Swiss Banking

Cloud-Leitfaden

November 2025
Leitfaden der SBVg
3. Auflage

Inhaltsverzeichnis

Hinweis:
Die Änderungen gegenüber der zweiten Auflage sind im rechtlichen und regulatorischen Leitfaden mit * gekennzeichnet und am Schluss des Dokuments aufgeführt. Blosse redaktionelle Anpassungen ohne materielle Tragweite sind nicht gekennzeichnet.

Vorwort

Die digitale Transformation der Finanzbranche schreitet unaufhaltsam voran und mit ihr die Bedeutung von Cloud-Dienstleistungen für den Finanzsektor. In der vorliegenden dritten Auflage des Cloud-Leitfadens der Schweizerischen Bankiervereinigung (SBVg) reflektieren wir Entwicklungen und Herausforderungen hinsichtlich der Nutzung der Cloud-Technologie durch Banken und Wertpapierhäuser.

Die Wettbewerbsfähigkeit des Schweizer Finanzsektors profitiert von den neuen Technologien: Cloud-Dienstleistungen können Banken und Wertpapierhäusern je nach zugrundeliegendem Sachverhalt einerseits Effizienzsteigerungen, Kostenvorteile und mehr Sicherheit und andererseits auch die Möglichkeit bieten, innovative Dienstleistungen rasch und flexibel zu entwickeln und auf den Markt zu bringen. Gleichzeitig spielen die Resilienz der Infrastruktur von Banken und Wertpapierhäusern sowie das Vertrauen in deren Funktionstüchtigkeit eine zentrale Rolle. Allerdings können Cloud-Dienstleistungen auch zu Risiken wie beispielsweise zu einer möglichen Abhängigkeit von Drittparteien führen und bei unsachgemässer Anwendung allfällige Kontrollverluste nach sich ziehen.

Es gelten rechtliche und regulatorische Auflagen, unabhängig von der eingesetzten Technologie. Insbesondere geht es um die Einhaltung der Berufsgeheimnisse gemäss Bankengesetz und Finanzinstitutsgesetz, die Berücksichtigung datenschutzrechtlicher Vorschriften sowie die Gewährleistung von Datensicherheit und Resilienz, zum Beispiel im Zusammenhang mit kritischen Daten gemäss Rundschreiben der Eidgenössischen Finanzmarktaufsicht (FINMA) 2023/01 – Operationelle Risiken und Resilienz.

Die Auslegung dieser Auflagen und insbesondere deren Umsetzung mittels angemessener technischer und organisatorischer Massnahmen (Kurzform TOM) kann je nach Geschäfts- und Betriebsmodell unterschiedlich herausfordernd sein. Aus diesem Grund hat eine Arbeitsgruppe unter der Leitung der SBVg bereits im Jahr 2019 einen rechtlichen und regulatorischen Leitfaden (nachfolgend «Leitfaden») für den Einsatz von Cloud-Dienstleistungen durch Banken und Wertpapierhäuser erarbeitet. Gegenstand dieses Leitfadens sind Empfehlungen, welche bei der Beschaffung und beim Einsatz von Cloud-Dienstleistungen durch die Institute herangezogen werden können.

Um den seit der Veröffentlichung des Leitfadens erfolgten rechtlichen und regulatorischen Entwicklungen, zum Beispiel im Bereich der Regulierung von operationellen Risiken, gebührend Rechnung zu tragen, wurde der Cloud-Leitfaden aktualisiert.

Der Leitfaden gliedert sich in zwei Teile. Der erste Teil dient der allgemeinen Einführung in die Thematik Cloud. Er veranschaulicht den Nutzen und die Vorteile der Cloud-Technologie für Banken und Wertpapierhäuser, beleuchtet die aus Sicht der SBVg sinnvollen Grundsätze sowie die wichtigsten regulatorischen Fragen im Zusammenhang mit dem Einsatz von Cloud-Dienstleistungen durch Banken und Wertpapierhäuser und bietet Lösungsansätze der SBVg. Der zweite Teil erläutert die rechtlichen und regulatorischen Empfehlungen der SBVg unter Berücksichtigung des Schweizer Rechts.

Ein weiterer wesentlicher Aspekt im Zusammenhang mit der Nutzung von Cloud-Dienstleistungen durch Banken und Wertpapierhäuser, ist die Definition sowie anschliessende Implementierung angemessener technischer und organisatorischer Massnahmen, welche die jeweils anwendbaren geschäftspolitischen

sowie rechtlichen Vorgaben hinsichtlich der Nutzung von Cloud-Technologien konkretisieren sowie operationalisieren. Dieser Herausforderung muss sich jedes Institut individuell unter Berücksichtigung des konkreten Anwendungsfalls stellen.

Das vorliegende Dokument erhebt keinen Anspruch auf Vollständigkeit. Es wird mit Rücksicht auf die zukünftigen technologischen und rechtlichen Entwicklungen aktualisiert und ergänzt. Die jeweils aktuelle Fassung des Leitfadens wird publiziert.

Management Summary

- Die **Benutzung der Cloud-Technologie** ist ein **kritischer Erfolgsfaktor** für die Schweiz und den Finanzplatz. Ein klares Verständnis der rechtlichen und regulatorischen Anforderungen an Banken und Wertpapierhäuser sowie die Fähigkeit, diese mittels angemessener technischer und organisatorischer Massnahmen zu konkretisieren und zu operationalisieren, sind unerlässlich.
- Das vorliegende Dokument stellt einen rechtlich **unverbindlichen Leitfaden** dar, der als Auslegungshilfe für die Praxis bei der Beschaffung und beim Einsatz von Cloud-Dienstleistungen durch die Institute herangezogen werden kann. Er fokussiert auf folgende vier Bereiche:
  - **Steuerung (Governance mit Risk Management):** Auswahl des Cloud-Anbieters und seiner Zulieferer (Unterakkordanten) sowie Zustimmung bei einem Wechsel der Zulieferer
  - **Datenbearbeitung:** Bearbeitung von Bankkundendaten
  - **Behörden und Verfahren:** Transparenz und Zusammenarbeit der Institute und der Cloud-Anbieter im Bereich behördlicher und gerichtlicher Massnahmen
  - **Audit:** Prüfung der Cloud-Dienstleistungen und der zur Erbringung der Dienstleistungen eingesetzten Cloud-Infrastruktur
- Der Leitfaden zeigt Instituten umsetzbare Lösungsansätze für die wichtigsten rechtlichen und regulatorischen Anforderungen auf. Der buchstäbliche Schlüsselaspekt der Cloud-Nutzung, die Einschätzung der **Risiken** und die daraus resultierende Definition angemessener technischer und organisatorischer Massnahmen, verbleiben **bei den einzelnen Instituten.**

Cloud-Dienstleistungen in der Praxis

Nutzen und Vorteile von Cloud-Dienstleistungen

Die digitale Transformation der Finanzbranche schreitet unaufhaltsam voran und mit ihr die Bedeutung von Cloud-Dienstleistungen für den Finanzsektor. Cloud-Dienstleistungen können Banken und Wertpapierhäusern je nach zugrundeliegendem Sachverhalt einerseits Effizienzsteigerungen und Kostenvorteile und andererseits auch die Möglichkeit bieten, innovative Dienstleistungen rasch und flexibel zu entwickeln und auf den Markt zu bringen. Zudem ermöglichen spezialisierte Cloud-Anbieter unter Umständen mehr Sicherheit für die Infrastruktur von Banken und Wertpapierhäusern. Damit sind Cloud-Dienstleistungen ein kritischer Erfolgsfaktor für den Schweizer Finanzplatz.

Viele Kundinnen und Kunden nutzen Cloud-Dienstleistungen im alltäglichen Leben, ohne sich dessen immer bewusst zu sein. Sie versenden Mails, streamen Musik und Filme oder speichern Urlaubsfotos auf der Cloud. Was im Privaten funktioniert, ist auch für hoch spezialisierte Institute und ihr komplexes Geschäft möglich. Unabhängig von der eingesetzten Technologie gelten jedoch rechtliche und regulatorische Auflagen.

Mit der Migration von Infrastruktur und Prozessen in eine Cloud können Institute die Zeit bis zur Marktreife für innovative Produkte und Dienstleistungen tendenziell verkürzen und damit ihre Wettbewerbsfähigkeit steigern. In der Cloud sind neue Technologien, wie beispielsweise künstliche Intelligenz, ohne grosse Investitionen in eigene Hardware und Software nutzbar. Durch Zugang zu einem grossen Datenpool und die entsprechende Rechenleistung wird die Analyse von grossen Datenmengen in Echtzeit ermöglicht. Damit können beispielsweise innovative und massgeschneiderte Beratungsdienstleistungen für die einzelne Kundin oder den einzelnen Kunden angeboten oder komplexe Compliance- und Risk-Prozesse automatisiert werden. Auch in der Entwicklung und im Testen von neuen Applikationen und Systemen ermöglicht die Cloud deutliche Effizienzgewinne: Innovative Ideen können einfach und flexibel ausprobiert, vertieft oder verworfen werden und sind dadurch leichter zu realisieren. Schliesslich kann das Funktionsangebot an Cloud-Dienstleistungen grundsätzlich im «Self Service» zu variablen Kosten genutzt werden, da nur direkt bezogene Leistungen abgerechnet werden. Dies eröffnet Instituten beispielsweise mehr Handlungsspielraum bei der Reaktion auf Bedürfnisschwankungen, indem benötigte IT-Ressourcen flexibel zu- oder abgeschaltet werden können.

Der Aufbau oder Einkauf der entsprechenden Kompetenzen und Ressourcen in der eigenen IT-Infrastruktur sind nicht mehr nötig. Dadurch wird die Nutzung von Cloud-Dienstleistungen gerade für kleine Institute attraktiv. Technologien, die früher grossen Unternehmen vorbehalten waren, werden auch für kleine Institute zugänglich und ermöglichen signifikante Skaleneffekte.[1] Allerdings müssen neue Kompetenzen für die effiziente und wirksame Verwaltung und Steuerung von bezogenen Cloud-Dienstleistungen aufgebaut und optimiert werden. Auch die Erfüllung der steigenden Anforderungen an den IT-Betrieb (IT-Sicherheit, Nachführen von Patches[2], Management des IT-Infrastruktur-Lifecycles) wird durch eine Cloud-Nutzung erleichtert.

Bei Schweizer Instituten ist ein zunehmendes Bewusstsein für die Nutzung von Cloud-Dienstleistungen zu beobachten. Gleichzeitig hat sich zwischen nationalen und internationalen Cloud-Anbietern erfreulicherweise eine Wettbewerbssituation eingestellt. Die zunehmende Inanspruchnahme von Cloud-Dienstleistungen wird den Finanzplatz und das Finanzökosystem in der Schweiz in Zukunft weiter stärken.

---

1 Aufgrund einer marginalen Kostengleichung können viele Institute eine eigene Cloud nicht zu den gleichen Kosten bereitstellen wie spezialisierte Cloud-Anbieter. Mit der Cloud können IT-Ressourcen beliebig zu- oder abgeschaltet und so präzise auf die schwankenden Erfordernisse der Geschäftstätigkeit abgestimmt werden.

2 Ein Programm, das Fehler in (meist grossen) Anwendungsprogrammen repariert.

Cloud Computing ist ein Modell der Datenverarbeitung, mit dem bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zugegriffen werden kann. Diese können schnell und mit minimalem Verwaltungsaufwand beziehungsweise geringer Serviceprovider-Interaktion zur Verfügung gestellt werden. Die Cloud kann in drei Varianten (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (Saas)) genutzt werden. Die Art der Cloud unterscheidet sich je nach Art der Bereitstellung (Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud).[3]

Grundsätzliche Überlegungen zur Nutzung von Cloud-Dienstleistungen

Abhängig vom institutsspezifischen Geschäfts- und Betriebsmodell sowie der jeweiligen Strategie sollten in einem ersten Schritt konkrete geschäftspolitische Ziele für die Nutzung von Cloud-Dienstleistungen festgelegt werden. In einem zweiten Schritt wird empfohlen, die dazugehörigen rechtlichen sowie regulatorischen Voraussetzungen zu identifizieren und auszulegen. Beides soll daraufhin in betriebsinternen Vorgaben, einschliesslich Vorgaben für technische und organisatorische Massnahmen[4] zur Auswahl, zum Einsatz und zur Kontrolle von Cloud-Dienstleistungen, konkretisiert werden.[5] Diese Vorgaben werden typischerweise im Rahmen institutsweiter Cloud-Projekte unter Einbezug einer Vielzahl von Stakeholdern und einer hohen Arbeitsteilung auf- bzw. umgesetzt. Eine verbindliche Governance mit klaren Aufgaben, Kompetenzen und Verantwortlichkeiten (inkl. Kontrollen) stellt dabei den ordnungsgemässen Betrieb nach Projektabschluss sicher.

Zusammenfassend kann festgehalten werden, dass es sich bei der Auswahl, der Beschaffung sowie beim Betrieb von Cloud-Dienstleistungen um einen stark arbeitsteiligen Prozess handelt, der durch eine Vielzahl geschäftspolitischer bzw. institutsspezifischer sowie externer Rahmenbedingungen gekennzeichnet ist.

Aus einer rechtlichen Sicht steht dabei das Management von Dienstleistern im Vordergrund; die jeweils anwendbaren rechtlichen sowie regulatorischen Rahmenbedingungen hängen insbesondere vom Zielbetriebsmodell («Target Operating Model») des Instituts, den Eigenschaften des jeweiligen Dienstleisters (Cloud-Anbieter), der Art der betroffenen Daten und vom Ort ihrer Datenbearbeitung, einschliesslich des Datenzugriffs beispielsweise bei Wartungsarbeiten, ab. Dabei gilt der Grundsatz, dass die Rahmenbedingungen strenger sind, je sensitiver die betroffenen Daten sind und je mehr Auslandsbezug die Datenbearbeitung aufweist.

---

3 Definition nach NIST (2011), abrufbar unter: https://csrc.nist.gov/publications/detail/sp/800-145/final.

4 Die Definition und Implementierung von angemessenen technischen und organisatorischen Massnahmen ist keine rechtliche Frage.

5 Dieses Vorgehen wurde in Bezug auf Personendaten zum Beispiel auch im totalrevidierten Datenschutzgesetz (DSG) ausdrücklich in Art. 7 Abs. 2 DSG abgebildet.

Generell gilt, dass ein Cloud-Anbieter diejenigen Rahmenbedingungen einhalten muss, welche auf das jeweilige Institut im Sinne eines Auftraggebers anwendbar sind, weshalb ihm die Pflichten entsprechend überbunden werden müssen. Daher ist es wichtig, dass das Institut über einen ausreichenden Reifegrad hinsichtlich der eigenen «Daten-Organisation» inklusive Daten und Risk Governance und deren granularen Steuerung verfügt und der Cloud-Anbieter genügend Flexibilität aufweist.

Zentrale Lösungsansätze der SBVg im Leitfaden

Der vorliegende Leitfaden enthält – ungeachtet allfälliger rechtlicher und regulatorischer Pflichten – rechtlich nicht-bindende Empfehlungen, die bei der Beschaffung und beim Einsatz von Cloud-Dienstleistungen durch Institute herangezogen werden können. Ausserdem enthält er auch Auslegungen der im Zusammenhang mit Cloud-Dienstleistungen anwendbaren Rechtsgrundlagen. Er fokussiert auf vier Bereiche:

- **Steuerung (Governance mit Risk Management):** Auswahl des Cloud-Anbieters und seiner Zulieferer (Unterakkordanten) sowie Zustimmung bei einem Wechsel der Zulieferer
- **Datenbearbeitung:** Bearbeitung von Bankkundendaten
- **Behörden und Verfahren:** Transparenz und Zusammenarbeit der Institute und der Cloud-Anbieter im Bereich behördlicher und gerichtlicher Massnahmen
- **Audit:** Prüfung der Cloud-Dienstleistungen und der zur Erbringung der Dienstleistungen eingesetzten Cloud-Infrastruktur

Der Leitfaden zeigt umsetzbare Lösungsansätze für die regulatorischen Anforderungen auf. Die SBVg übernimmt damit eine wichtige Aufgabe zu Gunsten des Schweizer Finanzplatzes. Gleichzeitig sollen die Institute bei der Anwendung des Leitfadens ihre Grösse, die Komplexität sowie die Aufbau- und Ablauforganisation ihres Geschäftsmodells risikobasiert und verhältnismässig berücksichtigen.

A) Auswahl und Wechsel von Cloud-Anbietern und Zulieferern[6]

Zweck der im Leitfaden aufgeführten Empfehlungen:
Das Institut soll **jederzeit über die wichtigsten Informationen verfügen, welche für die Auswahl eines Cloud-Anbieters** notwendig sind. Diese sollen auch die wesentlichen Zulieferer des Anbieters berücksichtigen.

6 Siehe dazu nachfolgend Kapitel II:5 des Leitfadens.

Cloud-Anbieter nutzen zum Zwecke einer effizienten und kompetitiven Leistungserbringung die Möglichkeit, Betriebsmodelle, die zum Einsatz kommenden Technologien, konzerninterne und -externe Leistungserbringer und weitere massgebliche Faktoren festzulegen und zu ändern (sogenannte Design-Autorität).

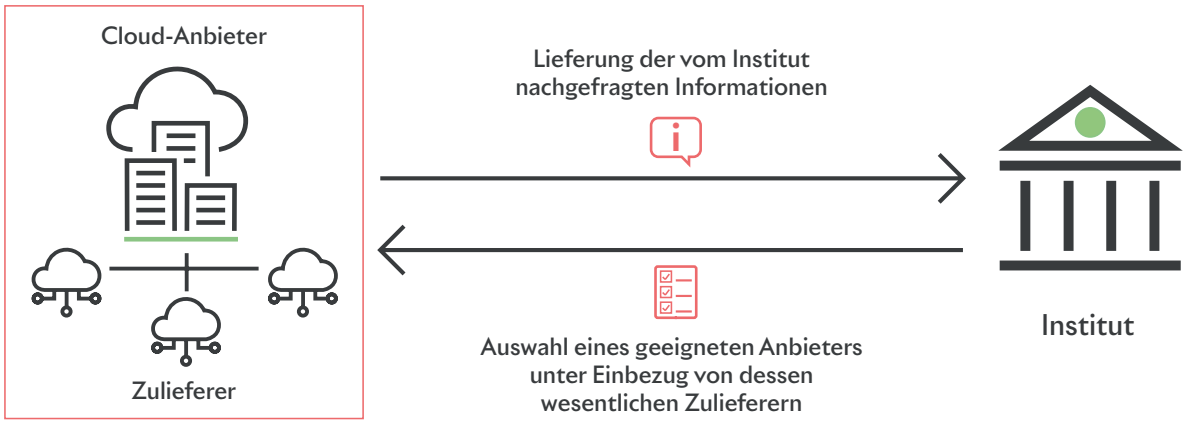
Bei der Auswahl der Cloud-Anbieter müssen daher insbesondere folgende Punkte berücksichtigt werden:

- Fähigkeit zur Erfüllung der vertraglichen Pflichten insbesondere mittels angemessener technischer und organisatorischer Massnahmen;
- wirtschaftliche Stabilität;
- Rechtsordnung, welcher der Cloud-Anbieter untersteht.

Weiter sollte geklärt werden, ob der Cloud-Anbieter bereit und in der Lage ist, neben den leistungsbezogenen Kriterien auch die massgeblichen Pflichten aus geltenden finanzmarktrechtlichen und datenschutzrechtlichen Vorgaben vertraglich zu übernehmen und mittels technischer und organisatorischer Massnahmen sicherzustellen.

Abbildung 1

Auswahl und Wechsel von Cloud-Anbietern und Zulieferern
Pflichten von Anbietern gegenüber dem Institut



Der Cloud-Anbieter sollte dem Institut die nachgefragten Informationen zur Verfügung stellen und muss insbesondere über einen allfälligen Wechsel eines wesentlichen Zulieferers informieren. Das Institut kann, sofern es damit nicht einverstanden ist, seinen Vertrag mit dem Cloud-Anbieter auflösen und die ausgelagerten Funktionen, Dienstleistungen und Bankkundendaten zurückführen oder auf neue Cloud-Anbieter übertragen.

Quelle: Schweizerische Bankiervereinigung (SBVg) 2025

Bei der Auswahl eines Cloud-Anbieters und seiner Zulieferer muss der Sicherheit (d.h. der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit) der Daten als integraler Bestandteil der zugrunde liegenden Sorgfaltsprüfung (Due Diligence) ein hoher Stellenwert beigemessen werden.

Ein Institut muss insbesondere über einen Wechsel eines wesentlichen Zulieferers vorgängig informiert werden (vgl. Abbildung 1).[7] Weiter muss das Institut geeignete Vorkehrungen treffen, um ausgelagerte Funktionen, Dienstleistungen sowie Bankkundendaten in den eigenen Betrieb zurückführen oder auf neue Cloud-Anbieter übertragen zu können. Dazu gehören insbesondere eine angemessene Kündigungsfrist, die Option auf Verlängerung des bisherigen Betriebsmodells und eine Wahlfreiheit in Bezug auf Datenexportschnittstellen und -formate.

B) Einhaltung des Bankkundengeheimnisses[8] in der Cloud[9]

Zweck der im Leitfaden aufgeführten Empfehlungen:
Die Einhaltung der rechtlichen sowie regulatorischen Vorgaben hinsichtlich des **Bankkundengeheimnisses** muss auch **in der Cloud jederzeit durch angemessene technische und organisatorische Massnahmen gewährleistet werden.**

Sofern im Rahmen der Cloud-Dienstleistungen Bankkundendaten oder Personendaten bearbeitet werden, sind das Bankkundengeheimnis und das Datenschutzgesetz zu berücksichtigen.[10]

Im Fokus des Leitfadens steht die Bearbeitung von bankkundengeheimnisrelevanten Daten. Diese werden vorliegend als Bankkundendaten bezeichnet. Der Leitfaden diskutiert diesbezüglich mögliche angemessene technische, vertragliche und organisatorische Massnahmen um das Risiko eines Zugriffs auf Bankkundendaten durch den Cloud-Anbieter und seine Zulieferer angemessen zu begrenzen (vgl. Abbildung 2).

---

7 Siehe dazu FINMA-RS 2018/3, Outsourcing, Auslagerungen bei Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten nach FINIG, Randziffer 33 sowie Art. 9 Abs. 3 DSG.

8 Exemplarisch wird in diesem Leitfaden auf das Bankkundengeheimnis eingegangen. Die entsprechenden Ausführungen zum Bankkundengeheimnis können analog auf weitere Berufsgeheimnisse wie z. B. das Berufsgeheimnis aus Art. 69 des Finanzinstitutsgesetzes (FINIG) angewendet werden. In Bezug auf Bankkundendaten sind das Geschäftsgeheimnis gemäss Art. 162 des Strafgesetzbuches (StGB) und – soweit Bankkundendaten auch als Personendaten qualifizieren – die berufliche Schweigepflicht gemäss Art. 62 DSG subsidiär anwendbar.

9 Siehe dazu nachfolgend Kapitel III:10 und Kapitel IV des Leitfadens.

10 Soweit es sich bei den Bankkundendaten um Personendaten handelt, gelten die Bestimmungen des anwendbaren Datenschutzrechts parallel.

Begriffe[11]

Bankkundendaten
Alle Angaben, die dem Bankkundengeheimnis nach Art. 47 BankG unterliegen. Jedes Institut legt im Rahmen der geschäftspolitischen und gesetzlichen Vorgaben selbst fest, welche konkreten Angaben unter den Begriff Bankkundendaten einzuordnen sind.

Personendaten gemäss Datenschutzgesetz (DSG)
Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[12]

Auslandsbezug und sogenannter «Foreign Lawful Access»[13]

Aufgrund des Betriebsmodells des Instituts und der eingesetzten Technologien kann es sein, dass die von einem Institut beigezogenen Cloud-Anbieter einen Auslandsbezug aufweisen. Ein solcher kann zum Beispiel vorliegen, wenn ein Cloud-Anbieter zu einem ausländischen Mutterkonzern gehört, sein Sitz im Ausland liegt oder wenn er Bankkundendaten im Ausland bearbeitet.

Im Rahmen des Bezuges von Cloud-Dienstleistungen muss das jeweilige Institut mit dem Cloud-Anbieter angemessene technische und organisatorische Massnahmen vereinbaren, um die Vertraulichkeit der Bankkundendaten bei den Cloud-Anbietern zu gewährleisten und beispielsweise vor Cyber-Kriminellen zu schützen.

Besteht ein Auslandsbezug, kann jedoch die Möglichkeit verbleiben, dass ausländische Behörden aufgrund des dadurch anwendbaren ausländischen Rechts eine Herausgabe von Bankkundendaten anordnen dürfen. In so einem Fall können die Bankkundendaten von den ausländischen Behörden nach Massgabe ihres anwendbaren ausländischen Rechts bearbeitet werden, zum Beispiel für eigene Untersuchungen oder Verfahren. Je nach anwendbarem ausländischen Recht kann es sein, dass im Vergleich zur Schweiz ein angemessener Schutz und vergleichbare Rechte (beispielsweise Zugriffs- bzw. Weitergabebeschränkungen oder Rechtsmittel) fehlen.

Aus Praktikabilitätsgründen dürfte im Zweifelsfall davon auszugehen sein, dass der Auslandsbezug zur Anwendung entsprechender ausländischer Gesetze und damit zu Zugriffen ausländischer Behörden führen kann, die aus Sicht der jeweiligen ausländischen Rechtsordnung zwar zulässig sind, jedoch aus Sicht der für Schweizer Institute massgeblichen schweizerischen Rechtsordnung als unzulässig angesehen werden könnten (sogenannter «Foreign Lawful Access»).

---

11 Die getroffene Begriffswahl ist nicht abschliessend.

12 Art. 5 lit. a DSG.

13 Siehe dazu nachfolgend Kapitel III:10 Randziffer 51 sowie Kapitel IV des Leitfadens.

Stellen angemessene technische und organisatorische Massnahmen mit an Sicherheit grenzender Wahrscheinlichkeit sicher, dass eine Herausgabe von Daten entweder gar nicht erfolgt oder nur in Bezug auf Daten, die keinen direkten oder indirekten Rückschluss durch – aus der Sicht des schweizerischen Rechts – unberechtigte Dritte auf die Identität der vom Bankkundengeheimnis geschützten Personen vorsehen, liegt keine bankkundengeheimnisrelevante Offenlegung vor.[14] Alternativ, das heisst wenn angemessene technische und organisatorische Massnahmen weder eine Herausgabe noch den Rückschluss mit an Sicherheit grenzender Wahrscheinlichkeit vermeiden können, stünde der Weg offen, Einwilligungen der betroffenen Personen und soweit erforderlich Bewilligungen der zuständigen Behörden einzuholen und so eine Offenlegung an ausländische Behörden zu rechtfertigen (siehe Abbildung 3).[15]

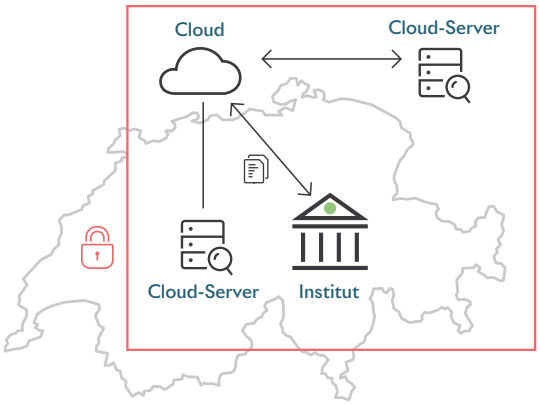
Abbildung 2

Bankkundengeheimnis in der Cloud

Bisheriger Schutz von Daten auf institutseigenen Servern

Schutz der Daten gemäss Bankkundengeheimnis gewährleistet. Jurisdiktion bildete in der Praxis Grenze in Bezug auf die Datenkontrolle.

Schutz von Daten in der Cloud



Schutz der Daten gemäss Bankkundengeheimnis durch technische, organisatorische und vertragliche Massnahmen gewährleistet.

Quelle: Schweizerische Bankiervereinigung (SBVg) 2025

14 Auch datenschutzrechtlich sind diese Daten gemäss der sog. relativen Methode nicht als Personendaten zu werten. Dies wurde gerichtlich bestätigt. Vgl. BGE 136 II 508 – Logistep sowie Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 19. Oktober 2016 in der Rechtssache C-582/14 – Patrick Breyer gegen Bundesrepublik Deutschland. Siehe zudem Erwägungsgrund 26 der EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), soweit diese anwendbar sein sollte: «Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.»

15 Siehe dazu nachfolgend Kapitel IV des Leitfadens.

Schutz von Bankkundendaten in der Cloud[16]

Mögliche technische Massnahmen[17]

Angemessene technische Massnahmen können bewirken, dass die in der Cloud bearbeiteten Daten nicht mehr als Bankkundendaten zu qualifizieren sind. Demensprechend sind anonymisierte Daten nicht als Bankkundendaten zu qualifizieren. Gleiches kann aus Sicht der Datenempfängerin oder des Datenempfängers für pseudonymisierte oder verschlüsselte Bankkundendaten gelten, beispielsweise wenn die Empfängerin oder der Empfänger nicht über eine Konkordanztabelle zu den Pseudonymen oder eine Möglichkeit zur Entschlüsselung der verschlüsselten Daten verfügt.[18]

- **Anonymisierung:** Bei der Anonymisierung werden personenbezogene Attribute (zum Beispiel Name und andere Identifikationsmerkmale einer Person) mit an Sicherheit grenzender Wahrscheinlichkeit irreversibel verändert, so dass niemand mehr auf die betroffene Person schliessen kann.
- **Pseudonymisierung:** Bei der Pseudonymisierung werden personenbezogene Attribute durch ein Kennzeichen, ein sogenanntes Pseudonym, ersetzt, sodass zwar das Institut, nicht aber die Empfängerin oder der Empfänger mit an Sicherheit grenzender Wahrscheinlichkeit einen Personenbezug herstellen kann.
- **Verschlüsselung:** Bei der Verschlüsselung handelt es sich um den Hauptanwendungsfall der Pseudonymisierung. Dabei wird ein Klartext[19] durch einen Schlüssel in einen Geheimtext umgewandelt. Die Ausgangsinformationen werden dadurch nur noch unter Verwendung des passenden Schlüssels wieder lesbar.

Mögliche organisatorische Massnahmen

- Angemessene Überwachung operativer Massnahmen der Cloud-Anbieter und deren Zulieferer durch das Institut;
- Prüfung der Sicherheits- und Vertraulichkeitsstandards des Cloud-Anbieters anhand von unabhängigen Berichten auf der Grundlage anerkannter Berichtsstandards.

16 Siehe beispielsweise auch Anhang C des Berichts der Bundeskanzlei von März 2025 zum rechtlichen Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung (2. Auflage), welcher einen groben Überblick über die Risiken und die jeweiligen Mitigierungsmassnahmen bietet.

17 Sie dazu nachfolgend Kapitel III:10.2 Randziffer 38 ff. des Leitfadens.

18 Siehe dazu Fussnote 14.

19 Der offene Wortlaut eines Textes beziehungsweise eine unverschlüsselte Nachricht.

Mögliche vertragliche Massnahmen[20]

- Angemessene vertragliche Festlegung der technischen und organisatorischen Massnahmen;
- Pflicht des Cloud-Anbieters, angemessene organisatorische und technische Massnahmen mit seinem Zulieferer zu vereinbaren;
- Vereinbarung der Wahrung der Vertraulichkeit durch den Cloud-Anbieter mittels konkreter Vorgaben für technische und organisatorische Massnahmen;
- Berücksichtigung der Sensitivität der Daten und die diesbezügliche Verantwortlichkeit des Cloud-Anbieters;
- Überwachung der Umsetzung und Einhaltung der technischen, organisatorischen und vertraglichen Massnahmen durch den Cloud-Anbieter und die Auditierung durch eine anerkannte Prüfgesellschaft;
- Vereinbarungen zum Vorgehen des Instituts oder des Cloud-Anbieters bei Anfragen von Behörden oder bei Verfahren, die eine Herausgabe oder Übermittlung von Bankkundendaten, die in der Cloud bearbeitet werden, zum Gegenstand haben;
- Vereinbarungen zum Vorgehen des Instituts oder des Cloud-Anbieters bei der Identifikation und Beurteilung von Vertraulichkeitsverletzungen durch Cyber-Kriminelle und dergleichen.

Zusammenspiel rechtlicher Vorgaben und TOM-Vorgaben mit entsprechenden Massnahmen[21]

Der Gesetzgeber und der Regulator sprechen im Zusammenhang mit Vorgaben für technische und organisatorische Massnahmen (TOM-Vorgaben) oft von einem sogenannten risikobasierten Ansatz.[22] In diesem Zusammenhang ist nicht die Missachtung rechtlicher oder regulatorischer Vorgaben im Sinne eines «kalkulierten Risikos» gemeint – im Gegenteil.

Die jeweils anwendbaren rechtlichen und regulatorischen Vorgaben sind im Einzelfall einzuhalten. Dies erfolgt jeweils mittels eigenständiger technischer und organisatorischer Massnahmen.

Bei der Definition angemessener technischer und organisatorischer Massnahmen gelangt der risikobasierte Ansatz zur Anwendung: Danach ist nach Massgabe der institutsspezifischen Geschäfts- und Betriebsmodelle sowie der jeweiligen Strategien die Eintretenswahrscheinlichkeit sowie das Schadensausmass einer Rechtsverletzung in gewissen Szenarien höher als in anderen.

---

20 Einige Institute behandeln vertragliche Massnahmen als Teil der organisatorischen Massnahmen. Unabhängig davon, handelt es sich bei technischen und organisatorischen Massnahmen generell nicht um rechtliche Fragen oder Vorgaben.

21 Siehe dazu Kapitel III:10.2 Randziffer 37 des Leitfadens.

22 Siehe dazu beispielsweise der erläuternde Bericht zur Verordnung über den Datenschutz (Datenschutzverordnung, DSV) vom 31. August 2022, S. 10, 17 f., 22, 28.

Der risikobasierte Ansatz äussert sich dergestalt, dass die definierten und entsprechend korrekt implementierten angemessenen technischen und organisatorischen Massnahmen nicht sämtliche theoretisch denkbaren Szenarien adressieren und verhindern müssen, sondern diejenigen Szenarien, deren Eintritt im konkreten Einzelfall nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens voraussehbar und bei pflichtgemässem Verhalten vermeidbar sind. Tritt nun ein Szenario ein, das in diesem Sinne nicht voraussehbar war, und konnte dieses Szenario trotz der korrekt umgesetzten, angemessenen technischen und organisatorischen Massnahmen nicht vermieden werden, sollte grundsätzlich kein (strafrechtlich) vorwerfbares Verhalten des Instituts bzw. der Entscheidungsträger vorliegen.[23]

Der vollständige Ausschluss sämtlicher Risiken ist weder praktisch möglich noch gesetzlich verlangt. Massgebend sollte sein, dass die im Einzelfall erforderliche Sorgfalt eingehalten wird, indem die voraussehbaren, institutsspezifischen Risiken adressiert und durch die zuständigen Rollen, Funktionen etc. mit angemessenen technischen und organisatorischen Massnahmen sichergestellt werden.

C) Transparenz und Zusammenarbeit der Institute und der Cloud-Anbieter im Bereich behördlicher und gerichtlicher Massnahmen[24]

Zweck der im Leitfaden aufgeführten Empfehlungen[25]:
Für Anfragen von ausländischen Behörden zur Herausgabe von Bankkundendaten ist ein **abgestimmtes Vorgehen zwischen Cloud-Anbieter und Institut** definiert.

Anfragen von Behörden oder Verfahren können die Herausgabe oder die Übermittlung von Bankkundendaten, welche in der Cloud bearbeitet werden, zum Gegenstand haben. Auch ausländische Gesetze können eine Herausgabe von Daten durch Cloud-Anbieter vorsehen.

Der Leitfaden sieht vor, dass ein abgestimmtes Vorgehen zwischen Cloud-Anbieter und Institut zur Behandlung von Anfragen von Behörden definiert ist, welche eine Herausgabe oder Übermittlung von Bankkundendaten zum Gegenstand haben.

---

23 Vgl. BGE 135 IV 56, E.2.1. Es existieren verschiedene Methoden zur Beurteilung der Eintretenswahrscheinlichkeit sowie des Schadensausmasses einer Rechtsverletzung.

24 Siehe dazu nachfolgend Kapitel IV des Leitfadens.

25 Die gleichen Empfehlungen könnten insbesondere auch im Rahmen anderer Berufsgeheimnisse oder im Falle von Geschäftsgeheimnissen anwendbar sein. Dabei bleiben datenschutzrechtliche Fragen vorbehalten und werden vorliegend nicht behandelt.

Stützt sich eine in der Sache zuständige Schweizer Behörde (bzw. zuständiges Schweizer Gericht) beim Ersuchen auf Herausgabe bzw. Übermittlung der Bankkundendaten auf eine ausreichende und klare Rechtsgrundlage der schweizerischen Rechtsordnung (inkl. auf von der Schweiz ratifizierte Staatsverträge), ist von einem sog. «Lawful Access» die Rede. Diesfalls sollte geprüft werden, ob die Herausgabe bzw. Übermittlung im Einzelfall von der jeweiligen Rechtsgrundlage auch tatsächlich abgedeckt ist.

Stützt sich hingegen eine ausländische Behörde auf eine eigene ausländische Rechtsgrundlage, liegt ein sogenannter «Foreign Lawful Access» vor. Eine Herausgabe von Bankkundendaten kann aus der Sicht der schweizerischen Rechtsordnung unzulässig sein (z. B. wenn die betroffenen Informationen durch das Bankkundengeheimnis geschützt sind) – auch dann, wenn die ausländische Rechtsgrundlage die Herausgabe beziehungsweise Übermittlung der Bankkundendaten rechtmässig vorsieht. Diesfalls gilt es, wie oben beschrieben, die Herausgabe der Bankkundendaten mittels angemessener, vorgängig implementierter technischer und organisatorischer Massnahmen entweder mit an Sicherheit grenzender Wahrscheinlichkeit zu vermeiden oder aber nur Informationen herauszugeben, die keinen direkten oder indirekten Rückschluss durch – aus der Sicht des schweizerischen Rechts – unberechtigte Dritte auf die Identität der vom Bankkundengeheimnis geschützten Person vorsehen. Falls dies nicht möglich sein sollte, wäre zu prüfen, ob die fragliche Herausgabe bzw. Übermittlung mit einer Einwilligung[26] des Instituts, einer Einwilligung[27] der betroffenen Personen, dem Entscheid eines zuständigen Schweizer Gerichts und/oder der Bewilligung der zuständigen Schweizer Behörde an ausländische Behörden gerechtfertigt werden kann (vgl. Abbildung 3).[28]

Auf jeden Fall sollte der Cloud-Anbieter das Institut rechtzeitig informieren, soweit dies rechtlich zulässig ist, falls ausländische Behörden eine Anfrage anbringen, welche die Übermittlung oder Bekanntgabe von Bankkundendaten zum Gegenstand haben. Ist es dem Cloud-Anbieter gemäss den Rechtsvorschriften, auf welche sich die ausländische Behörde beruft, untersagt das Institut zu benachrichtigen, so soll der Cloud-Anbieter selbständig die Rechtmässigkeit des Offenlegungsersuchens überprüfen und das Ersuchen anfechten, wenn dieses nach den Rechtsvorschriften, auf welche sich die ausländische Behörde beruft, rechtswidrig ist.[29] Bei der Anfechtung eines Ersuchens erwirkt der Cloud-Anbieter einstweilige Massnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten Bankkundendaten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist.[30]

Ausserdem sollten dem Institut die Rechte zur Verfahrensführung eingeräumt werden. Weiter sollte der Cloud-Anbieter das Institut bei der Behandlung von Anfragen ausländischer Behörden unterstützen.

---

26 Die Form bzw. Dokumentation der Einwilligung kann auf unterschiedliche Weise erfolgen und ist eine Frage des Risikomanagements und -appetits im Hinblick auf ein mögliches Beweisverfahren.

27 Siehe Fussnote 26.

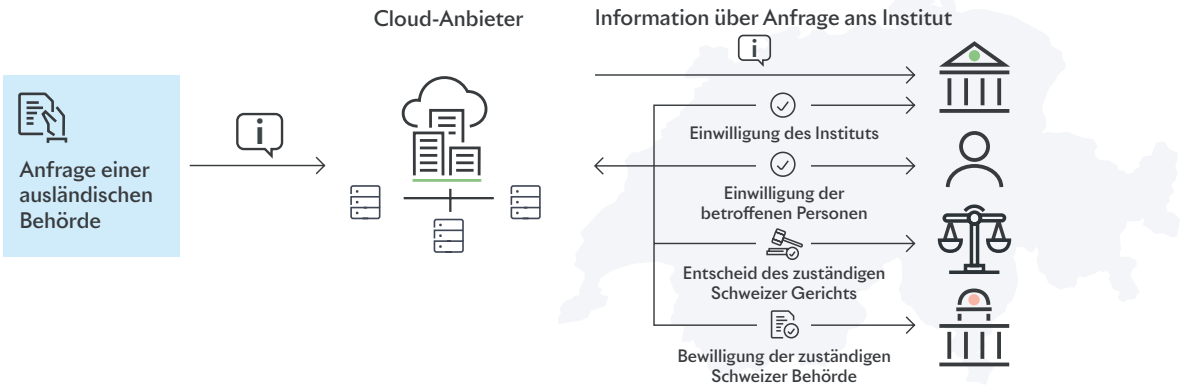
28 Im Zusammenhang mit Anfragen ausländischer Behörden sind unabhängig von der Qualifikation der relevanten Informationen als Bankkundendaten und/oder Personendaten weitere Vorschriften wie Art. 42c des Finanzmarktaufsichtsgesetzes (FINMAG) und Art. 271 StGB relevant, vgl. Ausführungen nachfolgend unter Kapitel IV des Leitfadens.

29 Analog der Klauseln 15.1. Benachrichtigung und 15.2. Überprüfung der Rechtmässigkeit und Datenminimierung des Anhangs des Durchführungsbeschlusses 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates.

30 Siehe Fussnote 29.

Abbildung 3

Anfrage von ausländischen Behörden
Herausgabe von Bankkundendaten unter bestimmten Voraussetzungen



Bei Anfragen ausländischer Behörden zur Herausgabe von Bankkundendaten, welche in der Cloud bearbeitet werden, hat der Cloud-Anbieter das Vorgehen mit dem Institut abzustimmen. Sofern die Herausgabe von Bankkundendaten nicht mittels technischer/organisatorischer Massnahmen mit an Sicherheit grenzender Wahrscheinlichkeit vermieden werden kann, dürfen Bankkundendaten nur im Einklang mit geltenden gesetzlichen Bestimmungen und je nach Einzelfall mit der Einwilligung des Instituts, der Einwilligung der betroffenen Personen, aufgrund eines Entscheids des zuständigen Schweizer Gerichts und/oder aufgrund einer Bewilligung der zuständigen Schweizer Behörde übermittelt werden.

Quelle: Schweizerische Bankiervereinigung (SBVg) 2025

D) Prüfung (Audit) der Cloud-Dienstleistungen und der eingesetzten Mittel[31]

Zweck der im Leitfaden aufgeführten Empfehlungen:
Der **Zugriff** durch Dritte auf **Daten in der Cloud zum Zwecke der Prüfung (Auditierung)** ist jederzeit gewährleistet.

Cloud-Dienstleistungen werden von den Cloud-Anbietern regelmässig aus hochsicheren Rechenzentren gegenüber einer grossen Anzahl von Kundinnen und Kunden erbracht. Die Prüfung (Auditierung) der von den Cloud-Anbietern eingesetzten Infrastrukturen erfordert ein hohes Mass an Spezialisierung.

Die Einhaltung der auf den Cloud-Anbieter anwendbaren gesetzlichen, regulatorischen und vertraglichen Anforderungen sollte regelmässig geprüft werden. Dazu gehören insbesondere Anforderungen bezüglich

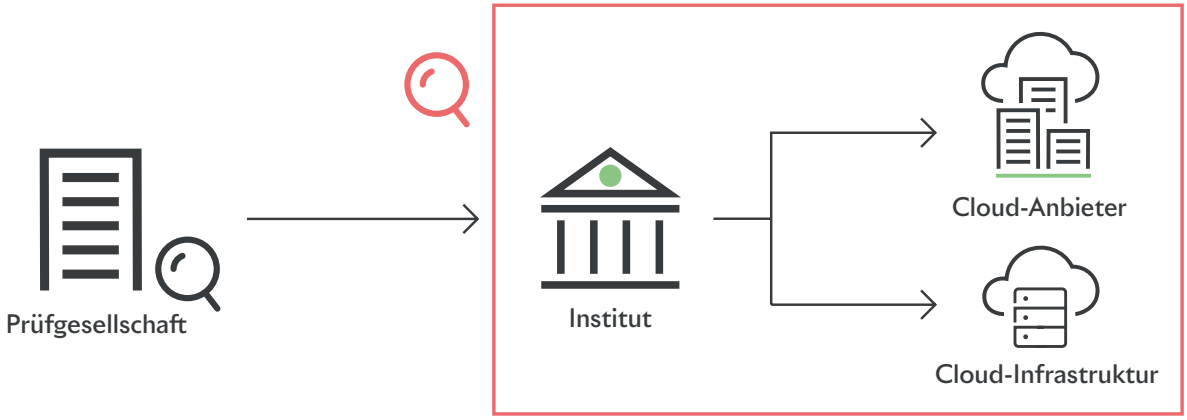
31 Siehe dazu nachfolgend Kapitel V des Leitfadens.

Outsourcing, Datenschutz und Informationssicherheit. Die Prüfungen sollten vom Institut, dessen externer Prüfgesellschaft oder von der FINMA durchgeführt und veranlasst werden können. Sogenannte Poolaudits durch mehrere Institute oder deren Prüfgesellschaften und indirekte oder begleitete Audits sind zulässig.

Eine Prüfung der konkret zur Erbringung der Cloud-Dienstleistungen eingesetzten IT-Infrastrukturen vor Ort, mit Ausnahme der Prüfung der Massnahmen zur physischen Sicherheit, ist nicht zwingend erforderlich. Ein logischer Zugriff[32] ist ausreichend. Die Prüfung der wesentlichen Unterakkordanten durch das Institut kann indirekt durch die Prüfung des Cloud-Anbieters erfolgen (vgl. Abbildung 4).

Abbildung 4

Prüfung (Auditierung) in der Cloud
Prüfung der Cloud-Infrastruktur erfordert hohe Spezialisierung



Es sollte sichergestellt werden, dass die Prüfgesellschaft bei der Prüfung des Institut mindestens einen logischen Zugriff auf die Cloud-Infrastruktur erhält.

Quelle: Schweizerische Bankiervereinigung (SBVg) 2025

32 Technische Zugriffskontrolle beziehungsweise Interaktion mit der Hardware über Fernzugriff im Gegensatz zum physikalischen Zugriff, der die Interaktionen mit der Hardware in der physischen Umgebung umfasst.

Rechtlicher und regulatorischer Cloud-Leitfaden

für den

Einsatz von Cloud-Dienstleistungen durch Banken und Wertpapierhäuser im Bereich des FINMA regulierten Outsourcings

Inhaltsverzeichnis

Kapitel I: Allgemeine Bestimmungen

1 Gegenstand und Zweck, Geltungsbereich und Unverbindlichkeit

(1)* Gegenstand dieses Leitfadens sind Empfehlungen, welche bei Beschaffung und Einsatz von Cloud-Dienstleistungen durch die Institute und die Anbieter herangezogen werden können. Es handelt sich um eine Auslegungshilfe für die rechtlichen und regulatorischen Vorgaben für die Praxis, insbesondere zu den folgenden vier Schwerpunktthemen:

- **Steuerung:** Auswahl des Anbieters und seiner Unterakkordanten sowie Zustimmung bei einem Wechsel der Unterakkordanten (Kapitel II)
- **Datenbearbeitung:** Bearbeitung von Bankkundendaten[1] (Kapitel III)
- **Behörden und Verfahren:** Transparenz und Zusammenarbeit der Institute und der Anbieter im Bereich behördlicher und gerichtlicher Massnahmen (Kapitel IV)
- **Audit:** Prüfung der Cloud-Dienstleistungen und der zur Erbringung der Dienstleistungen eingesetzten Cloud-Infrastruktur (Kapitel V)

Die zwischenzeitlichen Erfahrungen der unterschiedlichen Institute haben dazu geführt, dass die anfänglichen Rechtsfragen weiter geklärt sind; somit hat sich die Diskussion betreffend Cloud weg von rechtlichen Fragenstellungen hin zu nicht-rechtlichen Fragen rund um Vorgaben für angemessene technische und organisatorische Massnahmen gewandelt. Diese konkretisieren und operationalisieren die relevanten geschäftspolitischen, rechtlichen sowie regulatorischen Vorgaben, welche institutsspezifisch sind und die jeweils unterschiedlichen Geschäfts- und Betriebsmodelle abbilden. Zu diesem Zweck können die Institute bei der Anwendung des Leitfadens ihre Grösse und die Komplexität ihres Geschäftsmodells risikobasiert und verhältnismässig berücksichtigen.

(2) Der vorliegende Leitfaden wurde im Hinblick auf Cloud-Dienstleistungen ausgearbeitet, die von Anbietern im Auftrag von Instituten erbracht werden und die als Outsourcing wesentlicher Funktionen unter das FINMA-RS 18/3 fallen.

(3)* Der vorliegende Leitfaden ist unverbindlicher Natur und stellt keine Selbstregulierung dar.

---

1 Im Fokus des Leitfadens steht die Bearbeitung sämtlicher bankkundengeheimnisrelevanten Daten. Diese werden vorliegend als Bankkundendaten bezeichnet.

2 Begriffe

(4)* Für die Zwecke dieses Leitfadens bezeichnet der Begriff:

a. **«Anbieter»** den Anbieter der Cloud-Dienstleistungen ausserhalb des Instituts bzw. der Unternehmensgruppe des Instituts.
b. **«BankG»** das Bundesgesetz über die Banken und Sparkassen (Bankengesetz), SR 952.0.
c. **«BankV»** die Verordnung über die Banken und Sparkassen (Bankenverordnung), SR 952.02.
d. **«Bankkundendaten»** alle Angaben, die dem Bankkundengeheimnis nach Art. 47 BankG unterliegen. Jedes Institut legt im Rahmen der geschäftspolitischen und gesetzlichen Vorgaben selbst fest, welche konkreten Angaben unter den Begriff Bankkundendaten einzuordnen sind.
e. **«Bankkundengeheimnis»**[2] das gemäss Art. 47 BankG geschützte Geheimnis.
f. **«bearbeiten»** wie er gemäss Datenschutzgesetz definiert wird. Der Begriff «bearbeiten» umfasst auch den Begriff «verarbeiten»[3].
g. **«Cloud»** oder **«Cloud Computing»** wie es vom National Institute of Standard and Technology (NIST)[4] oder von der European Union Agency for Network and Information Security (ENISA)[5] definiert wird; Cloud oder Cloud Computing umfasst die Service-Modelle Infrastructure-as-a–Service (IaaS), Platform-as-a Service (PaaS), und Software-as-a-Service (SaaS), und kann in den Liefermodellen Public Cloud, Private Cloud oder Hybrid Cloud bereitgestellt werden.[6]
h. **«Cloud-Dienstleistungen»** die Service-Modelle des Anbieters im Bereich Cloud Computing im Auftrag des Instituts.
i. **«DSG»** das Bundesgesetz über den Datenschutz (Datenschutzgesetz), SR 235.1.
j. **«FINIG»** das Bundesgesetz über die Finanzinstitute (Finanzinstitutsgesetz), SR 954.1.
k. **«FINIV»** die Verordnung über die Finanzinstitute (Finanzinstitutsverordnung), SR 954.11.
l. **«FINMAG»** das Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz), SR 956.1.
m. **«FINMA-RS 18/3»** das Rundschreiben der Eidgenössischen Finanzmarktaufsicht 2018/3, Outsourcing, Auslagerungen bei Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten nach FINIG, Datum des Erlasses: 21. September 2017, in der jeweils geltenden Fassung.

---

2 Exemplarisch wird in diesem Leitfaden auf das Bankkundengeheimnis eingegangen. Die entsprechenden Ausführungen können jedoch analog zum Beispiel auf das Berufsgeheimnis aus Art. 69 FINIG angewendet werden. In Bezug auf Bankkundendaten sind das Geschäftsgeheimnis gemäss Art. 162 StGB und – soweit Bankkundendaten auch als Personendaten qualifizieren – die berufliche Schweigepflicht gemäss Art. 62 DSG subsidiär anwendbar.

3 Gemäss Definition in der EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), soweit diese anwendbar sein sollte.

4 The NIST Definition of Cloud Computing (2011)

5 European Network and Information Security Agency (ENISA), Cloud Computing Security Risk Assessment (2009)

6 Cloud oder Cloud Computing umfasst bspw. auch Function-as-a-Service (FaaS).

n. **«FINMA-RS 23/1»** das Rundschreiben der Eidgenössischen Finanzmarktaufsicht 2023/1, Operationelle Risiken und Resilienz – Banken, Management der operationellen Risiken und Sicherstellung der operationellen Resilienz, Datum des Erlasses: 7. Dezember 2022, in der jeweils geltenden Fassung.
o. **«Institut»** Banken und Wertpapierhäuser gemäss Randziffer 5 des FINMA-RS 18/3.
p. **«ISG»** das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz), SR 128.
q. **«kritische Daten»** Daten gemäss Randziffer 7 des FINMA RS 23/01.
r. **«Kundinnen und Kunden»** die Kundinnen und Kunden eines Instituts.
s. **«Leitfaden»** die in dem vorliegenden Dokument festgehaltenen Grundsätze und Empfehlungen.
t. **«Meldepflicht»** die Meldepflichten gemäss Art. 24 DSG, Art. 74a ff. ISG, FINMA-Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG[7] und FINMA-RS 23/1 Randziffer 81.
u. **«Personendaten»** wie er gemäss Datenschutzgesetz definiert wird. Der Begriff «Personendaten» umfasst auch den Begriff «personenbezogene Daten».[8]
v. **«StGB»** das schweizerische Strafgesetzbuch, SR 311.0
w. **«wesentliche Unterakkordanten»** Unterakkordanten, welche im Rahmen der Erbringung der Cloud-Dienstleistungen durch den Anbieter (i) wesentliche Funktionen im Sinne des FINMA-RS 18/3 erbringen, oder (ii) nach Einschätzung des Instituts als wesentliche Unterakkordanten zu bezeichnen sind.

7 Die FINMA präzisiert in ihrer Aufsichtsmitteilung 03/2024 vom 7. Juni 2024 die Anforderungen an die Meldepflicht von Cyber-Attacken.

8 Gemäss Definition in der Datenschutz-Grundverordnung, soweit diese anwendbar sein sollte.

Kapitel II: Steuerung (Governance mit Risk Management)

Rechtliche Grundlagen

- Art. 3 und 47 BankG, Art. 12 BankV
- Art. 2, 5, 6, 9, 41 ff. und 69 FINIG, Art. 66 und 68 FINIV
- DSG
- FINMA-RS 23/1
- FINMA-RS 18/3

3 Entscheid zur Beschaffung von Cloud-Dienstleistungen

(5) Cloud-Computing zeichnet sich durch eine grosse Vielfalt an verfügbaren Dienstleistungen aus. Neben hochstandardisierten Cloud-Infrastrukturen und -Dienstleistungen werden spezifische Lösungen angeboten. Der Entscheid zur Beschaffung von Cloud-Dienstleistungen sollte daher mittels eines strukturierten Verfahrens erfolgen.

(6)* Erfolgt der Entscheid zur Beschaffung von Cloud-Dienstleistungen auf der Grundlage einer vorgängig durchzuführenden Risikoanalyse[9], sollten neben den mit dem Beziehen der Cloud-Dienstleistungen verbundenen Chancen und Risiken der Wesentlichkeit der Cloud-Dienstleistungen im Sinne von FINMA-RS 18/3 sowie der Qualifikation der im Rahmen der Cloud-Dienstleistungen bearbeiteten Daten, insbesondere Bankkundendaten, Rechnung getragen werden.

(7) Hinsichtlich der Bewertung der Risiken berücksichtigt das Institut auch die Risiken, welche mit einer mangelhaften Erbringung der Cloud-Dienstleistungen oder mit dem vollständigen oder teilweisen Ausfall der Cloud-Dienstleistungen oder des Anbieters verbunden sein können.

(8)* Sind mit der Beschaffung, dem Beziehen oder der Beendigung des Bezugs der Cloud-Dienstleistungen Risiken verbunden, sollten angemessene mitigierende Massnahmen festgelegt werden, welche im Rahmen des Risikomanagements während der Laufzeit des Einsatzes der Cloud-Dienstleistungen umgesetzt, fortgebildet und überwacht werden. Folglich sollte nach der Phase der Beschaffung («change the bank») eine hinreichende Struktur in der Aufbau- sowie Ablauf-

9 Beispielsweise wären Risiken zu bewerten, welche im Zusammenhang mit der Datensicherheit oder den operationellen Risiken stehen.

organisation geschaffen werden, um den ordentlichen Betrieb («run the bank») der Cloud-Dienstleistung mittels angemessener technischer und organisatorischer Massnahmen, Dokumentationen[10], Kontrollen sowie Governance zu gewährleisten.

4 Verantwortlichkeiten und Rollen

(9)* Aufgrund der Regulierung des Instituts sind gegebenenfalls finanzmarktrechtliche Vorschriften und, sofern im Rahmen der Cloud-Dienstleistungen Bankkundendaten oder Personendaten bearbeitet werden, das Bankkundengeheimnis und das Datenschutzgesetz[11] zu berücksichtigen.

(10) Bei Zuweisung der Verantwortlichkeiten und Bestimmung der Rollen sind die Service-Modelle und Liefermodelle zu berücksichtigen. Der Anbieter sollte dabei in geeigneter Weise und im erforderlichen Umfang mitwirken und dem Institut die sachdienlichen Informationen zur Verfügung stellen. Idealerweise erfolgt diese Mitwirkung bereits während des Angebotsverfahrens.

(11) Zieht der Anbieter bei Erbringung der Cloud-Dienstleistungen Unterakkordanten bei, sollte dieser Umstand bei Festlegung der Rollen und Verantwortlichkeiten hinsichtlich der wesentlichen Unterakkordanten in geeigneter Weise berücksichtigt werden.

(12) Der Vertrag zwischen dem Institut und dem Anbieter sollte die entsprechenden Rechte und Pflichten der Parteien und weiteren Beteiligten, auch hinsichtlich deren Umsetzung, regeln.

5 Auswahl und Wechsel des Anbieters und wesentlicher Unterakkordanten

(13) Anbieter, insbesondere solche von hochstandardisierten Cloud-Dienstleistungen, bedingen sich zum Zwecke einer effizienten und kompetitiven Leistungserbringung regelmässig die Freiheit aus, die Betriebsmodelle, die zum Einsatz kommenden Technologien, konzerninterne und externe Leistungserbringer und weitere massgebliche Faktoren festzulegen und zu ändern (Design-Autorität).

(14)* Es ist im Interesse des Instituts, dass die Fähigkeit zur Erfüllung der jeweiligen Bedürfnisse hinsichtlich technischer und organisatorischer Massnahmen und vertraglichen Pflichten, die wirtschaftliche Stabilität, die Rechtsordnungen, denen der Anbieter und seine Unterakkordanten unterstehen, und weitere massgebliche Punkte bei der Auswahl des geeigneten Anbieters berücksichtigt werden.[12] Wesentliche Unterakkordanten sollten in die Bewertung einbezogen werden. Der Anbieter sollte bei Erhebung der vom Institut diesbezüglich nachgefragten Informationen in geeigneter Art und Weise mitwirken.

---

10 Insbesondere im Fall von Dienstleistungsverträgen, in denen über Links auf Anhänge verwiesen wird, sollte das Institut die zum Zeitpunkt des Vertragsschlusses gültigen Anhänge herunterladen und ablegen.

11 Das Datenschutzgesetz inkl. zugehörige Verordnung sowie die Datenschutz-Grundverordnung, soweit diese anwendbar sein sollte.

12 Sofern Personendaten bearbeitet werden, sind die im DSG normierten Prüfpflichten, z.B. im Rahmen einer Datenschutz-Folgenabschätzung oder einer Auftragsbearbeitung, zu berücksichtigen und deren Inhalt und Umfang institutsspezifisch und unter Berücksichtigung des jeweiligen Geschäfts- und Betriebsmodells auszugestalten.

(15) Die Bewertung etwaiger Risiken sollte insbesondere auch eine Festlegung der mitigierenden Massnahmen und die Verantwortlichkeiten zu deren Umsetzung beinhalten.

(16)* Ausserdem sollte bei der Auswahl eines Anbieters zusätzlich zu den leistungsbezogenen Kriterien dessen Bereitschaft zur Übernahme der massgeblichen Pflichten aus finanzmarktrechtlichen[13] und datenschutzrechtlichen Vorgaben und die Ausgestaltung des Betriebsmodells berücksichtigt werden. Bei der Auswahl eines Anbieters und dessen Unterakkordanten, welche Bankkundendaten des Instituts oder Personendaten bearbeiten, muss die Sicherheit (d.h. die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit) der Daten ein ausschlaggebendes Kriterium sowie integraler Bestandteil der zugrunde liegenden Sorgfaltsprüfung (Due Diligence[14]) sein.

(17)* Ein Wechsel des Anbieters (bspw. Konzerngesellschaft in anderer Rechtsordnung) sollte unter Vorbehalt der vorgängigen Zustimmung des Instituts stehen, wobei diese schriftlich oder auf anderweitig nachweisbare Art erteilt werden kann. Rein konzerninterne Umstrukturierungen innerhalb derselben Rechtsordnung, die auf die bisherigen Verhältnisse, Kriterien und Risiken keine massgeblichen Auswirkungen zeitigen, können von einer solchen Zustimmung ausgenommen werden. Der Anbieter sollte sich auf Verlangen des Instituts bereit erklären, entsprechende Regelungen vorzusehen, welche den Wechsel des den Anbieter oder einen wesentlichen Unterakkordanten beherrschenden Unternehmens regeln.

(18)* Der Einbezug neuer wesentlicher Unterakkordanten oder deren Wechsel muss den im FINMA RS 03/18 festgelegten Grundsätzen folgen.[15] Die vertragliche Vereinbarung von Kriterien für den Einbezug wesentlicher Unterakkordanten, deren Einhaltung der Anbieter sicherzustellen und deren Erfüllung der Anbieter dem Institut vorgängig nachzuweisen hat, kann dem Institut zusätzliche Sicherheit bieten. Erforderlich ist jedenfalls, dass das Institut vor Einbezug eines neuen wesentlichen Unterakkordanten durch den Anbieter informiert wird und dem Institut innerhalb einer Frist die Beendigung der Leistungserbringung durch den Anbieter, gegebenenfalls aus wichtigem oder berechtigtem Grund, offensteht. Das Institut sollte in diesen Fällen die geeigneten Vorkehrungen treffen, insbesondere sich eine angemessene Kündigungsfrist und eine geeignete Beendigungsunterstützung des Anbieters ausbedingen, gegebenenfalls auch Verlängerungsoptionen unter Aufrechterhaltung des bisherigen Betriebsmodells sowie eine Wahlfreiheit in Bezug auf Datenexportschnittstellen und -formate, sodass die ausgelagerten Funktionen und Dienstleistungen sowie die Bankkundendaten zurückgeführt oder auf einen neuen Anbieter übertragen werden können. Dabei sollten auch sogenannte Lock-In Effekte und Menge, Anzahl sowie Kritikalität der ausgelagerten Funktionen und Bankkundendaten berücksichtigt werden.

---

13 Einschliesslich angemessener Vertraulichkeitsbestimmungen.

14 Es sind klare Kriterien für die Beurteilung des Umgangs des Anbieters mit kritischen Daten zu definieren und vor Vertragsvereinbarung zu prüfen (siehe FINMA-RS 23/1, Randziffer 82).

15 FINMA RS 03/18 Randziffer 33.

6 Datenzentren und Betriebszentren

(19)* Zuweilen bestehen Bedenken, wonach mit der Nutzung von Cloud-Dienstleistungen eine Lokalisierung der Orte, wo Daten bearbeitet werden, nicht mehr möglich sei (Ubiquität der Daten). Aus Sicht der Institute ist das Vertrauen ihrer Kundinnen und Kunden über den Umgang mit deren Daten von zentralem Interesse.

(20) Die Standorte, an denen sich die durch das Institut genutzten oder nutzbaren Cloud-Infrastrukturen befinden (Datenzentren) und von denen aus die Cloud gegebenenfalls betrieben wird (Betriebszentren) sowie Verlegungen derselben während der Laufzeit, sollten vom Anbieter bekannt gegeben werden. Die diesbezüglichen Angaben sollten die Informationen umfassen, welche (juristische) Personen, namentlich der Anbieter und die wesentlichen Unterakkordanten, die Daten- und Betriebszentren betreiben, im Eigentum haben oder auf andere Weise kontrollieren.

(21)* Eine Verlegung von Standorten während der Vertragslaufzeit in eine andere Rechtsordnung sollte einem vertraglich definierten Änderungsverfahren unterstehen und abhängig vom individuellen Schutzbedürfnis, der vorgängigen Zustimmung des Instituts unterliegen, zumindest soweit Personendaten bearbeitet werden oder die Unterakkordanten als wesentlich zu qualifizieren sind.[16] Dabei soll der Anbieter die mit der Verlegung einhergehenden Risiken aufzeigen und dem Institut alle zur Entscheidungsfindung sachdienlichen Informationen, insbesondere auch über die jeweils angewendeten Sicherheitsmassnahmen, unterbreiten.

(22)* Weitere sich aus einem Datenzugriff durch Dritte ergebende Anforderungen werden in den folgenden Kapiteln beschrieben.

16 Hinsichtlich Zustimmung, Verlängerungsoption und ggf. Beendigung des Vertrages gelten die in Randziffer 18 genannten Prinzipien.

Kapitel III: Daten und Datensicherheit

Rechtliche Grundlagen

- Art. 47 BankG
- Art. 69 FINIG
- FINMA RS 23/1
- FINMA-RS 18/3
- DSG

7 Klassifizierung der Daten und Informationen

(23)* Um eine einwandfreie Umsetzung der datenschutzrechtlichen Vorgaben und eine Wahrung des Bankkundengeheimnisses zu gewährleisten, sind auch die Vorgaben des FINMA-RS 23/1 hinsichtlich kritischer Daten zu beachten. Demnach sollte eine Identifizierung und Klassifizierung der mittels der Cloud-Dienstleistungen bearbeiteten Bankkundendaten durch das Institut vorgenommen werden.

(24)* Dies soll es dem Institut, und soweit erheblich auch dem Anbieter, ermöglichen, die anwendbaren rechtlichen und regulatorischen Vorschriften bezüglich der Datenbearbeitung und Datenflüsse, der Zugriffskonzepte sowie die Angemessenheit weiterer technischer und organisatorischer Massnahmen inkl. Kontrollen zu beurteilen und zu definieren.

(25)* Dabei sollte in Betracht gezogen werden, ob und wieweit Kundinnen und Kunden über eine Auslagerung der Bearbeitung von Bankkundendaten an einen Anbieter von Cloud-Dienstleistungen in der Schweiz oder im Ausland informiert wurden oder, sofern und soweit notwendig, einer solchen Auslagerung zugestimmt haben.[17]

(26)* Massgebliche Änderungen der Klassifizierung der ausgelagerten Bankkundendaten während der Vertragslaufzeit sollten erfasst und notwendige Massnahmen vor solchen Auslagerungen umgesetzt werden.

17 Dazu Kapitel III:10 unten.

8 Speicherorte und Datenflüsse, Zugriffskonzept

(27)* Der Anbieter sollte es dem Institut ermöglichen, die Orte der Bearbeitung (insbesondere Speicherorte) von Bankkundendaten zu prüfen[18] und diese Orte der Bearbeitung mittels technischer und organisatorischer Massnahmen zu kontrollieren. Auch sollte das Institut in der Lage sein, seine Pflichten gegenüber den Kundinnen und Kunden bezüglich Transparenz nachzukommen und entsprechend die Orte der Bearbeitung, insbesondere die Speicherorte der Bankkundendaten, in dem für diese Zwecke erforderlichen Detaillierungsgrad, zu kennen.

(28)* Bankkundendaten betreffende Datenflüsse, welche in der Sphäre des Anbieters und gegebenenfalls seiner Unterakkordanten zu verzeichnen sind, sollten dem Institut im Voraus offengelegt und die den Datenflüssen zugrunde liegende Architektur sollte, soweit erforderlich, hinreichend genau mittels technischer und organisatorischer Massnahmen festgelegt und vertraglich abgebildet werden.

(29)* Zu Letzterem gehört auch die Definition und Umsetzung eines Zugriffskonzepts[19] durch den Anbieter. Erteilte Zugriffsberechtigungen sollten vom Anbieter auf Nachfrage offengelegt werden und Zugriffe auf Bankkundendaten sollten vom Anbieter in angemessener Art und Weise überwacht und aufgezeichnet werden.

(30)* Ein solches Zugriffskonzept sollte auch den Zweck des Zugriffes hinreichend eng festlegen und sich dazu äussern, in welchen genau definierten Fällen ein Zugriff auf Systeme, mit denen Bankkundendaten bearbeitet werden, erfolgen kann beziehungsweise freigegeben wird. Zu solchen Fällen können etwa Notfälle oder andere kritische, nicht anders zu behebende Ausfälle der Cloud-Infrastruktur gezählt werden.

9 Allgemeine technische und organisatorische Massnahmen der Datensicherheit

(31)* Im Allgemeinen sollten vom Anbieter angemessene technische und organisatorische Massnahmen zum Schutz der bearbeiteten Bankkundendaten des Instituts angeboten und im Vertrag abgebildet werden. Dabei sollten internationale und lokale technische Standards[20] berücksichtigt werden. Ferner sollte der Anbieter angemessene technische und organisatorische Massnahmen mit seinen Unterakkordanten vereinbaren.

(32)* Der Anbieter sollte sicherstellen, dass seine Mitarbeitenden und diejenigen der Unterakkordanten, welche Zugriff auf Bankkundendaten haben, sich nachweislich zur Geheimhaltung und vertraulichen Behandlung verpflichten und entsprechend informiert, geschult und mit geeigneten Massnahmen

18 Die Anforderungen für eine solche Prüfung ergeben sich aus Kapitel V unten.

19 Hinsichtlich Zugriffe auf Bankkundendaten.

20 Z.B. Standards der International Organization for Standardization (ISO) und des National Institute of Standards and Technology (NIST) (Regeln der Berufskunde).

überwacht werden.[21] Eine solche Verpflichtung der Mitarbeitenden wird als hinreichend erachtet, wenn sie gegenüber dem Anbieter oder seiner Unterakkordanten im Rahmen des Arbeitsverhältnisses abgegeben wird. Es wird den Anbietern empfohlen, die datenschutzrechtlichen Vorgaben einzuhalten und die in der Schweiz tätigen Mitarbeitenden ausdrücklich auf das Bankkundengeheimnis sowie weitere anwendbare gesetzliche Vertraulichkeitsverpflichtungen und die Strafandrohung bei deren Verletzung hinzuweisen.

10 Bankkundengeheimnis und Sicherheitsmassnahmen

10.1 Einleitende Bemerkungen

(33)* Vor der Inanspruchnahme von Cloud-Dienstleistungen muss das Institut klären, ob eine diesbezügliche Entbindung vom Bankkundengeheimnis gemäss Art. 47 BankG[22] durch die Kundin oder den Kunden notwendig ist. Dies wäre insbesondere dann der Fall, wenn das jeweilige Institut zum Ergebnis gelangen würde, dass eine Offenbarung von Bankkundendaten gegenüber Unbefugten nicht mit an Sicherheit grenzender Wahrscheinlichkeit mittels angemessener technischer oder organisatorischer Massnahmen vermieden werden kann. Diesfalls würde das Institut die Gefahr laufen, das Bankkundengeheimnis vorsätzlich oder fahrlässig zu verletzen.

(34)* Vorliegend wird vertreten, dass eine Entbindung vom Bankkundengeheimnis durch die Kundin oder den Kunden nicht notwendig ist, wenn das Institut angemessene technische, organisatorische und vertragliche Massnahmen hinsichtlich der Sicherheit der im Rahmen der Cloud-Dienstleistungen bearbeiteten Bankkundendaten vorgesehen hat, um eine Offenbarung der Bankkundendaten gegenüber Unbefugten mit an Sicherheit grenzender Wahrscheinlichkeit auszuschliessen.

Dieses Kapitel enthält einen Überblick über die dieser Auffassung zugrundeliegende Argumentation sowie die zu ergreifenden Sicherheitsmassnahmen.

10.2 Mögliche technische, organisatorische und vertragliche Massnahmen[23]

(35)* Eine Verletzung des Bankkundengeheimnisses besteht in einer durch das Institut vorsätzlich oder fahrlässig verursachten tatsächlichen Offenbarung von Bankkundendaten an Unbefugte.[24] Art. 47 Abs. 1 BankG ist ein Erfolgsdelikt, allein die Möglichkeit einer Kenntnisnahme von Bankkundendaten durch Unbefugte stellt keine Verletzung des Bankkundengeheimnisses dar.

---

21 Vgl. FINMA-RS 23/1, Randziffer 80.

22 Vgl. Fussnote 2.

23 Einige Institute behandeln vertragliche Massnahmen als Teil der organisatorischen Massnahmen. Unabhängig davon, handelt es sich bei technischen und organisatorischen Massnahmen generell nicht um rechtliche Fragen oder Vorgaben.

24 Siehe Urteil des Bundesgerichts 6B_1403/2017 vom 8. August 2017.

(36)* Wenn der Anbieter und seine Unterakkordanten im Rahmen der Cloud-Dienstleistungen nicht tatsächlich Kenntnis von den in der Cloud bearbeiteten Bankkundendaten nehmen, liegt keine Offenbarung im Sinne des Art. 47 Abs. 1 BankG vor. Das Institut muss das Risiko des Zugriffs auf Bankkundendaten durch den Anbieter und seine Unterakkordanten durch technische, organisatorische und vertragliche Massnahmen allerdings angemessen begrenzt haben.

(37)* Die jeweils zu implementierenden Massnahmen ergeben sich aus den anwendbaren rechtlichen und regulatorischen Bestimmungen.[25] Die Beurteilung der Angemessenheit dieser Massnahmen ist jedoch keine Rechtsfrage und sollte unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Bearbeitung der Bankkundendaten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte der betroffenen Kunden erfolgen.

Hierbei kann berücksichtigt werden, dass nach Massgabe der institutsspezifischen Geschäfts- und Betriebsmodelle sowie der jeweiligen Strategien die Eintretenswahrscheinlichkeit und das Schadensausmass einer Rechtsverletzung in gewissen Szenarien höher ist als in anderen. Angemessene technische und organisatorische Massnahmen müssen daher nicht sämtliche theoretisch denkbaren Szenarien adressieren und verhindern, sondern lediglich diejenigen, deren Eintritt im konkreten Einzelfall nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens voraussehbar und bei pflichtgemässem Verhalten mit an Sicherheit grenzender Wahrscheinlichkeit vermeidbar sind.[26] Dabei muss die im Einzelfall erforderliche Sorgfalt eingehalten werden.

Im Folgenden werden einige Massnahmen beispielhaft aufgeführt.[27]

(38)* **Angemessene technische Massnahmen zum Schutz von Bankkundendaten:**

Angemessene technische Massnahmen können bewirken, dass das Institut die in der Cloud bearbeiteten Daten nicht mehr als Bankkundendaten klassifizieren muss. Dementsprechend sind anonymisierte Daten nicht als Bankkundendaten zu qualifizieren. Gleiches kann aus Sicht der Datenempfängerin oder des Datenempfängers für pseudonymisierte bzw. verschlüsselte Bankkundendaten gelten, beispielsweise wenn die Empfängerin oder der Empfänger nicht über eine Konkordanztabelle zu den Pseudonymen bzw. eine Möglichkeit zur Entschlüsselung der verschlüsselten Daten verfügt.[28]

Als geeignete technischen Verfahren zum angemessenen Schutz von Bankkundendaten werden insbesondere die nachfolgend aufgeführten Sicherheitsmassnahmen betrachtet.

---

25 Vgl. auch FINMA-RS 23/1, Randziffer 79.

26 Vgl. BGE 135 IV 56, E. 2.1. Dieses Vorgehen wird auch als risikobasierter Ansatz bezeichnet. Es existieren verschiedene Methoden zur Beurteilung der Eintretenswahrscheinlichkeit sowie des Schadensausmasses einer Rechtsverletzung.

27 Siehe beispielsweise auch Anhang C des Berichts der Bundeskanzlei von März 2025 zum rechtlichen Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung (2. Auflage), welcher einen groben Überblick über die Risiken und die jeweiligen Mitigierungsmassnahmen bietet.

28 Auch datenschutzrechtlich sind diese Daten gemäss der sog. relativen Methode nicht als Personendaten zu werten. Dies wurde gerichtlich bestätigt. Vgl. BGE 136 II 508 – Logistep sowie Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 19. Oktober 2016 in der Rechtssache C-582/14 – Patrick Breyer gegen Bundesrepublik Deutschland. Siehe zudem Erwägungsgrund 26 der Datenschutz-Grundverordnung, soweit diese anwendbar sein sollte: «Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren».

(39)* Anonymisierung: Mit an Sicherheit grenzender Wahrscheinlichkeit anonymisierte Daten (irreversible Methodik) sind nicht mehr als Bankkundendaten und/oder Personendaten zu qualifizieren. Die in diesem Abschnitt aufgeführten Anforderungen gelten daher nicht für anonymisierte Daten.

(40)* Pseudonymisierung: Sofern es sich um Bankkundendaten handelt, sollte die jeweilige Zuordnungsregel unter Kontrolle des Instituts angemessen geschützt werden. Insbesondere sollten die Rechte zur Verwendung der Referenztabelle nach Massgabe des Need-to-know-Prinzips eingeschränkt und die Zugriffe nachvollziehbar protokolliert werden.

(41)* Verschlüsselung: Bei der Verschlüsselung von Bankkundendaten sollte darauf geachtet werden, dass der Verschlüsselungsschlüssel vor unberechtigten Zugriffen geschützt wird und der Zugriff unter der Kontrolle des Instituts steht, selbst wenn der Verschlüsselungsschlüssel auch dem Anbieter zur Verfügung steht oder bei diesem aufbewahrt und zur automatisierten Ver- und Entschlüsselung der Bankkundendaten im Rahmen der Cloud-Dienstleistung verwendet wird. Das Institut sollte auf der Grundlage einer Beurteilung der Risiken insbesondere im Hinblick der Klassifizierung der Bankkundendaten abwägen, welche Verfahren zur Ausprägung der Kontrolle des Verschlüsselungsschlüssels angemessen sind.

Das Verschlüsselungsverfahren wie auch die Stärke des Verschlüsselungsschlüssels müssen den gegenwärtigen Sicherheitsstandards Rechnung tragen, sodass die Verschlüsselung als kryptographisch sicher betrachtet werden kann. Das bestimmt sich jeweils nach dem Stand der Technik (Regeln der Berufskunde).

Eine Übermittlung von Bankkundendaten sollte grundsätzlich verschlüsselt erfolgen. Das Verschlüsselungsverfahren wie auch die Stärke des Verschlüsselungsschlüssels müssen den gegenwärtigen Sicherheitsstandards Rechnung tragen, sodass die Übermittlung als kryptographisch sicher betrachtet werden kann.

(42)* **Organisatorische Massnahmen zum Schutz von Bankkundendaten:**

Die durch den Anbieter und seine Unterakkordanten durchgeführten operativen Massnahmen sollten durch das Institut angemessen überwacht werden können.

Die erforderliche Prüfung der Sicherheits- und Vertraulichkeitsstandards des Anbieters sollte anhand von unabhängigen Berichten auf der Grundlage anerkannter Berichtsstandards[29] erfolgen.

(43)* **Vertragliche Massnahmen zum Schutz von Bankkundendaten:**

Vertragliche Massnahmen bilden in der Regel die vereinbarten technischen und organisatorischen Massnahmen ab. Zu den vertraglichen Massnahmen gehören insbesondere:

- Die angemessene vertragliche Festlegung der technischen und organisatorischen Massnahmen im Vertrag zwischen dem Anbieter und dem Institut sowie die Pflicht des Anbieters zur Vereinbarung angemessener organisatorischer und technischer Massnahmen mit den Unterakkordanten des Anbieters;

29 Beispielsweise Prüfungsstandards der Berichterstattungsoptionen nach ISAE 3000 oder SOC2.

- die Vereinbarung der Wahrung der Vertraulichkeit durch den Anbieter mittels konkreter Vorgaben für technische und organisatorische Massnahmen;
- die Berücksichtigung der Sensitivität der Daten und die diesbezügliche Verantwortlichkeit des Anbieters;
- die Überwachung der Umsetzung und Einhaltung der technischen, organisatorischen und vertraglichen Massnahmen und die Auditierung durch eine anerkannte Prüfgesellschaft;
- die Vereinbarungen gemäss Kapitel IV (Behörden und Verfahren) sowie zum Vorgehen bei der Identifikation und der Beurteilung von Vertraulichkeitsverletzungen durch Cyber-Kriminelle und dergleichen.[30]

10.3 Kreis der Geheimnisträger

(44)* Je nach Service-Modell der Cloud-Dienstleistungen kann es notwendig sein, dass Mitarbeitende des Anbieters und seiner Unterakkordanten die in der Cloud bearbeiteten Bankkundendaten im Klartext, d.h. weder verschlüsselt bzw. pseudonymisiert, bearbeiten und damit tatsächlich zur Kenntnis nehmen. In dem Fall stellt sich die Frage, ob der Anbieter und seine Unterakkordanten als Unbefugte im Sinne des Art. 47 Abs. 1 BankG zu qualifizieren sind. Klarstellend wird festgehalten, dass eine vollautomatisierte Ver- und Entschlüsselung im Rahmen der Cloud-Dienstleistung nicht als Klartext-Datenbearbeitung im Sinne dieses Abschnitts anzusehen ist.

(45) Der Anbieter und seine Unterakkordanten sind keine Unbefugten im Sinne des Art. 47 Abs. 1 BankG. Die Inanspruchnahme von Cloud-Dienstleistungen eines Anbieters entspricht grundsätzlich dem ernsthaften Interesse des Instituts an der Optimierung der Servicequalität, der Kosten und der Datensicherheit. Bereits die Botschaft über die Revision des BankG nimmt ausdrücklich auf die Beauftragtenstellung von IT-Dienstleistern Bezug.[31] Ausserdem hat das Institut regelmässig Weisungsbefugnis[32] gegenüber dem Anbieter und seinen Unterakkordanten. Sie sind deshalb als Beauftragte im Sinne des Art. 47 Abs. 1 BankG zu qualifizieren und dürfen in den Kreis der Geheimnisträger einbezogen werden.

(46)* Auch im Ausland ansässige Anbieter und Unterakkordanten sind Beauftragte und damit zulässige Geheimnisträger. Dies entspricht dem Sinn und Zweck des Art. 47 Abs. 1 BankG und ist dem Wortlaut nach nicht ausgeschlossen.[33]

(47) Die Risikoerhöhung durch eine Klartext-Datenbearbeitung im Ausland ist allerdings im Rahmen

---

30 Diesfalls sind, je nach betroffenen Daten (Schutzobjekt), unterschiedliche Rechtsgrundlagen anwendbar und damit verschiedene Abklärungen erforderlich, Fristen und Meldeschwellen einzuhalten und Behörden zuständig. Vgl. z.B. Art. 24 DSG, FINMA-Aufsichtsmitteilung 05/2020 Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG, FINMA-RS 23/1 Randziffer 81 sowie Art. 74a ff. ISG. Zu beachten ist im Vertrag mit dem Anbieter, dass sich diese Meldepflichten nicht ausschliesslich auf Bankkundendaten beziehen.

31 Botschaft über die Revision des BankG vom 13. Mai 1970, BBL 1970, 1182: «Mit der Unterstellung von Beauftragten sollen insbesondere auch Rechenzentren erfasst werden, die von Banken mit der elektronischen Datenverarbeitung betraut werden».

32 FINMA RS 03/18, Randziffer 21.

33 Die Notwendigkeit eines ausdrücklichen Ausschlusses folgt aus dem Legalitätsprinzip des Art. 1 StGB.

der anwendbaren Sicherheitsmassnahmen zu berücksichtigen. Ausschlaggebend für die Beurteilung der Angemessenheit können unter anderem auch die länderspezifischen Risiken sein, insbesondere, aber nicht ausschliesslich, die Frage, ob die jeweilige Gesetzgebung einen angemessenen Schutz gegen Datenschutzverletzungen gewährleistet.

(48)* Die jeweiligen technischen, organisatorischen und vertraglichen Massnahmen ergeben sich ebenfalls aus den anwendbaren rechtlichen und regulatorischen Bestimmungen.[34]

(49) Die im Folgenden aufgeführten zusätzlichen technischen und organisatorischen Massnahmen können in Bezug auf ein erhöhtes Auslandsrisiko als angemessen betrachtet werden.

- Die Klartext-Bearbeitung durch Mitarbeitende des Anbieters oder seiner Unterakkordanten im Ausland sollte nur soweit dies für den sicheren und zuverlässigen Betrieb der Cloud notwendig ist und unter zeitlicher und sachlicher Hinsicht eng definierten Bedingungen erfolgen;
- Die Bearbeitungsvorgänge müssen vom Anbieter überwacht und aufgezeichnet werden und das Institut sollte die Möglichkeit haben, die Kontrolle über den Zeitpunkt, die Dauer und den Umfang der Bearbeitung zu erhalten. Der Anbieter muss in der Lage sein, die Bearbeitung bei Verdacht auf unautorisierte Bearbeitungsvorgänge unverzüglich zu beenden;
- das Institut muss vom Anbieter über die Bearbeitung informiert werden oder die Möglichkeit haben sich selbst zu informieren;
- das Institut muss besonderen Wert auf die Vereinbarungen gemäss Kapitel IV (Behörden und Verfahren) legen.

(50)* Wie vorstehend dargelegt, stellt eine Klartext-Bearbeitung von Bankkundendaten durch Mitarbeitende des Anbieters und seiner Unterakkordanten grundsätzlich keine Offenlegung an Unbefugte und damit keine Verletzung des Bankkundengeheimnisses durch das Institut dar.

(51)* Eine Offenbarung von Bankkundendaten an Unbefugte könnte dann angenommen werden, wenn ausserhalb der Sphäre des Anbieters befindliche Dritte, wie z.B. ausländische Behörden, aufgrund der Inanspruchnahme der Cloud-Dienstleistungen Kenntnis von Bankkundendaten erlangen. Der Auslandsbezug könnte zur Anwendung entsprechender ausländischer Gesetze und damit zu Zugriffen ausländischer Behörden führen, die aus Sicht der ausländischen Rechtsordnung zwar zulässig sind, jedoch aus Sicht der für Schweizer Institute massgeblichen schweizerischen Rechtsordnung als unzulässig angesehen werden könnten (sog. «Foreign Lawful Access»). Wird die Herausgabe von Bankkundendaten mittels angemessener, vorgängig implementierter technischer und organisatorischer Massnahmen entweder mit an Sicherheit grenzender Wahrscheinlichkeit vermieden oder aber werden nur Informationen herausgegeben, die keinen direkten oder indirekten Rückschluss durch – aus der Sicht des schweizerischen Rechts – unberechtigte Dritte auf die Identität der vom Bankkundengeheimnis geschützten Person vorsehen, liegt keine vorsätzliche oder fahrlässige Handlung und somit keine strafbare Verletzung des Bankkundengeheimnisses vor.[35]

---

34 Vgl. auch FINMA-RS 23/1, Randziffer 79.

35 Damit scheidet im Fall der blossen Möglichkeit eines Zugriffs auf Bankkundendaten auch die Annahme eines strafbaren Versuchs der Offenbarung an Unbefugte aus.

10.4 Informationspflichten des Instituts

(52)* Soweit im Rahmen der Cloud-Dienstleistungen Personendaten bearbeitet werden, besteht eine datenschutzrechtliche Informationspflicht gegenüber den betroffenen Personen, die mittels der generellen Datenschutzerklärung des Instituts erfüllt werden kann. Die Information ist im Sinne des Transparenzgrundsatzes einfach und verständlich zu gestalten. Klarstellend wird festgehalten, dass das Datenschutzrecht grundsätzlich nicht die Bekanntgabe der einzelnen Anbieter und ihrer Unterakkordanten verlangt.

(53) Weitere Informationspflichten, die sich aus Gründen ausserhalb des Datenschutzrechts ergeben können, sind im Einzelfall zu beurteilen. Zu berücksichtigen sind zum Beispiel der Erwartungshorizont der Kundin oder des Kunden, vertragliche Vereinbarungen, auftragsrechtliche Bestimmungen und der Grundsatz von Treu und Glauben. Als Anhaltspunkte können z.B. der Marktauftritt und die Kommunikation des Instituts im Hinblick auf vorgängige Beauftragungen von Dienstleistern dienen.

11 Massnahmen zur Sicherstellung der Verfügbarkeit und Rückführung

(54)* Auf Bankkundendaten, welche im Ausland oder in der Schweiz gespeichert und bearbeitet werden, sollte das Institut jederzeit aus der Schweiz zugreifen können. Der Anbieter sollte sich dazu verpflichten, die Cloud-Dienstleistungen auch in Fällen der Sanierung oder Abwicklung des Instituts gegenüber dem Institut, einer Nachfolge- oder Auffanggesellschaft und gegebenenfalls der FINMA insoweit zu erbringen, als dass damit ein solcher Zugriff aus der Schweiz auf Informationen im Ausland oder in der Schweiz gewährleistet wird.[36]

(55)* Der Anbieter sollte sich dazu verpflichten, die Bankkundendaten im Rahmen der Beendigungsunterstützung, in Fällen der Sanierung oder Abwicklung des Instituts und auf Weisung des Instituts oder der FINMA jederzeit dem Institut, einer Nachfolge- oder Auffanggesellschaft, oder einem Nachfolge-Anbieter zurückzuführen, sofern dem Anbieter die dazu notwendigen Mittel[37] und Kenntnisse[38] vorliegen. Der Anbieter sollte diesfalls die Bankkundendaten in einem standardisierten, maschinell lesbaren Format nach Wahl des Instituts zurück übertragen.

---

36 Für wesentliche Outsourcings siehe FINMA-RS 18/3, Randziffer 31.

37 Etwa Verschlüsselungsschlüssel.

38 Insbesondere bei Cloud -Dienstleistungen im Rahmen von IaaS oder PaaS hat der Anbieter gegebenenfalls keine Kenntnisse über die vom Institut gewählte Architektur und/oder die vom Institut eingesetzten Komponenten.

(56) Setzt der Anbieter proprietäre Lösungen ein, welche zu Lock-In-Effekten führen, sollte sich der Anbieter bereit erklären, das Institut bei der Migration auf andere Lösungen oder bei der Lizenzierung solcher Lösungen zu unterstützen.[39]

Kapitel IV: Behörden und Verfahren

Rechtliche Grundlagen

- Art. 271 StGB
- Art. 273 StGB
- Art. 47 BankG
- Art. 16 f. DSG
- Staatsverträge für internationale Rechtshilfe
- FINMA-RS 23/1
- Art. 42c FINMAG

(57)* Der Anbieter hat sich mit dem Institut abzustimmen, nach welchem Verfahren vorzugehen ist, wenn Anfragen von Behörden eine Herausgabe oder Übermittlung von in der Cloud bearbeiteten Bankkundendaten zum Gegenstand haben.[40] Sofern und soweit kein zwingendes gesetzliches Recht entgegensteht, hat sich der Anbieter gegenüber dem Institut zu den nachfolgend in Randziffer 58-60 genannten technischen und organisatorischen Massnahmen vertraglich zu verpflichten:

(58)* Der Anbieter, sowie die Unterakkordanten und Konzerngesellschaften des Anbieters dürfen nur im Einklang mit anwendbaren gesetzlichen und regulatorischen Bestimmungen und je nach Einzelfall mit (i) einer vorgängigen Einwilligung des Instituts[41], (ii) einer vorgängigen Einwilligung

39 Je nach Anwendungsbereich können insbesondere ausländische Rechtsgrundlagen wie beispielsweise die EU-Verordnung 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der EU-Verordnung 2017/2394 und der EU-Richtlinie 2020/1828 (EU-Datenverordnung) zu diesen Aspekten zusätzliche rechtliche Vorgaben vorsehen.

40 Die gleichen Grundsätze könnten insbesondere auch im Rahmen anderer Berufsgeheimnisse oder im Falle von Geschäftsgeheimnissen anwendbar sein. Dabei bleiben datenschutzrechtliche Fragen vorbehalten und werden vorliegend nicht behandelt.

41 Die Form bzw. Dokumentation der Einwilligung kann auf unterschiedliche Weise erfolgen und ist eine Frage des Risikomanagements und -appetits im Hinblick auf ein mögliches Beweisverfahren.

der betroffenen Personen[42], (iii) aufgrund eines Entscheids des zuständigen Schweizer Gerichts, und/oder (iv) aufgrund einer Bewilligung der zuständigen Schweizer Behörde, Bankkundendaten, welche in der Cloud bearbeitet werden, in ausländischen Verfahren an ausländische Behörden oder sonstige Parteien im Ausland übermitteln oder bekanntgeben.

(59)* Der Anbieter soll das Institut rechtzeitig vor Herausgabe der Bankkundendaten informieren und dem Institut die Rechte zur Verfahrensführung einräumen und das Institut bei der Behandlung von Anfragen ausländischer Behörden unterstützen.

(60)* Falls dem Anbieter eine vorgängige Anzeige an das Institut der Übermittlung oder Bekanntgabe von Bankkundendaten an ausländische Behörden oder sonstige Parteien im Ausland aufgrund von zwingendem Recht nicht möglich ist, sollte der Anbieter im Rahmen der getroffenen Vereinbarung und im Interesse des Instituts und dessen Kundinnen und Kunden die angemessenen Rechts- oder Schutzmassnahmen ergreifen.[43] Zudem soll der Anbieter selbständig die Rechtmässigkeit des Offenlegungsersuchens überprüfen und das Ersuchen anfechten, wenn dieses nach den Rechtsvorschriften, auf welche sich die ausländische Behörde beruft, rechtswidrig ist. Bei der Anfechtung eines Ersuchens sollte der Anbieter einstweilige Massnahmen ergreifen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten Bankkundendaten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist.[44]

(61)* Überdies soll der Anbieter das Institut in genereller Art und Weise über Anzahl (pro Jahr), Gegenstand und Vorgehen von Verfahren informieren, welche nach anwendbaren ausländischen Gesetzen oder Regulationen eine Übermittlung oder Bekanntgabe von Bankkundendaten zum Gegenstand haben oder haben könnten und auf den Anbieter sowie auf die Unterakkordanten[45] oder Konzerngesellschaften des Anbieters[46] anwendbar sind.

(62) Das Institut soll, gegebenenfalls unter geeigneter Mitwirkung des Anbieters, die Risiken bewerten, welche sich ergeben, wenn ausländische Behörden die Wirksamkeit der eingesetzten technischen, organisatorischen und vertraglichen Massnahmen gemäss Randziffer 10 übersteuern können.[47]

---

42 Siehe Fussnote 41.

43 Siehe Kapitel II und III, insbesondere die Ausführungen zum Bankkundengeheimnis und der datenschutzrechtlichen Transparenz.

44 Analog der Klauseln 15.1. Benachrichtigung und 15.2. Überprüfung der Rechtmässigkeit und Datenminimierung des Anhangs des Durchführungsbeschlusses 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates.

45 Unterakkordanten, welche Zugriff auf Bankkundendaten haben.

46 Siehe Fussnote 37.

47 Siehe Randziffer 37.

Kapitel V: Prüfung (Audit) der Cloud-Dienstleistungen und der eingesetzten Mittel

Rechtliche Grundlagen

- Art. 18 und 23 ff. BankG sowie Ausführungsbestimmungen BankV
- Art. 61 und 63 FINIG
- FINMA-RS 23/1 Randziffer 71-82 sowie dazugehörige Prüfpunkte zum Management der Risiken kritischer Daten
- FINMA-RS 18/3

(63) Cloud-Dienstleistungen werden von den Anbietern regelmässig aus hochsicheren Rechenzentren gegenüber einer grossen Anzahl von Kundinnen und Kunden[48] erbracht. Die Prüfung (Auditierung) der von den Anbietern eingesetzten Infrastrukturen erfordert eine hohe Spezialisierung; dabei sollten die Vertraulichkeitsverpflichtungen des Anbieters gegenüber seinen anderen Kundinnen und Kunden beachtet werden.

(64) Die Einhaltung der auf den Anbieter mittels Vertrag überbundenen Anforderungen (inkl. technische und organisatorische Massnahmen), die sich aus den rechtlichen und regulatorischen Anforderungen ergeben (insbesondere bezüglich Outsourcing, Datenschutz und Informationssicherheit), sollte regelmässig geprüft werden, wobei zu berücksichtigen ist, dass sich die Wirksamkeit von Massnahmen erst aus einer Kombination der Kontrollen beim Anbieter und beim Institut ergibt. Der Anbieter soll in angemessenem Umfang mitwirken. Teil der Prüfung kann auch die Erfüllung der vertraglich vereinbarten Leistungen sein.

(65) Die Prüfungen sollten vom Institut, dessen externer Prüfgesellschaft oder von der FINMA durchgeführt und veranlasst werden können.[49] Sogenannte Poolaudits durch mehrere Institute oder deren Prüfgesellschaften, und indirekte oder begleitete Audits, bei denen die Prüfung und Berichtserstattung durch die Prüfgesellschaft des Anbieters oder durch eine vom Anbieter bezeichnete Prüfgesellschaft durchgeführt wird, sind zulässig, sofern die Prüfgesellschaft über die notwendige Unabhängigkeit und fachliche Kompetenz verfügt. Dies gilt auch hinsichtlich Prüfungen, welche von der FINMA veranlasst werden.

48 Public Cloud.

49 Für wesentliche Outsourcings siehe FINMA-RS 18/3, Randziffer 26.

(66) Eine Prüfung der konkret zur Erbringung der Cloud-Dienstleistungen eingesetzten IT-Infrastrukturen vor Ort, mit Ausnahme der Prüfung der Massnahmen zur physischen Sicherheit, ist nicht zwingend erforderlich. Die Gewährung eines logischen Zugriffs zugunsten des Instituts, seiner Prüfgesellschaft oder der zuständigen Behörde kann dafür als ausreichend betrachtet werden. Der Anbieter kann die Modalitäten eines solchen Zugriffsrechts direkt mit der Aufsichtsbehörde regeln.

(67) Es wird festgehalten, dass im Fall von Cloud-Dienstleistungen mit Auslandsbezug die vertragliche Vereinbarung des Rechts zu direkter oder indirekter Prüfung des Anbieters durch das Institut, seine Prüfgesellschaft, die Prüfgesellschaft des Anbieters und die FINMA dem Erfordernis einer angemessenen Abklärung der Prüfrechte genügt.

(68) Die vorstehenden Grundsätze sollten auch in Bezug zu wesentlichen Unterakkordanten festgelegt werden. Mangels Vertrags zwischen Institut und Unterakkordanten sollte dies mittels Überbindung der vertraglichen Pflichten des Anbieters auf seine Unterakkordanten geschehen.

(69)* Die Prüfung der wesentlichen Unterakkordanten kann indirekt durch die Prüfung des Anbieters erfolgen, wobei eine direkte Prüfung der wesentlichen Unterakkordanten erforderlich werden kann und deshalb vertraglich mit dem Anbieter zu vereinbaren ist.

Der rechtliche und regulatorische Leitfaden wurde mit Wirkung ab November 2025 wie folgt geändert:

Geänderte Randziffern	1, 3, 4, 6, 8, 9, 14, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 48, 50, 51, 52, 54, 55, 57, 58, 59, 60, 61 und 69
Angepasste Rechtsgrundlagen (Box) in	Kapitel II, III, IV, V
Angepasste Begrifflichkeiten in	Randziffern 1, 4, 6, 9, 16, 18, 23, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 50, 51, 54, 55, 57, 58, 59, 60 und 61 sowie in Fussnoten 19, 35 und 45
Geänderte Fussnoten	9, 13, 15, 19, 35, 45 und 46
Neu eingefügte Fussnoten	1, 2, 3, 6, 7, 8, 10, 11, 12, 14, 16, 18, 20, 21, 22, 23, 25, 26, 27, 28,30, 34, 36, 39, 40, 41, 42, 44, 47 und 49
Anderes	Aufhebung des Titels von Kapitel III:10.5 (vor Randziffer 53); Anpassung des Titels von Kapitel II, Kapitel III:10.2 und III:10.4

Schweizerische
Bankiervereinigung
Aeschenplatz 7
CH-4002 Basel
office@sba.ch
www.swissbanking.ch