# Musterklausel für das Schweizer Berufs- und Amtsgeheimnis beim EInsatz von Cloud-Lösungen[[1]](#footnote-1)

Unternehmen und Institutionen, die einem Schweizer Berufs- oder Amtsgeheimnis unterstehen (z.B. Art. 320 ff. Schweizerisches Strafgesetzbuch), dürfen einem Dienstleister geheime Daten nur unter der Einhaltung von gewissen Voraussetzungen zur Verfügung stellen. Sie müssen sicherstellen, dass der Dienstleister ein angemessenes Mass an Informationssicherheit bietet und bestimmte Regelungen in den Vertrag mit dem Dienstleister aufgenommen wurden. Die Musterklausel in diesem Dokument berücksichtigt den in der Schweiz üblichen Standard für Cloud-Lösungen. Staatliche Organe müssen noch weitere Voraussetzungen prüfen, regulierte Unternehmen ebenfalls.

"**Kundendaten**" beziehen sich alle Informationen, die der Kunde ("**Kunde**") in der Cloud-Lösung (die "**Dienstleistung**") des Dienstleisters (der "**Dienstleister**") bearbeitet, dem Dienstleister anderweitig zur Verfügung stellt oder die dieser zur Bearbeitung für den Kunden erhält. Kontodaten, für den Betrieb nötige Identifikatoren oder Ressourcenbezeichnung sowie Nutzungsstatistiken gehören normalerweise nicht dazu (sie dürfen daher keine dem Berufs- oder Amtsgeheimnis unterliegenden Daten enthalten). Es ist zu beachten, dass das Schweizer Berufsgeheimnis und ebenso das Amtsgeheimnis *nicht auf* Personendaten (d.h. Informationen über identifizierbare natürliche Personen) beschränkt ist, sondern auch Informationen über juristische Personen, Behörden und andere Stellen umfassen kann. Die Musterklausel ist in den Vertrag zwischen dem Dienstleister und dem Kunden (der "**Vertrag**") aufzunehmen.

Musterklausel:

*"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.[[2]](#footnote-2) Der Dienstleister wird Kundendaten[[3]](#footnote-3) so lange vertraulich behandeln, wie es das anwendbare Recht vorschreibt (auch nach Beendigung des Vertrages)[[4]](#footnote-4) und sie nur so verwenden, wie es für die Aufrechterhaltung oder Erbringung der Dienstleistung erforderlich ist.[[5]](#footnote-5) Kundendaten dürfen nicht an Dritte weitergeben werden, ausser dies ist erforderlich, um den Anweisungen des Kunden, den Pflichten gemäss Vertrag oder einer gültigen und verbindlichen Anordnung einer zuständigen staatlichen Behörde (wie einer gerichtlichen Verfügung) nachzukommen.[[6]](#footnote-6) Der Dienstleister wird im Falle einer 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 nicht der Fall ist, versuchen, die Erlaubnis zur Information des Kunden einzuholen) und dem Kunden es ermöglichen eine solche Anordnung anzufechten und einzuschränken, sowie (b) selbst alle rechtlichen Möglichkeiten ausschöpfen, um eine solche Anordnung auf der Grundlage von Mängeln nach dem Recht der anfordernden Behörde, dem sonst anwendbaren Recht und dem Prinzip der 'International Comity' sowie etwaiger Konflikte mit dem schweizerischen Recht anzufechten und einzuschränken, und in jedem Fall nur das Minimum an Kundendaten herausgeben, das zur Erfüllung der Anordnung erforderlich ist.[[7]](#footnote-7) Der Dienstleister wird seinen Mitarbeitenden und Unterakkordanten mindestens gleichwertige Pflichten wie in dieser Klausel auferlegen, soweit sie Zugang zu Kundendaten im Klartext haben können,[[8]](#footnote-8) und Mitarbeitenden (auch der Unterakkordanten) Zugang zu Kundendaten im Klartext nur auf einer Need-to-know-Basis gewähren und nur (i) mit vorheriger Genehmigung des Kunden [oder soweit zur Vertragserfüllung zwingend nötig (und nur den Mitarbeitenden des Dienstleisters, nicht der Unterakkordanten)][[9]](#footnote-9), (ii) soweit nötig zur Behebung eines BCM-Notfalls, der keine Verzögerung zulässt, oder (iii) soweit dies erforderlich ist, um einer gültigen und verbindlichen Anordnung einer zuständigen staatlichen Behörde (wie etwa einer gerichtlichen Verfügung) nachzukommen.[[10]](#footnote-10) Wenn der Dienstleister Leistungen Dritter nutzt, wird er angemessene Massnahmen ergreifen, damit diese Anbieter keinen Klartext-Zugang zu den Kundendaten erhalten.[[11]](#footnote-11) Alle Bestimmungen des zwischen dem Kunden und dem Dienstleister geschlossenen Auftragsverarbeitungsvertrags, 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 Kundendaten.[[12]](#footnote-12) Der Anbieter weist ein angemessenes Mass an Informationssicherheit nach, indem er dem Kunden jährlich und ohne zusätzliche Kosten einen SOC 2 Typ 2 oder gleichwertigen Prüfbericht vorlegt, der die gesamte Verarbeitung von Kundendaten abdeckt. Er behebt etwaige Mängel ohne schuldhaften Verzug.[[13]](#footnote-13)"*

Die obige Musterklausel wurde auf Basis von Erkenntnissen aus Verhandlungen mit Hyperscalern und Cloud-Service-Anbietern erstellt. Diese Klauseln werden erfahrungsgemäss für sie im Falle von Kunden mit Berufs- und Amtsgeheimnispflichten typischerweise akzeptabel sein. Wenn der Dienstleister selbst die Infrastruktur eines Hyperscalers nutzt und seine eigenen Verträge mit einem solchen Hyperscaler im Hinblick auf die obige Musterklausel aktualisieren möchte, sind wir gerne behilflich. Im Falle von Microsoft sollte der Dienstleister zum Beispiel das Äquivalent zu den Standard-Amendments M744 und M329 in Kombination mit dem neuesten DPA (zurzeit: Januar 2024) auf Englisch anfordern, um vergleichbare Bestimmungen zu erhalten. Ausserdem muss der Anbieter möglicherweise bestimmte Serviceoptionen gegenüber dem Hyperscaler aktivieren, um dessen Zugriff auf seine Daten einzuschränken (im Fall von Microsoft kann dies die Speicherung und Verarbeitung in der Schweiz, die "Customer Lockbox" und eine zusätzliche Verschlüsselung umfassen).

Darüber hinaus sollte der Vertrag nach Möglichkeit Schweizer Recht unterliegen mit einem Gerichtsstand in der Schweiz. Die Haftung für unmittelbare Schäden aufgrund einer Verletzung der obigen Musterklausel kann begrenzt sein, darf aber nicht ganz ausgeschlossen werden (selbst wenn Haftungsbeschränkungen nach Schweizer Recht gelten).[[14]](#footnote-14)

Vertragliche Regeln alleine genügen nicht zur Wahrung des Berufs- oder Amtsgeheimnisses. Es müssen jeweils auch sonst angemessene Massnahmen zur Wahrung der Informationssicherheit bestehen. Diese sind auch zu vereinbaren (üblicherweise im Rahmen des Auftragsverarbeitungsvertrags, auf den die Klausel verweist). Hier empfehlen wir, dass diese sog. TOMS (technische und organisatorische Massnahmen der Sicherheit) von einer Fachperson überprüft werden.

Kommen ausländische Anbieter direkt oder indirekt (als Unterakkordanten) zum Einsatz, besteht grundsätzlich ein Restrisiko eines ausländischen Behördenzugriffs. Die Eintrittswahrscheinlichkeit eines solchen Behördenzugriffs muss der Amts- oder Berufsgeheimnisträger einschätzen und es muss hinreichend gering sein, so dass kein Grund zur Annahme besteht, dass es dazu kommt. Es gibt hierzu eine mittlerweile etablierte Methode.[[15]](#footnote-15)

1. Dies dient ausschliesslich zu Informationszwecken und stellt keine Rechtsberatung dar. Die Nutzung erfolgt auf eigene Gefahr. Wenn Sie sich nicht sicher sind, sollten Sie sich Rechtsrat holen. Die Musterklausel darf für Verträge beliebig angepasst werden. Fragen: dataprivacy@vischer.com. Die aktuellste Version steht auf [www.rosenthal.ch](http://www.rosenthal.ch) zum Download bereit. [↑](#footnote-ref-1)
2. Der Dienstleister muss wissen, dass die Bearbeitung möglicherweise beruflichen und anderen gesetzlichen Geheimhaltungspflichten unterliegt. [↑](#footnote-ref-2)
3. Viele Verträge sehen nur vor, dass der Dienstleister sich verpflichtet bestimmte Sicherheitsmassnahmen zu ergreifen. Dies reicht nach Schweizer Recht für Dienstleister (insbesondere für ausländische) nicht aus. Es ist eine vertragliche Verpflichtung des Dienstleisters nötig, die Kundendaten vertraulich zu behandeln. [↑](#footnote-ref-3)
4. Die vertragliche Geheimhaltungsverpflichtung muss über die Laufzeit des Vertrages hinaus bestehen. Nach schweizerischem Recht sehen viele Verträge eine unbegrenzte Geheimhaltung vor. Es reicht jedoch aus zu vereinbaren, dass die Vertraulichkeit so lange besteht, wie es das schweizerische Recht vorschreibt, d.h. solange die durch die Geheimhaltung geschützten Personen ein berechtigtes Interesse an der Geheimhaltung der Informationen haben. [↑](#footnote-ref-4)
5. Informationen, die dem Amts- oder Berufsgeheimnis unterliegen, sollten nicht für andere Zwecke als die des Kunden verwendet werden dürfen (z.B. dürfen sie nicht für Zwecke des Dienstleisters verwendet werden, wie z.B. für das Training von KI-Systemen, für statistische Analysen usw.). [↑](#footnote-ref-5)
6. Diese Ausnahmen sind gerechtfertigt und üblich, denn es gibt Dienstleistungen, bei denen der Dienstleister verpflichtet werden kann, Daten an Behörden herauszugeben. [↑](#footnote-ref-6)
7. Dies ist eine typische kurze "defend-your-data"-Klausel, wie sie von Hyperscalern wie Microsoft verwendet wird (siehe z.B. das Microsoft Data Processing Addendum, Appendix C). Sie ähnelt den Bestimmungen in Klausel 15 der EU Standardvertragsklauseln der Europäischen Kommission. Alternativ können diese Klauseln verwendet werden, sofern sie so abgeändert werden, dass sie Kundendaten (und nicht nur Personendaten) abdecken und mit dem Schweizer Recht im Einklang stehen. [↑](#footnote-ref-7)
8. Die Verpflichtungen in dieser Musterklausel müssen auch den Mitarbeitern und Unterakkordanten des Dienstleisters auferlegt werden. Es reicht nicht aus, dass der Dienstleister für deren Handlungen und Unterlassungen bloss verantwortlich ist. [↑](#footnote-ref-8)
9. In gewissen Fällen kann es erforderlich sein, dass Mitarbeitende eines Dienstleisters für die Vertragserfüllung auf die Daten im Klartext zugreifen. Das sollte jedoch eingeschränkt werden, und möglichst nur den Dienstleister, nicht den Unterakkordanten betreffen (z.B. Hyperscaler). [↑](#footnote-ref-9)
10. Hier geht es nur um den manuellen Zugriff des Dienstleisters auf Kundendaten im Klartext. Dienstleister haben in der Regel selbst ein Interesse daran, einen solchen Zugriff zu beschränken. Dabei kann es sich um Serviceanfragen des Kunden, Notfälle (z.B. Systemausfälle) oder besondere rechtliche Situationen handeln (z.B. eine Strafuntersuchung, in welcher eine Behörde via Provider an Beweismittel gelangen will). [↑](#footnote-ref-10)
11. Wenn der Dienstleister die Infrastruktur eines Hyperscalers nutzt, liegt es in der Regel in der Hand des Dienstleisters, die Kundeninhalte zu verschlüsseln oder anderweitig so zu schützen, dass der Hyperscaler (normalerweise) nicht auf die Kundendaten im Klartext zugreifen kann. Völlig ausgeschlossen werden kann das aber in der Regel nicht, was rechtlich auch nicht nötig ist, solange z.B. eine "defend-your-data" Klausel besteht und angemessene Schutzmassnahmen getroffen sind und das Restrisiko eines ausländischen Behördenzugriffs hinreichend gering ist. [↑](#footnote-ref-11)
12. Weitere Bestimmungen, die im Rahmen des Schweizer Amts- und Berufsgeheimnisses erforderlich sind, sind in der Regel in Auftragsbearbeitungsverträgen enthalten. Zu diesen Bestimmungen gehört die Verpflichtung, den Kunden über neue Unterauftragsbearbeiter mit Zugriff auf Kundeninhalte zu informieren (inkl. Widerspruchs- oder Kündigungsrecht), die TOMS und die Verpflichtung, über jede Sicherheitsverletzung in Bezug auf Kundendaten zu informieren. Auftragsbearbeitungsverträge sind in der Regel auf die Bearbeitung von Personendaten beschränkt; um Kundendaten zu schützen, die keine Personendaten sind, muss der Geltungsbereich dementsprechend erweitert werden. Dies ist in der Regel kein Problem, zumal die Dienstleister Kundendaten normalerweise nicht unterschiedlich behandeln, je nachdem, ob es sich um Personendaten handelt oder nicht. Achtung: Die Figur des Unterauftragsbearbeiters ist nicht ganz deckungsgleich wie jener des Unterakkordanten, aber im Normalfall macht das für vorliegende Zwecke keinen Unterschied. [↑](#footnote-ref-12)
13. 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 Hyperscalers ist daher nicht ausreichend, da er nicht die gesamte Wertschöpfungskette abdeckt). Drittens erfordert ihre Überprüfung Expertenwissen. [↑](#footnote-ref-13)
14. 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-14)
15. Die "Methode Rosenthal" besteht aus einem Excel, mit dem die Eintrittswahrscheinlichkeit in einem systematischen Prozess für einzelne Jurisdiktionen (insbesondere die USA) ermittelt werden kann. Es ist als Open Source unter <https://vischerlnk.com/flara> kostenlos zu beziehen (FAQ: https://vischerlnk.com/flarafaq). [↑](#footnote-ref-15)