# MusterklauselN für das Schweizer Berufs- und Amtsgeheimnis beim EInsatz von Schweizer Lösungen Für Künstliche intelligenz (KI)[[1]](#footnote-1)

Die folgenden Bestimmungen werden in den Vertrag zwischen Dienstleister und Kunden integriert und können auf bestimmte Dienstleistungen, wie zum Beispiel Endpoints für grosse Sprachmodelle, beschränkt sein; sie setzen einen hinreichenden Auftragsverarbeitungsvertrag (AVV) voraus:

## Umfassende Variante

*Der Dienstleister nimmt zur Kenntnis, dass die Bearbeitung von Kundendaten dem schweizerischen Amts-, Berufs- und sonstigen gesetzlichen Geheimhaltungspflichten (z.B. Art. 320 ff. Schweizerisches Strafgesetzbuch) unterliegen kann. Zu den in dieser Klausel referenzierten Kundendaten gehören alle Informationen, die der Kunde im Rahmen der Inanspruchnahme der Dienstleistung dem Dienstleister übermittelt, von diesem für den Kunden beschafft (z.B. aus Drittservices) oder im Rahmen die Dienstleistung generiert (z.B. Output generativer KI) werden. Der Dienstleister wird Kundendaten so lange vertraulich behandeln, wie es das anwendbare Recht vorschreibt (auch nach Beendigung des Vertrages) und sie nur so verwenden, wie es für die Aufrechterhaltung oder Erbringung der Dienstleistung erforderlich ist. Kundendaten dürfen nicht an Dritte weitergeben werden, ausser dies ist erforderlich, um den Anweisungen des Kunden, den Pflichten gemäss Vertrag oder einer nach Schweizer Recht gültigen, verbindlichen und vollstreckbaren Anordnung einer zuständigen Schweizer Behörde (wie einer gerichtlichen Verfügung) nachzukommen. Der Dienstleister wird im Falle einer staatlichen Anordnung auf Zugang zu, oder Herausgabe von, Kundendaten zusätzlich zu seinen anderen Verpflichtungen, und bevor er einer solchen Anordnung nachkommt, (a) sofern rechtlich zulässig den Kunden informieren (und, wenn dies rechtlich nicht zulässig ist, versuchen, die Erlaubnis zur Information des Kunden einzuholen) und dem Kunden es ermöglichen eine solche Anordnung anzufechten und einzuschränken, sowie, solange der Kunde nichts anderes instruiert (und auf Kosten des Kunden), (b) selbst alle rechtlichen Möglichkeiten ausschöpfen, um eine solche Anordnung unter Berufung auf die vorstehend genannten gesetzlichen Geheimnispflichten anzufechten und einzuschränken (z.B. durch Siegelung), und in jedem Fall nur das Minimum an Kundendaten herausgeben, das zur Erfüllung der Anordnung erforderlich ist. Der Dienstleister wird seinen Mitarbeitenden und Unterakkordanten mindestens gleichwertige Pflichten wie in dieser Klausel vertraglich auferlegen, soweit sie Zugang zu Kundendaten im Klartext haben können. Er wird Mitarbeitenden (auch der Unterakkordanten) Zugang zu Kundendaten im Klartext nur auf einer Need-to-know-Basis gewähren und nur (i) mit vorheriger Einzelgenehmigung des Kunden, (ii) soweit nötig zur Behebung eines BCM-Notfalls, der keine Verzögerung zulässt, oder (iii) soweit dies erforderlich ist, um einer nach Schweizer Recht gültigen, verbindlichen und vollstreckbaren Anordnung einer zuständigen Schweizer Behörde nachzukommen. Wenn der Dienstleister Leistungen Dritter nutzt, wird er angemessene Massnahmen ergreifen, damit diese Dritten keinen Klartext-Zugang zu den Kundendaten erhalten können. Im Falle des Betriebs von API für KI-Dienstleistungen (z.B. LLM-Endpoints) dürfen weder die Anfragen bzw. der Input der Kunden noch die Antwort bzw. der Output der KI gespeichert oder protokolliert werden ("Zero Data Retention", kein "Data at-rest"). Ein Abuse Monitoring durch Mitarbeitende, das zum Zugriff auf Kundendaten im Klartext führt, ist untersagt, ebenso eine Verwendung der Kundendaten für eigene Zwecke (insbesondere Trainingszwecke). Die Dienstleistungen, bei welchen Kundendaten in den Systemen des Dienstleisters im Klartext vorliegen (einschliesslich des Betriebs von API), dürfen ausschliesslich in der Schweiz erbracht werden. Kundendaten im Klartext dürfen weder ins Ausland übermittelt noch aus dem Ausland zugänglich sein (gemeint sind auch verschlüsselte Daten, sofern der Schlüssel einer Person im Ausland zugänglich ist). Alle Bestimmungen des zwischen dem Kunden und dem Dienstleister geschlossenen Auftragsverarbeitungsvertrags (AVV), insbesondere die technischen und organisatorischen Massnahmen des Dienstleisters zum Schutz von Personendaten, die Genehmigung neuer Unterauftragsbearbeiter und die Benachrichtigung über Datensicherheitsverletzungen, gelten sinngemäss auch für alle Kundendaten. Die Bestimmungen dieser Klausel, die einen besseren Schutz von Kundendaten vorsehen, gehen jedoch dem AVV und den restlichen vertraglichen Bestimmungen mit dem Dienstleister vor. Die Massnahmen des Dienstleisters zur Informationssicherheit müssen im Hinblick auf die vorstehend genannten gesetzlichen Geheimnispflichten angemessen sein. Der Anbieter weist ein angemessenes Mass an Informationssicherheit nach, indem er dem Kunden jährlich und ohne zusätzliche Kosten* ***[Option 1 (besser):*** *einen SOC 2 Typ 2 oder gleichwertigen Prüfbericht* ***| Option 2:*** *einen angemessenen Prüfbericht****]*** *[[2]](#footnote-2) vorlegt, der die gesamte Verarbeitung von Kundendaten abdeckt; dem Kunden bleibt (auf dessen Kosten) ein Recht zur Prüfung der Einhaltung dieser Klausel vorbehalten. Der Dienstleister behebt etwaige Defizite ohne schuldhaftes Zögern. Für schuldhafte Verletzungen dieser Klausel haftet der Dienstleister mindestens bis zu einer Summe der* ***[****doppelten jährlichen Gebühren aller Dienstleistungen unter dem Vertrag mit dem Kunden****]*** *[[3]](#footnote-3).*

## Variante mit Optionen

***[****Die nachfolgenden Bestimmungen zum Berufs- und Amtsgeheimnis gelten für folgende Dienstleistungen als vereinbart:*

🞏 *Alle* 🞏 *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****]***

*Der Dienstleister nimmt zur Kenntnis, dass die Bearbeitung von Kundendaten dem schweizerischen Amts-, Berufs- und sonstigen gesetzlichen Geheimhaltungspflichten (z.B. Art. 320 ff. Schweizerisches Strafgesetzbuch) unterliegen kann. Zu den in dieser Klausel referenzierten Kundendaten gehören alle Informationen, die der Kunde im Rahmen der Inanspruchnahme der Dienstleistung dem Dienstleister übermittelt, von diesem für den Kunden beschafft (z.B. aus Drittservices) oder im Rahmen die Dienstleistung generiert (z.B. Output generativer KI) werden.*

*Der Dienstleister wird Kundendaten so lange vertraulich behandeln, wie es das anwendbare Recht vorschreibt (auch nach Beendigung des Vertrages) und sie nur so verwenden, wie es für die Aufrechterhaltung oder Erbringung der Dienstleistung erforderlich ist. Kundendaten dürfen nicht an Dritte weitergeben werden, ausser dies ist erforderlich, um den Anweisungen des Kunden, den Pflichten gemäss Vertrag oder einer nach Schweizer Recht gültigen, verbindlichen und vollstreckbaren Anordnung einer zuständigen Schweizer Behörde (wie einer gerichtlichen Verfügung) nachzukommen. Der Dienstleister wird im Falle einer staatlichen Anordnung auf Zugang zu, oder Herausgabe von, Kundendaten zusätzlich zu seinen anderen Verpflichtungen, und bevor er einer solchen Anordnung nachkommt, (a) sofern rechtlich zulässig den Kunden informieren (und, wenn dies rechtlich nicht zulässig ist, versuchen, die Erlaubnis zur Information des Kunden einzuholen) und dem Kunden es ermöglichen eine solche Anordnung anzufechten und einzuschränken, sowie, solange der Kunde nichts anderes instruiert (und auf Kosten des Kunden), (b) selbst alle rechtlichen Möglichkeiten ausschöpfen, um eine solche Anordnung unter Berufung auf die vorstehend genannten gesetzlichen Geheimnispflichten anzufechten und einzuschränken (z.B. durch Siegelung), und in jedem Fall nur das Minimum an Kundendaten herausgeben, das zur Erfüllung der Anordnung erforderlich ist.*

*Der Dienstleister wird seinen Mitarbeitenden und Unterakkordanten mindestens gleichwertige Pflichten wie in dieser Klausel vertraglich auferlegen, soweit sie Zugang zu Kundendaten im Klartext haben können. Er wird Mitarbeitenden (auch der Unterakkordanten) Zugang zu Kundendaten im Klartext nur auf einer Need-to-know-Basis gewähren.* ***[****Der Kunde wird dem Dienstleister Kundendaten, die diesen Regelungen zum Berufs- und Amtsgeheimnis unterliegen sollen, ausserhalb der Nutzung der Dienstleistungen (z.B. via API) nur über Kanäle übermitteln, die seitens Dienstleister hierfür als geeignet bezeichnet wurden.****]***

***[****Es gelten ferner folgende Bestimmungen, sofern sie für die betreffende Dienstleistung vereinbart sind (z.B. durch Vermerk im Leistungsbeschrieb):****]***

* ***[Restricted Operator Access:]*** *Der Dienstleister gewährt Mitarbeitenden (auch der Unterakkordanten) Zugang zu Kundendaten im Klartext nur (i) mit vorheriger Einzelgenehmigung des Kunden, (ii) soweit nötig zur Behebung eines BCM-Notfalls, der keine Verzögerung zulässt, oder (iii) soweit dies erforderlich ist, um einer nach Schweizer Recht gültigen, verbindlichen und vollstreckbaren Anordnung einer zuständigen Schweizer Behörde nachzukommen. Wenn der Dienstleister Leistungen Dritter nutzt, wird er angemessene Massnahmen ergreifen, damit diese Dritten keinen Klartext-Zugang zu den Kundendaten erhalten können.*
* ***[ZDR:]*** *Im Falle des Betriebs von API für KI-Dienstleistungen (z.B. LLM-Endpoints) dürfen weder die Anfragen bzw. der Input der Kunden noch die Antwort bzw. der Output der KI gespeichert oder protokolliert werden ("Zero Data Retention", kein "Data at-rest"). Ein Abuse Monitoring durch Mitarbeitende, das zum Zugriff auf Kundendaten im Klartext führt, ist untersagt, ebenso eine Verwendung der Kundendaten für eigene Zwecke (insbesondere Trainingszwecke).*
* ***[CH-only:]*** *Die Dienstleistungen, bei welchen Kundendaten in den Systemen des Dienstleisters im Klartext vorliegen (einschliesslich des Betriebs von API), dürfen ausschliesslich in der Schweiz erbracht werden. Kundendaten im Klartext dürfen weder ins Ausland übermittelt noch aus dem Ausland zugänglich sein (gemeint sind auch verschlüsselte Daten, sofern der Schlüssel einer Person im Ausland zugänglich ist).*
* ***[EU/EFTA-only****: Kundendaten dürfen ausschliesslich in der Schweiz gespeichert ("at-rest") und ausschliesslich in Ländern der EU oder der EFTA auf andere Weise bearbeitet werden ("in-process"). Ein Zugriff auf Kundendaten im Klartext durch Behörden von ausserhalb der Schweiz muss mit an Sicherheit grenzende Wahrscheinlichkeit ausgeschlossen sein.****]***

*Alle Bestimmungen des zwischen dem Kunden und dem Dienstleister geschlossenen Auftragsverarbeitungsvertrags (AVV), insbesondere die technischen und organisatorischen Massnahmen des Dienstleisters zum Schutz von Personendaten, die Genehmigung neuer Unterauftragsbearbeiter und die Benachrichtigung über Datensicherheitsverletzungen, gelten sinngemäss auch für alle Kundendaten. Die Bestimmungen dieser Klausel, die einen besseren Schutz von Kundendaten vorsehen, gehen jedoch dem AVV und den restlichen vertraglichen Bestimmungen mit dem Dienstleister vor. Die Massnahmen des Dienstleisters zur Informationssicherheit müssen im Hinblick auf die vorstehend genannten gesetzlichen Geheimnispflichten angemessen sein. Der Anbieter weist ein angemessenes Mass an Informationssicherheit nach, indem er dem Kunden jährlich und ohne zusätzliche Kosten* ***[Option 1 (besser):*** *einen SOC 2 Typ 2 oder gleichwertigen Prüfbericht* ***| Option 2:*** *einen angemessenen Prüfbericht****]****vorlegt, der die gesamte Verarbeitung von Kundendaten abdeckt; dem Kunden bleibt (auf dessen Kosten) ein Recht zur Prüfung der Einhaltung dieser Klausel vorbehalten. Der Dienstleister behebt etwaige Defizite ohne schuldhaftes Zögern. Für schuldhafte Verletzungen dieser Klausel haftet der Dienstleister mindestens bis zu einer Summe der* ***[****doppelten jährlichen Gebühren aller Dienstleistungen unter dem Vertrag mit dem Kunden****]****.*

1. Dies dient ausschliesslich zu Informationszwecken und stellt keine Rechtsberatung dar. Die Nutzung erfolgt auf eigene Gefahr. Wenn Sie sich nicht sicher sind, holen Sie Rechtsrat. Fragen: [dataprivacy@vischer.com](mailto:dataprivacy@vischer.com). Die aktuellste Version steht auf [www.rosenthal.ch](http://www.rosenthal.ch) bereit. [↑](#footnote-ref-1)
2. ISO 27001, auf die sich viele Anbieter beziehen, ist kein genügender Nachweis für eine angemessene Datensicherheit. Ein Audit-Bericht ist erforderlich, wonach ein unabhängiger Dritter die einzelnen Sicherheitsmassnahmen überprüft und bestätigt hat, dass sie vorhanden und wirksam sind ("Typ 2"). "SOC 2" ist ein standardisiertes Format für solche Audit-Berichte und weit verbreitet. In der Praxis gibt es drei Probleme: Erstens sind diese Berichte für den Anbieter kostspielig (sie können jedoch für alle Kunden verwendet werden). Zweitens müssen sie die gesamte Verarbeitung von Kundeninhalten abdecken, nicht nur die Hosting- und Rechenzentrumsleistungen, die möglicherweise von einem Unterakkordanten eingekauft wurden (der SOC 2 Typ 2-Bericht eines involvierten Unterakkordanten ist daher nicht ausreichend, da er nicht die gesamte Wertschöpfungskette abdeckt). Drittens erfordert ihre Überprüfung Expertenwissen. [↑](#footnote-ref-2)
3. Siehe BGE 145 II 229. Der Kunde muss die Möglichkeit haben, den Dienstleister bis zu einem gewissen Grad haftbar zu machen, wenn dieser das Berufsgeheimnis verletzt. Wenn die Haftung ausser für grobe Fahrlässigkeit und Vorsatz ausgeschlossen ist, reicht dies in der Regel nicht aus. [↑](#footnote-ref-3)