1 StGB qualifiziert.[220]

Erlangen Hilfspersonen im Rahmen ihrer Tätigkeit Kenntnis von Informationen von Mandantinnen, stellt dies keine strafbare Offenbarung eines der Geheimnisträgerin anvertrauten Geheimnisses dar.[221] Dies deshalb, weil Hilfspersonen nach Art. 321 Ziff. 1 StGB ebenfalls dem Berufsgeheimnis unterstehen.

Dies gilt auch in Bezug auf die berufliche Schweigepflicht nach Art. 62 DSG, bei welcher der Begriff des Offenbarens demjenigen von Art. 321 StGB entspricht.[222] So wird nach Art. 62 DSG ein Geheimnis offenbart, wenn die Geheimhaltungspflichtige es einer dazu nicht ermächtigten dritten Person zur Kenntnis bringt oder ihr die Kenntnisnahme ermöglicht.[223] Hilfspersonen, darunter auch die Auftragsbearbeiterin, gelten dabei jedoch nicht als unberechtigte Dritte.[224]

Somit wird durch den Betrieb des BFH-KI-Prototypen auf einem kanzleiinternen Server, auf den auch Hilfspersonen Zugriff haben können, weder die Berufsgeheimnispflicht nach Art. 321 StGB noch die berufliche Schweigepflicht nach Art. 62 DSG verletzt.

Externe Hosting-Lösung (IaaS) und KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS)

Anbieterinnen von Cloud-Lösungen (IaaS und SaaS), werden in der Lehre mehrheitlich als Hilfspersonen qualifiziert.[225] Folgt man dieser Argumentation, liegt durch den Betrieb des BFH-KI-Prototypen auf einem Schweizer Server einer Drittanbieterin oder durch die Nutzung einer KI-Dienstleistung einer Schweizer Cloud-Anbieterin keine Offenbarung von Geheimnissen vor.[226] Dies gilt insbesondere für Mandatsinformationen, die im Zusammenhang mit der Benutzung des BFH-KI-Prototypen auf den Server oder der KI-Dienstleistung zumindest zwischengespeichert werden, da Hilfspersonen nach Art. 321 Abs. 1 StGB ebenfalls dem Berufsgeheimnis unterstehen.[227] Dasselbe gilt für die berufliche Schweigepflicht nach Art. 62 DSG.

Auch hier ist zu beachten, dass bei einem IaaS-Modell die Daten entweder erst bei der Cloud-Providerin oder bereits vor der Übertragung über das Internet (unter Verwendung von HTTPS: Hypertext Transmission Protocol Secure) durch die Anwaltskanzlei verschlüsselt werden können, sodass ausschliesslich die Anwaltskanzlei Zugang zu den Daten hat.[228]

Bei SaaS-Modellen, bei denen die Software in der Cloud zur Verfügung gestellt wird, muss die Softwareapplikation Zugriff auf die unverschlüsselten Dateien haben, was wiederum bedeutet, dass die Daten

---

[219] Diese Angaben beruhen auf den Websiteinformationen der jeweiligen Anbieter. Für die Richtigkeit, Vollständigkeit und Aktualität dieser Information wird keine Verantwortung übernommen.

[220] Siehe vorne Kapitel 3.2.1.3 «Hilfsperson».

[221] Siehe vorne Kapitel 3.2.1.4 «Offenbarung»; a.M. WOHLERS, Auslegung einer Datenbearbeitung und Berufsgeheimnis, S. 25.

[222] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[223] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 19.

[224] BSK DSG-MATHYS/THOMANN, Art. 62 Rz. 22.

[225] SCHWARZENEGGER/THOUVENIN /STILLER, S. 40; CASANOVA, S. 49; HÜRLIMANN/STEIGER, S. 203; SURY /GOGNIAT, S. 203; A.M. WOHLERS, Outsourcing durch Berufsgeheimnisträger, S. 117.

[226] SCHWARZENEGGER/THOUVENIN /STILLER, S. 40; CASANOVA, S. 49; HÜRLIMANN/STEIGER, S. 203; SURY /GOGNIAT, S. 203; A.M. WOHLERS, Outsourcing durch Berufsgeheimnisträger, S. 117.

[227] SCHWARZENEGGER/THOUVENIN /STILLER, S. 42; HÜRLIMANN/STEIGER, S. 203; a.M. WOHLERS, Auslegung einer Datenbearbeitung und Berufsgeheimnis, S. 25.

[228] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 26.

für die Cloud-Providerin im Klartext sichtbar sind.[229] Bei SaaS-Modellen ist es daher von höchster Relevanz, dass die Cloud-Providerin als Hilfsperson qualifiziert wird. Würde die Cloud-Anbieterin bei Saas-Modellen nicht als Hilfsperson gelten, läge eine strafrechtlich relevante Offenbarung im Sinne von Art. 321 Abs. 1 Ziff. 1 StGB sowie Art. 62 DSG vor. Wie oben bereits erwähnt, wird in der Lehre jedoch mehrheitlich die Qualifikation der Cloud-Providerin als Hilfsperson bejaht.[230]

Auch in diesem Fall muss, beispielsweise durch vertragliche Vereinbarung, sichergestellt werden, dass aussenstehende Dritte keinen Zugriff auf den betriebenen BFH-KI-Prototypen oder die von der Anwaltskanzlei bezogene KI-Dienstleistung haben, die im Zusammenhang mit Mandatsinformationen (Geheimnissen) genutzt werden.

6.5.3 Anwaltsrecht

Kanzleiinterner Server

Unter Berücksichtigung der anwaltsrechtlichen Pflichten, insbesondere des Berufsgeheimnisses nach Art. 13 BGFA, ist durch vertragliche sowie gegebenenfalls durch technische und physische Massnahmen sicherzustellen, dass sämtliche Hilfspersonen, die Zugriff auf den Server und damit auf den BFH-KI-Prototypen mit mandatsbezogenen Informationen haben, der Geheimhaltungspflicht unterstellt sind (Art. 13 Abs. 2 BGFA).[231]

Lokale Open-Source-KI-Lösung

Die Offline-Nutzung der Open-Source-KI-Desktop-Varianten, bei denen sämtliche Daten im lokalen Arbeitsspeicher verbleiben,[232] ist grundsätzlich mit Art. 13 BGFA vereinbar.

Externe Hosting-Lösung (IaaS) und KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS)

Wie in Kapitel 4.3 erläutert wurde, ist der Begriff der Hilfsperson nach Art. 13 Abs. 2 BGFA weit gefasst zu verstehen.[233] Somit sind Hilfspersonen nach Art. 13 Abs. 2 BGFA alle Personen, die die Anwältin zur Unterstützung ihrer Berufstätigkeit beizieht und die im Zusammenhang mit dieser Tätigkeit einen Zugang zu Mandatsinformationen haben.[234] Dabei muss aber keinen direkten Sachzusammenhang zur eigentlichen Berufstätigkeit bestehen, massgebend ist vielmehr, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu Mandatsinformationen einschliesst.[235]

Soweit die Cloud-Anbieterin Zugriff auf Mandatsinformationen hat, kann diese als Hilfsperson nach Art. 13 BGFA qualifiziert werden.

Unter Berücksichtigung des Berufsgeheimnisses nach Art. 13 BGFA, sind bereits bei der Auswahl der Cloud-Anbieterin verschiedene Kriterien zu beachten, wie Erfahrung und Ruf der Anbieterin sowie die finanzielle Situation oder die Anzahl der Mitarbeiterinnen.[236] Sodann ist durch vertragliche sowie gegebenenfalls durch technische und physische Massnahmen sicherzustellen, dass sämtliche Hilfspersonen, der Geheimhaltungspflicht unterstellt sind (Art. 13 Abs. 2 BGFA).[237] Somit muss auch die Cloud-Anbieterin, wie andere Hilfspersonen, vertraglich zur Einhaltung des Berufsgeheimnisses verpflichtet werden.[238] Anwältinnen müssen in der Praxis die AGBs einer Cloud-Anbieterin entsprechend überprüfen.[239]

---

[229] SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 26.

[230] Siehe Kapitel 3.2.1.3.

[231] Vgl. NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56; BGE 145 II 229, E. 7.6; SCHILLER, Rn. 541.

[232] Diese Angaben beruhen auf den Websiteinformationen der jeweiligen Anbieter. Für die Richtigkeit, Vollständigkeit und Aktualität dieser Information wird keine Verantwortung übernommen.

[233] NATER/ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[234] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 51.

[235] NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 53.

[236] SAV-Wegleitung für IT-Outsourcing und Cloud-Computing, S. 4.

[237] Vgl. NATER/ ZINDEL, Kommentar zum Anwaltsgesetz, Art. 13 Rz. 56; BGE 145 II 229, E. 7.6; SCHILLER, Rn. 541.

[238] SCHWARZENEGGER/THOUVENIN /STILLER, S. 38.

[239] SCHWARZENEGGER/THOUVENIN /STILLER, S. 38.

Ferner ergibt sich aus dem BGFA, dass Anwältinnen die Einhaltung der Verschwiegenheitsverpflichtung in zumutbarer Weise überwachen müssen.[240]

6.5.4 Allgemeine Bemerkungen

Allgemein ist bei einem kanzleiintern betriebenen Server zu empfehlen, eine IT-Sicherheitsstrategie zu erarbeiten.[241] Zudem muss sichergestellt werden, dass kanzleiinterne Daten das interne Netzwerk nicht verlassen oder ausserhalb der Infrastruktur gespeichert werden.[242]

Kann dies nicht gewährleistet werden, dürfen vertrauliche Informationen, Unternehmensgeheimnisse, persönliche Daten von Mitarbeiterinnen, Klientinnen oder Geschäftspartnerinnen oder anderen Personen nicht im Zusammenhang mit dem BFH-KI-Prototyp benutzt werden.[243]

7 Gesamtfazit

Die Studie identifiziert vier Ansätze, wie KMUs, die dem Berufsgeheimnis unterliegen (insb. Anwaltskanzleien), KI-Tools erfolgreich in ihre Arbeitsprozesse integrieren und nutzen können.

Die vier möglichen Lösungsansätze, die allesamt auf Open-Source-KI-Modellen basieren, unterscheiden sich wie folgt:

1. Lokale-Open-Source KI-Lösung,
2. Serverbasierte Eigenlösung,
3. Externe Hosting-Lösung (IaaS),
4. KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS).

In Kapitel 4 wurden zunächst die rechtlichen Rahmenbedingungen dargestellt, die für die Umsetzung der vier Lösungsvorschläge relevant sind. Die Studie beschränkt sich hier auf die relevanten Vorgaben des Datenschutzrechtes, des Berufsgeheimnis nach Art. 321 StGB sowie des anwaltsrechtlichen Berufsgeheimnisses nach Art. 13 BGFA.

Aufbauend darauf wurden in Kapitel 5 exemplarische Anwendungsfälle (Use Cases) erarbeitet, anhand derer ein Open Source BFH-KI-Prototypen entwickelt wurde (Kapitel 6).

Anschliessend umschreibt Kapitel 7 die oben genannten vier Lösungsansätze und zeigt konkrete Möglichkeiten auf, wie diese umgesetzt werden könnten und wie sie rechtlich einzuordnen sind.

Die Ergebnisse lassen sich wie folgt zusammenfassen.

7.1 Lokale Open-Source-KI-Lösung und serverbasierte Eigenlösung

7.1.1 Technische Umsetzung

Bei der lokalen Open-Source-KI-Lösung werden Anwendungen wie *LM-Studio* oder *GPT4all* direkt auf dem eigenen Laptop betrieben. Diese Variante ermöglicht eine vollständig offline erfolgende Datenverarbeitung, wodurch keine Daten an Dritte oder an die Anbieterin der Anwendung übermittelt werden. Allerdings erfordert der Betrieb solcher Modelle erhebliche Rechenressourcen, die in der Regel die Leistungsfähigkeit herkömmlicher Endgeräte übersteigen.

Alternativ kann der entwickelte BFH-KI-Prototyp auf einem eigenen, kanzleiinternen Server betrieben werden. Diese serverbasierte Eigenlösung erlaubt eine zentrale und kontrollierte Nutzung der KI, ohne dass Daten die Kanzleiumgebung verlassen. Die Anschaffungskosten für einen entsprechenden Server belaufen sich auf einmalig rund CHF 7'000, zuzüglich jährlicher Wartungs- und Betriebskosten.

---

[240] SCHWARZENEGGER/THOUVENIN /STILLER, S. 38.

[241] Vgl. STRAUB, S. 5.

[242] SAV-Wegleitung für den Umgang mit künstlicher Intelligenz, S. 1.

[243] Vgl. SAV-Wegleitung für den Umgang mit künstlicher Intelligenz, S. 1.

7.1.2 Wichtigste rechtliche Erkenntnisse

Aus datenschutzrechtlicher Sicht erfolgt bei beiden Varianten eine Bearbeitung von Personendaten, weshalb die Vorgaben des Datenschutzgesetzes (DSG) einzuhalten sind. Dazu gehören insbesondere die Bearbeitungsgrundsätze gemäss Art. 6 DSG sowie die Gewährleistung der Datensicherheit im Sinne von Art. 8 DSG, namentlich hinsichtlich Integrität, Verfügbarkeit und Vertraulichkeit der bearbeiteten Daten *(Kapitel 4.1).* Externe IT-Dienstleisterinnen, die beispielsweise für Wartungsarbeiten beigezogen werden, gelten in der Regel als Auftragsbearbeiterinnen im Sinne von Art. 5 lit. k DSG, sofern sie im Rahmen ihrer Tätigkeit einen systematischen Zugriff auf Personendaten hat. Entsprechend sind die Anforderungen von Art. 9 DSG einzuhalten, insbesondere die Pflicht, dass eine Datenbearbeitung nur nach den Weisungen der Verantwortlichen (d. h. der Anwältin oder des Anwalts) erfolgen darf *(Kapitel 4.1 und 7.5.1).*

Aus strafrechtlicher Perspektive werden IT- Spezialistinnen im Auftrags- oder Anstellungsverhältnis, die in dieser Funktion Kenntnis von Informationen über die Geheimnisherrin erhalten, in der Lehre grundsätzlich als Hilfspersonen im Sinne von Art. 321 Ziff. 1 StGB qualifiziert und unterstehen damit denselben Geheimhaltungspflichten wie die Anwältin selbst. Die Kenntnisnahme von Geheimnissen durch diese Hilfspersonen stellt somit keine unzulässige Offenbarung dar. Entsprechendes gilt auch im Hinblick auf die berufliche Schweigepflicht gemäss Art. 62 DSG *(Kapitel 4.2 und 7.5.2).*

Auch aus anwaltsrechtlicher Sicht sind IT-Dienstleisterinnen als Hilfspersonen einzustufen. Die Anwältin oder der Anwalt ist verpflichtet, vertraglich sicherzustellen, dass sämtliche Hilfspersonen der Geheimhaltungspflicht unterstehen, und hat bei deren Auswahl die erforderliche Sorgfalt walten zu lassen *(Kapitel 4.3 und 7.5.3).*

Die Offline-Nutzung von Open-Source-KI-Anwendungen, bei denen sämtliche Daten im lokalen Arbeitsspeicher verbleiben, ist schliesslich mit den Vorgaben von Art. 13 BGFA vereinbar und verletzt die Berufsgeheimnispflicht gemäss Art. 321 StGB nicht *(Kapitel 7.1).*

7.2 Externe Hosting-Lösung (IaaS) und Bezug von KI-Dienstleistungen von einer Schweizer Cloud-Anbieterin (SaaS)

7.2.1 Technische Umsetzung

Die externe Hosting-Lösung des BFH-KI-Prototyps kann über eine Schweizer Cloud-Anbieterin im Rahmen eines Infrastructure as a Service (IaaS)-Modells realisiert werden. Dabei würde der Betrieb des Prototyps beispielsweise auf einem Server von Infomaniak erfolgen. Die jährlichen Kosten für eine solche IaaS-Lösung belaufen sich auf rund CHF 2500. Alternativ besteht die Möglichkeit, anstelle des eigenen Betriebs und der Nutzung des BFH-KI-Prototyps auf einer externen Infrastruktur eine KI-Dienstleistung direkt von einer Cloud-Anbieterin zu beziehen (SaaS-Lösung). Auch dies könnte über eine Anbieterin wie Infomaniak erfolgen. Die jährlichen Kosten liegen bei dieser Variante zwischen CHF 6400 und 8200. Dabei ist jedoch zu berücksichtigen, dass die angebotene KI-Dienstleistung im Gegensatz zum eigenen entwickelten BFH-KI-Prototyp nicht zwingend auf die spezifischen Bedürfnisse einer Anwaltskanzlei zugeschnitten ist.

7.2.2 Wichtigste rechtliche Erkenntnisse

Aus datenschutzrechtlicher Sicht ist festzuhalten, dass bei der Nutzung von Cloud-Dienstleistungen, unabhängig davon, ob es sich um IaaS- oder SaaS-Lösungen handelt, Personendaten bearbeitet werden. Somit sind die datenschutzrechtlichen Vorgaben des DSG zwingend einzuhalten, insbesondere die Bearbeitungsgrundsätze gemäss Art. 6 DSG sowie die Gewährleistung der Datensicherheit nach Art. 8 DSG, welche die Integrität, Verfügbarkeit und Vertraulichkeit der bearbeiteten Daten sicherstellen *(Kapitel 4.1).* Bei einer IaaS-Lösung können die Daten in der Regel verschlüsselt bei der Cloud-Anbieterin gespeichert werden, wodurch die Anbieterin keinen Zugriff auf den Inhalt der Daten hat. Diese gelten daher mangels Bestimmbarkeit nicht als Personendaten, womit die Bestimmungen des DSG nicht zur Anwendung gelangen. Im Gegensatz dazu hat die Cloud-Anbieterin bei einer SaaS-Lösung Zugriff auf die Daten, da diese unverschlüsselt gespeichert werden. Sie wird daher als Auftragsbearbeiterin im Sinne von Art. 5 lit. k DSG qualifiziert. Folglich müssen die Voraussetzungen von Art. 9 DSG eingehalten und insbesondere ein Data Processing Agreement (DPA) abgeschlossen werden, welches die zulässige Datenbearbeitung im Rahmen der Auftragsbearbeitung regelt *(Kapitel 4.1 und 7.5.1).*

Aus strafrechtlicher Perspektive werden Cloud-Anbieterinnen in der Lehre mehrheitlich als Hilfspersonen qualifiziert (*Kapitel 4.2 und 7.5.2*). Damit unterstehen sie dem Berufsgeheimnis gemäss Art. 321 Abs. 1 StGB sowie der beruflichen Schweigepflicht nach Art. 62 DSG. *(Kapitel 4.2.2 und 7.5.2).* Folgt man dieser Argumentation, stellt die Kenntnisnahme von Geheimnissen bzw. geheimen Personendaten durch die Hilfsperson keine Offenbarung nach Art. 321 Ziff. 1 StGB bzw. Art. 62 DSG dar.

Bei SaaS-Modellen, bei welchen ein Zugriff auf unverschlüsselte Daten besteht, ist es von höchster Relevanz, dass die Cloud-Providern als Hilfsperson qualifiziert wird. Folgt man hingegen der Mindermeinung und stuft die Cloud-Anbieterin bei Saas-Modellen nicht als Hilfsperson ein, dann liegt eine strafrechtlich relevante Offenbarung im Sinne von Art. 321 Abs. 1 Ziff. 1 StGB sowie Art. 62 DSG vor.

Auch aus anwaltsrechtlicher Sicht gelten Cloud-Anbieterinnen als Hilfspersonen. Besonders beim SaaS-Modell, bei dem die Anbieterin auf Daten zugreifen kann, ist es jedoch erforderlich, dass die Anwältin vertraglich sicherstellt, dass sämtliche Hilfspersonen der Geheimhaltungspflicht unterstellt sind. *(Kapitel 7.5.3).*

7.3 BFH-KI-Prototyp

Im Rahmen der Studie wurde von der BFH auf Grundlage der in Kapitel 5 definierten Use Cases ein KI-Prototyp entwickelt. In Kapitel 6 wird beschrieben, welche Technologien bei der Umsetzung verwendet wurden, wie der Chatbot aufgebaut ist und über welche Funktionen der Prototyp verfügt.

Für die Nutzung des Chatbots ist ein separates Login erforderlich. Da der kontinuierliche Betrieb des Chatbots mit Kosten verbunden ist, kann kein dauerhafter Betrieb des Tools gewährleistet werden. Nach Abschluss des Projekts wird individuell festgelegt, wie lange und für welche Benutzerinnen und Benutzer der Prototyp zugänglich bleibt.

7.4 Fazit

Die Studie zeigt, dass die Integration von KI-Tools in KMU, die dem Berufsgeheimnis unterliegen, unter bestimmten Voraussetzungen rechtlich und technisch umsetzbar ist. Basierend auf den dargestellten Ergebnissen hat sich die Nutzung des BFH-KI-Prototyps entweder auf einem eigenen Server oder auf einem Server einer vertrauenswürdigen Cloud-Anbieterin (IaaS) als beste Lösung erwiesen. Dies gilt sowohl aus Kostensicht als auch aus rechtlicher Perspektive, da die Informationen (Personendaten und Geheimnisse) entweder kanzleiintern bearbeitet werden oder verschlüsselt bei der Cloud-Anbieterin gespeichert werden.

Literaturverzeichnis

BLECHTA GABOR P./VASELLA DAVID (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Auflage, Basel 2024 (zit. BSK DSG- BEARBEITERIN)

CASANOVA THOMAS, Datenverknüpfung in ausgewählten Bereichen: Gesundheitswesen, in: Datenverknüpfung, Problematik und rechtlicher Rahmen / L'interconnexion de données, Problématique et cadre juridique, EPINEY ASTRID/PROBST THOMAS/GAMMENTHALER NINA (Hrsg.), Forum Europarecht, Zürich 2011, SS. 41-52

DONATSCH ANDREAS/THOMMEN MARC/WOHLERS WOLFGANG, Strafrecht IV: Delikte gegen die Allgemeinheit, in: JOSITSCH (Hrsg.) Zürcher Grundrisse des Strafrechts, 5. Aufl., Zürich 2017

FELLMANN WALTER/ZINDEL GAUDENZ G., Kommentar zum Anwaltsgesetz: Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) BGFA, 2. Aufl., Zürich/Basel/Genf 2011 (zit: BEARBEITERIN, Kommentar zum Anwaltsgesetz)

FELLMANN WALTER, Anwaltsrecht, 2. Auflage, Bern 2017 (zit. WALTER)

FÖRSTER MORITZ, Keine Garantien: Microsoft muss EU-Daten an USA übermitteln, 21. Juli 2025, abrufbar unter: https://www.heise.de/news/Nicht-souveraen-Microsoft-kann-Sicherheit-von-EU-Daten-nicht-garantieren-10494684.html

GAUCH PETER/STÖCKLI HUBERT (Hrsg.), Präjudizienbuch OR, Die Rechtsprechung des Bundesgerichts (1875-2023), 11. Auflage, Zürich 2025 (zit. BEARBEITERIN, Präjudizienbuch OR)

GRAF DAMIAN K. (Hrsg.), StGB Annotierter Kommentar, Bern 2020 (zit. BEARBEITERIN, StGB Annotierter Kommentar)

HÜRLIMANN DANIEL/STEIGER MARTIN, Auf dem Weg zur digitalen Anwaltskanzlei trotz Berufsgeheimnis und Datenschutz, Anwaltsrevue 5/2021, SS.199-205

HUSI-STÄMPFLI SANDRA/MORAND ANNE-SOPHIE, Datenschutzrecht, 2. Auflage, Zürich 2024

KÖCHLI ROLAND, KI im Einsatz, Anwaltsrevue 2024, SS. 372-379

KOHLMEIER SVEN, Der Einsatz von KI: Was wir juristisch wissen und was nicht; 25. April 2024, abrufbar unter: https://www.swissict.ch/der-einsatz-von-ki-was-wir-juristisch-wissen-und-was-nicht/ (zit. KOHLMEIER, Der Einsatz von KI: Was wir juristisch wissen und was nicht)

KOHLMEIER SVEN, KI-Einsatz in Anwaltskanzleien und Unternehmen, 1. März 2024, abrufbar unter: https://wickipartners.ch/news/ki-in-anwaltskanzleien (zit. KOHLMEIER, KI-Einsatz in Anwaltskanzleien und Unternehmen)

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht, 4. Aufl., Basel 2019 (zit: BSK StGB-BEARBEITERIN)

SAV-Wegleitung für IT-Outsourcing und Cloud-Computing, abrufbar unter: https://digital.sav-fsa.ch/documents/1060627/1169162/20221111_cloud+guidelines_D.pdf/20669277-0dc0-4f60-1e69-3d9386f469f8?t=1676907814384 (zuletzt besucht am 24. Juli 2025).

SAV-Wegleitung für den Umgang mit künstlicher Intelligenz, abrufbar unter: https://digital.sav-fsa.ch/documents/1060627/0/SAV-Wegleitung_f%C3%BCr_den_Umgang_mit_k%C3%BCnstlicher_Intelligenz_16.2.25.pdf/0b498c8a-85aa-e089-32a2-18da59ee658c?t=1740988650613 (zuletzt besucht am 11. August 2025).

SCHILLER KASPAR, Schweizerisches Anwaltsrecht, Zürich/ Basel/Genf 2009

SCHWARZENEGGER CHRISTIAN/THOUVENIN FLORENT/STILLER BURKHARD, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Schriften aus dem ITSL, herausgegeben von Florent Thouvenin und Rolf H. Weber, Zürich/Basel/Genf 2019, abrufbar unter https://digital.sav-fsa.ch/digitale-kanzlei-nutzung-von-clouddiensten (zuletzt besucht am 22. Juli 2025)

SCHWARZENEGGER CHRISTIAN/THOUVENIN FLORENT/STILLER BURKHARD/GEORGE DAMIAN, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue 2019, SS. 25-32

STRAUB WOLFGANG, Vom Keller zur Cloud – digitales Arbeiten in der Anwaltskanzlei, in: Jusletter 1. Mai 2017, abrufbar unter: https://www.it-recht.ch/wp-content/uploads/2017/05/Jusletter_vom-keller-zur-cloud_d8e198657b_de.pdf

SURY URSULA/GOGNIAT YVES, Umzug einer Kanzlei in die Cloud, Anwaltsrevue 2015, SS. 201–206

TRECHSEL STEFAN/VEST HANS (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. Aufl., Zürich 2021 (zit: PK StGB-BEARBEITERIN)

WOHLERS WOLFGANG, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Zürich 2016 (zit. WOHLERS, Auslegung einer Datenbearbeitung und Berufsgeheimnis)

WOHLERS WOLFGANG, Outsourcing durch Berufsgeheimnisträger, digma 2016, SS. 114-117 (zit. WOHLERS, Outsourcing durch Berufsgeheimnisträger)