SwissBanking

Juni 2020, 2. Auflage

Cloud-Leitfaden

Wegweiser für sicheres Cloud Banking

Inhaltsverzeichnis

Vorwort

Cloud-Dienstleistungen eröffnen Banken und Effektenhändlern neue Möglichkeiten für innovative Geschäftsmodelle und effizientere Prozesse. Die Wettbewerbsfähigkeit des Bankensektors wird mit der gezielten Migration der Bankeninfrastruktur von On-Premise-Systemen (in den eigenen Räumlichkeiten, vor Ort oder lokal) in eine Cloud-Umgebung nachhaltig verbessert. Die Nutzung von Cloud-Dienstleistungen ist aktuell jedoch mit rechtlichen und regulatorischen Unsicherheiten verknüpft. Diese verzögern die Migration der Bankeninfrastruktur in die Cloud.

Unter der Leitung der Schweizerischen Bankiervereinigung (SBVg) hat eine Arbeitsgruppe einen rechtlichen und regulatorischen Leitfaden (nachfolgend Leitfaden) für den Einsatz von Cloud-Dienstleistungen durch Banken und Effektenhändler erarbeitet. Gegenstand dieses Leitfadens sind Empfehlungen, welche bei Beschaffung und Einsatz von Cloud-Dienstleistungen durch die Institute und die Cloud-Anbieter herangezogen werden können.

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 beleuchtet die aus Sicht der SBVg wichtigsten regulatorischen Fragen und die Lösungsansätze der SBVg im Leitfaden. Der zweite Teil erläutert im Detail die rechtlichen und regulatorischen Empfehlungen der SBVg.

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

Management Summary

- Die **Benutzung der Cloud** ist ein **kritischer Erfolgsfaktor** für die Schweiz und den Finanzplatz. Für eine konforme Nutzung der Cloud durch die Banken waren aber noch rechtliche und regulatorische Unsicherheiten zu klären.
- Die SBVg hat eine **Arbeitsgruppe** einberufen mit dem Ziel, diese Unsicherheiten rasch zu klären. Die Arbeitsgruppe hat sich auf die Erarbeitung eines juristisch **unverbindlichen Leitfadens** als Auslegungshilfe für die Praxis fokussiert. In vier Bereichen werden die Unsicherheiten als hoch beziehungsweise als hinderlich für eine Migration in die Cloud eingestuft:
  - **Steuerung (Governance)**: Auswahl des Cloud-Anbieters und seiner Unterakkordanten (Zulieferer) sowie Zustimmung bei einem Wechsel der Unterakkordanten
  - **Datenbearbeitung**: Bearbeitung von Daten über Bankkunden und Bankkundengeheimnis
  - **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
- Die Klärung der regulatorischen Fragen im Leitfaden **ermöglicht den Banken schnelles und flexibles Handeln** und bietet pragmatische und sichere Lösungen. Dieses Vorgehen ist einer spezifischen Cloud-Regulierung vorzuziehen. Denn diese wäre langsam, nicht technologieneutral und durch die technischen Entwicklungen schnell überholt.
- Die Einschätzung der **Risiken** einer Migration in die Cloud verbleibt auch mit dem Leitfaden **bei den einzelnen Bankinstituten**. Jede Bank entscheidet selbst, wie breit sie Cloud-Lösungen nutzen möchte.

Grundlagen Cloud Banking

Nutzen und Vorteile von Cloud Banking

Digitale Innovationen und Agilität in Bezug auf neue Entwicklungen sind eine Voraussetzung für die Wettbewerbsfähigkeit des Schweizer Finanzplatzes. Dazu gehört auch der Einsatz von Cloud-Dienstleistungen. Cloud-Dienstleistungen ermöglichen innovative Produkte und Kostenersparnisse. Zudem ermöglichen spezialisierte Cloud-Anbieter mehr Sicherheit für die Bankinfrastruktur. Damit sind Cloud-Dienstleistungen beziehungsweise Cloud Banking ein kritischer Erfolgsfaktor für den Schweizer Finanzplatz.

Viele Bankkunden nutzen Cloud-Dienstleistungen im alltäglichen Leben, ohne sich dessen bewusst zu sein. Sie versenden Mails, streamen Musik und Filme oder speichern Urlaubsfotos auf der Cloud. Was im Privaten funktioniert, sollte auch für hoch spezialisierte Banken und ihr komplexes Geschäft möglich sein. Dies ist heute aufgrund verschiedener rechtlicher und regulatorischer Unsicherheiten jedoch nicht der Fall.

Mit der Migration von Infrastruktur und Prozessen in eine Cloud können Banken die Zeit bis zur Marktreife für innovative Produkte und Dienstleistungen radikal verkürzen und damit ihre Wettbewerbsfähigkeit deutlich steigern. In der Cloud sind neue Technologien wie beispielsweise künstliche Intelligenz ohne grosse Investitionen in eigene Hardware und Software nutzbar. Durch Zugang auf einen grossen Datenpool und die entsprechende Rechenleistung wird die Analyse von grossen Datenmengen in Echtzeit ermöglicht. Damit können beispielsweise innovative und massgeschneiderte Beratungsdienstleistungen für den einzelnen Kunden angeboten oder komplexe Compliance- und Risk-Prozesse automatisiert werden. Auch in der Entwicklung und im Testing 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 ermöglicht die Nutzung der Cloud volle Kostentransparenz und somit eine wirksamere Unternehmungsführung. Da nur direkt bezogene Leistungen abgerechnet werden, kann ein Unternehmen auf Bedürfnisschwankungen mittels Zu- oder Abschaltung von IT-Ressourcen flexibel reagieren. Das Funktionsangebot ist im «Self Service» zu variablen Kosten nutzbar.

Der Aufbau oder Einkauf der entsprechenden Kompetenzen und Ressourcen in der eigenen IT-Infrastruktur sind nicht mehr nötig. Dadurch wird die Migration in eine Cloud gerade für kleine Banken attraktiv. Gewisse Technologien, die früher grossen Unternehmen vorbehalten waren, werden auch für kleine Banken zugänglich (Demokratisierung des Technologiezugangs) und ermöglichen signifikante Skaleneffekte[1]. Gerade kleinere Banken können den steigenden Anforderungen an den IT-Betrieb (IT-Sicherheit, Nachführen von Patches[2], Management des IT-Infrastruktur-Lifecycles) immer weniger gerecht werden.

Bei Schweizer Banken ist ein zunehmendes Bewusstsein für die Vorteile von Cloud Computing und der Wunsch nach einem Wechsel in die Cloud zu beobachten. Gleichzeitig hat sich zwischen nationalen und internationalen Cloud-Anbietern erfreulicherweise eine Wettbewerbssituation eingestellt. Aufgrund ihrer besonderen Bedürfnisse können Banken diese Dienstleistungen namentlich für kundenbezogene Daten noch nicht vollumfänglich nutzen. Die zunehmende Inanspruchnahme von Cloud-Dienstleistungen wird den Finanzplatz und das Finanzökosystem in der Schweiz in Zukunft aber weiter stärken.

1 Aufgrund einer marginalen Kostengleichung können viele Banken eine eigene Cloud nicht zu den gleichen Kosten bereitstellen wie spezialisierte Cloud-Anbieter. Mit einer zunehmenden Aufgabenbündelung 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.

Definitionen

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 Service-provider-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].

Cloud Banking wird in diesem Zusammenhang als die Bereitstellung und Erbringung von Bank- und Finanzdienstleistungen auf Grundlage der Cloud-Technologie definiert.

Regulatorische Fragen in Bezug auf Cloud Banking

Aufgrund des grossen Potenzials im Bereich Cloud Banking engagiert sich die SBVg stark, um die Rahmenbedingungen zu verbessern. Behörden, Provider und die Branche stehen dabei in einem engen Austausch.

Aktuell bilden rechtliche und regulatorische Unsicherheiten mit nicht abschliessend beurteilbaren Risiken eine wesentliche Hürde für die breitere Nutzung von Cloud-Dienstleistungen. Dazu gehören:

- **Steuerung (Governance)**: Auswahl des Cloud-Anbieters und seiner Unterakkordanten (Zulieferer) sowie Zustimmung bei einem Wechsel der Unterakkordanten
- **Datenbearbeitung**: Bearbeitung von Daten über Bankkunden und Bankkundengeheimnis
- **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

Insbesondere fehlten bisher eine Auslegung des geltenden gesetzlichen Rahmens und das Verständnis, welche technischen, organisatorischen und vertraglichen Massnahmen zur Risikominderung in den oben genannten Fällen geeignet sind.

Mit diesem Leitfaden versucht die Arbeitsgruppe der SBVg Grundlagen für die erleichterte Beschaffung und den Einsatz von Cloud-Dienstleistungen durch Banken und Effektenhändler zu erstellen. Die SBVg übernimmt damit eine wichtige Aufgabe zur Klärung der rechtlichen Rahmenbedingungen bezüglich Cloud Banking. Das Vorgehen ist effizient und verhindert, dass jede Bank individuell die gleichen Abklärungen vornehmen muss. Zudem kann die Arbeitsgruppe wertvolles Knowhow bündeln. Von einer breiten Anwendung der Cloud-Technologie dank Rechtssicherheit profitiert schliesslich jedes einzelne Institut und ihre Kunden hinsichtlich innovativer Produkte und Kostenvorteilen.

Der vorliegende Leitfaden der SBVg ist eine Sammlung von rechtlich nicht-bindenden Empfehlungen, die bei der Beschaffung und beim Einsatz von Cloud-Dienstleistungen durch Banken und die Cloud-Anbieter herangezogen werden können. Der Leitfaden enthält auch Auslegungen, welche Rechtsunsicherheiten oder fehlende Rechtsprechung für die zum Teil neuartigen Herausforderungen beim Einsatz der Cloud-Dienstleistungen schliessen sollen. Mit dem Leitfaden wird ein schnelles und flexibles Handeln mit pragmatischen Lösungen ermöglicht. Dieses Vorgehen ist einer spezifischen Cloud-Regulierung vorzuziehen, da diese langsam, nicht technologieneutral und schnell veraltet wäre. Die Institute sollen bei der Anwendung des Leitfadens ihre Grösse und die Komplexität ihres Geschäftsmodells risikobasiert und verhältnismässig berücksichtigen.

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

Zentrale Lösungsansätze der SBVg im Leitfaden

A) Auswahl und Wechsel von Cloud-Anbietern und Zulieferern

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

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 unter anderem folgende Punkte berücksichtig werden:

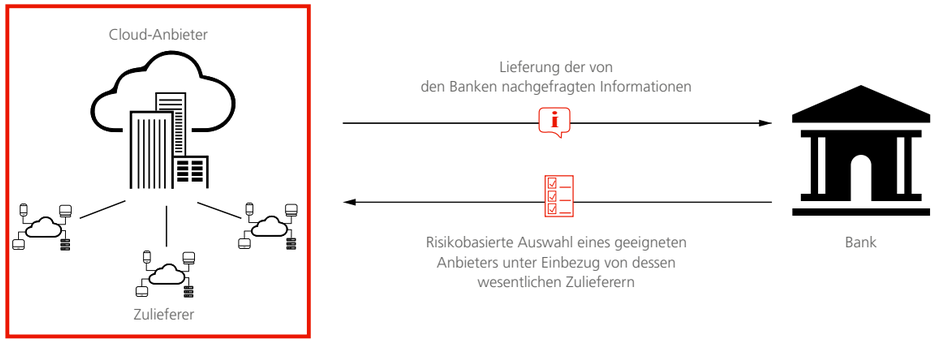
- Fähigkeit zur Erfüllung der vertraglichen Pflichten;
- wirtschaftliche Stabilität;
- Jurisdiktion, welcher der Cloud-Anbieter untersteht.

Weiter sollte geklärt werden, ob der Cloud-Anbieter bereit ist, neben diesen leistungsbezogenen Kriterien auch die wesentlichen Pflichten aus geltenden finanzmarktrechtlichen und datenschutzrechtlichen Vorgaben zu übernehmen.

Abb. 1

Auswahl und Wechsel von Cloud-Anbietern und Zulieferern

Pflichten von Anbietern gegenüber der Bank



Der Cloud-Anbieter sollte der Bank die nachgefragten Informationen zur Verfügung stellen sowie über einen allfälligen Wechsel eines wesentlichen Zulieferers informieren. Die Bank kann, sofern sie damit nicht einverstanden ist, ihren Vertrag mit dem Cloud-Anbieter auflösen und die ausgelagerten Funktionen, Dienstleistungen und allfällige geschützte Informationen zurückführen oder auf neue Cloud-Anbieter übertragen.

Quelle: Schweizerische Bankiervereinigung (SBVg) 2019

Bei der Auswahl eines Cloud-Anbieters und dessen Zulieferern müssen der Vertraulichkeit und Sicherheit der Daten als integraler Bestandteil der zugrunde liegenden Sorgfaltsprüfung (Due Diligence) ein hoher Stellenwert beigemessen werden.

Eine Bank soll über einen Wechsel eines wesentlichen Zulieferers vorgängig informiert werden (vgl. Abbildung 1). Weiter sollte die Bank geeignete Vorkehrungen treffen, um ausgelagerte Funktionen, Dienstleistungen sowie geschützte Informationen in den eigenen Betrieb zurückführen oder auf neue Cloud-Anbieter übertragen zu können. Dazu gehören zum Beispiel eine angemessene Kündigungsfrist oder die Option auf die Verlängerung des bisherigen Betriebsmodells.

B) Einhaltung des Bankkundengeheimnisses in der Cloud

> Zweck der im Leitfaden aufgeführten Empfehlungen:
> Das **Bankkundengeheimnis** und der **Schutz der Daten** werden auch **in der Cloud jederzeit gewährleistet**.

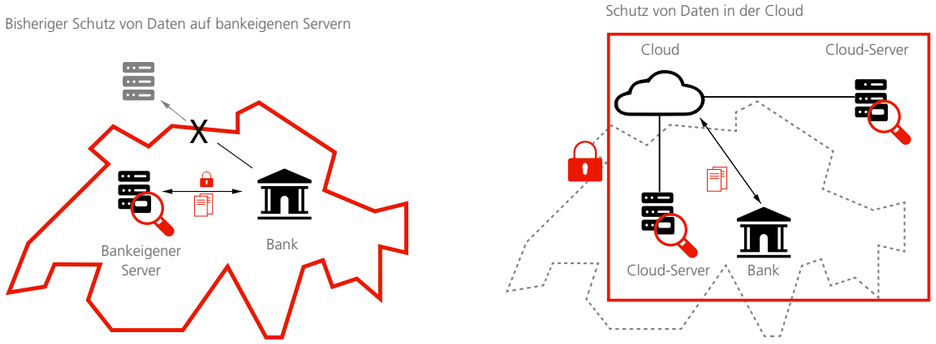
Sofern im Rahmen der Cloud-Dienstleistungen Kundendaten (CID) oder Personendaten bearbeitet werden, sind das Bankkundengeheimnis und die Datenschutzgesetze zu berücksichtigen.

Bisher gilt hier bei Banken das «Over-the-border out-of-control Prinzip»: Sobald Daten ausserhalb der Schweiz gespeichert werden, befanden sie sich ausserhalb des Kontrollbereichs der Schweizer Gerichte. Als Folge werden weder CID ausserhalb der Schweiz gehalten noch der Zugriff aus dem Ausland ermöglicht. Die Aufrechterhaltung dieses Prinzips würde in seiner Absolutheit eine Nutzung der Cloud verunmöglichen.

Im Fokus des Leitfadens steht dabei die Bearbeitung von CID, die Gegenstand des Bankkundengeheimnisses nach Art. 47 BankG sind. Der Leitfaden definiert diesbezüglich technische, vertragliche und organisatorische Massnahmen, um das Risiko eines Zugriffs auf CID durch den Cloud-Anbieter und seine Zulieferer angemessen zu begrenzen (vgl. Abbildung 2).

Abb. 2

Das Bankkundengeheimnis in der Cloud



Schutz der Daten gemäss Bankkundengeheimnis gewährleistet. «Over the border out of control»: Jurisdiktion bildete in der Praxis Grenze in Bezug auf die Datenkontrolle.

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

Quelle: Schweizerische Bankiervereinigung (SBVg) 2019

Schutz von Kundendaten in der Cloud

Technische Massnahmen

- **Anonymisierung**: Bei der Anonymisierung werden personenbezogene Attribute (zum Beispiel Name und andere Identifikationsmerkmale einer Person) irreversibel beziehungsweise unwiederbringlich verändert, dass nicht mehr auf die betroffene Person geschlossen werden kann. Die Daten sind folglich nicht mehr als CID beziehungsweise Personendaten zu klassifizieren.
- **Pseudonymisierung**: Bei der Pseudonymisierung werden personenbezogene Attribute durch ein Kennzeichen, ein sogenanntes Pseudonym, ersetzt. Die Zuordnungsregel dieser Pseudonymisierung sollte unter der Kontrolle der Bank in der Schweiz stehen und angemessen geschützt werden. Jeder Zugang sollte nach dem Need-to-know-Prinzip geschützt und der Zugriff nachvollziehbar protokolliert werden.

- **Verschlüsselung**: Bei der Verschlüsselung wird ein Klartext[4] durch einen Schlüssel in einen Geheimtext umgewandelt. Die Ausgangsinformationen werden dadurch nur noch unter Verwendung des passenden Schlüssels wieder lesbar. Der Zugriff auf diesen Verschlüsselungsschlüssel sollte unter der Kontrolle der Bank stehen und vor unberechtigten Zugriffen geschützt sein, darf aber dem Cloud-Anbieter zur Verfügung stehen oder bei diesem aufbewahrt werden. Das Verschlüsselungsverfahren wie auch die Stärke des Verschlüsselungsschlüssels müssen den gegenwärtigen Sicherheitsstandards Rechnung tragen, sodass die Verschlüsselung als kryptographisch sicher betrachtet werden kann. Eine Übermittlung von CID sollte immer verschlüsselt erfolgen.

Organisatorische Massnahmen

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

Vertragliche Massnahmen

- Angemessene vertragliche Festlegung der technischen und organisatorischen Massnahmen;
- Pflicht des Cloud-Anbieters, organisatorische und technische Massnahmen auf seine Zulieferer zu überbinden, sofern diese CID bearbeiten;
- Vereinbarung der Wahrung der Vertraulichkeit durch den Cloud-Anbieter;
- 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 der Bank oder des Cloud-Anbieters bei Anfragen von Behörden oder bei Verfahren, welche eine Herausgabe oder Übermittlung von geschützten Informationen, welche in der Cloud bearbeitet werden, zum Gegenstand haben.

4 Der offene Wortlaut eines Textes beziehungsweise eine unverschlüsselte Nachricht.

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

> Zweck der im Leitfaden aufgeführten Empfehlungen:
> Für Anfragen von ausländischen Behörden zur Herausgabe von geschützten Informationen ist ein **abgestimmtes Vorgehen zwischen Cloud-Anbieter und Institut** definiert.

Anfragen von Behörden oder Verfahren können die Herausgabe oder die Übermittlung von geschützten Informationen, 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 werden sollte, das eine Herausgabe oder Übermittlung von geschützten Informationen zum Gegenstand hat.

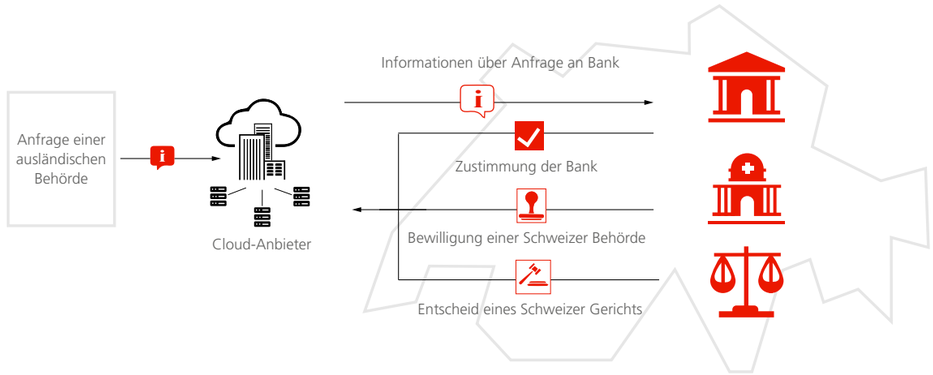
Soweit rechtlich möglich, sollten geschützte Informationen nur im Falle einer schriftlichen Zustimmung des Instituts, des Entscheids eines zuständigen Schweizer Gerichts oder der Bewilligung einer Schweizer Behörde an ausländische Behörden übermittelt werden (vgl. Abbildung 3).

Der Cloud-Anbieter sollte das Institut rechtzeitig informieren, soweit dies rechtlich zulässig ist, falls ausländische Behörden eine Anfrage anbringen, welche die Übermittlung oder Bekanntgabe von geschützten Informationen in der Cloud zum Gegenstand haben. Ausserdem sollten dem Institut die Rechte zur Verfahrensführung eingeräumt werden. Weiter soll der Cloud-Anbieter das Institut bei der Behandlung von Anfragen ausländischer Behörden unterstützen.

Abb. 3

Anfrage von ausländischen Behörden

Herausgabe geschützter Informationen unter bestimmten Voraussetzungen



Bei Anfragen ausländischer Behörden zur Herausgabe geschützter Informationen, welche in der Cloud bearbeitet werden, hat der Cloud-Anbieter das Vorgehen mit der Bank abzustimmen. Geschützte Informationen dürfen nur im Einklang mit geltenden gesetzlichen Bestimmungen und der schriftlichen Zustimmung der Bank, aufgrund eines Entscheids des zuständigen Schweizer Gerichts oder aufgrund einer Bewilligung der zuständigen Schweizer Behörde übermittelt werden.

Quelle: Schweizerische Bankiervereinigung (SBVg) 2019

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

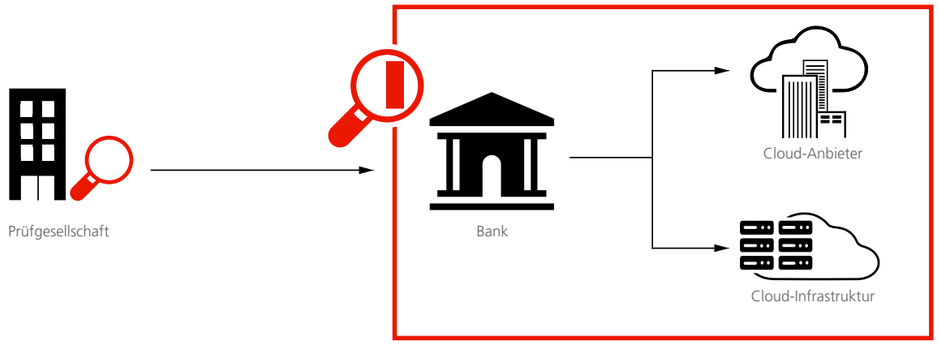
Zweck der im Leitfaden aufgeführten Empfehlungen:
Der **Zugriff** durch Dritte **auf Daten in der Cloud zum Zwecke der Prüfung (Auditierung)** ist jederzeit gewährleistet.

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

Abb. 4

Prüfung (Auditierung) in der Cloud

Prüfung der Cloud-Infrastruktur erfordert hohe Spezialisierung



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

Quelle: Schweizerische Bankiervereinigung (SBVg) 2019

Die Einhaltung der auf den Cloud-Anbieter anwendbaren gesetzlichen, regulatorischen und vertraglichen Anforderungen sollte regelmässig geprüft werden. Dazu gehören insbesondere Anforderungen bezüglich Outsourcing, Datenschutz und Informationssicherheit. Die Prüfungen sollten vom Institut, deren interner und 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[5] ist ausreichend. Die Prüfung der wesentlichen Unterakkordanten durch das Institut kann indirekt durch die Prüfung des Cloud-Anbieters erfolgen (vgl. Abbildung 4).

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

Rechtlicher und regulatorischer Leitfaden

für den

Einsatz von Cloud-Dienstleistungen durch Banken und Effektenhändler 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 Daten über Bankkunden und Bankkundengeheimnis (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)

In diesen Leitfaden wurden auch Auslegungen aufgenommen, welche Rechtsunsicherheiten oder fehlende Rechtsprechung für die zum Teil neuartigen Herausforderungen beim Einsatz der Cloud-Dienstleistungen schliessen sollen und demzufolge nicht mit allen zuständigen Stellen gefestigt wurden. Die Institute können aber 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 im Sinne des FINMA-RS 08/10 dar.

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) «**Anhang 3 FINMA-RS 08/21**» Anhang 3 «Umgang mit elektronischen Kundendaten» des FINMA-RS 08/21.
c) «**BankG**» das Bundesgesetz über die Banken und Sparkassen (Bankengesetz, BankG), SR 952.0.
d) «**BankV**» die Verordnung über die Banken und Sparkassen (Bankenverordnung, BankV), SR 952.02.
e) «**Bankkundengeheimnis**» das gemäss Art. 47 BankG geschützte Geheimnis.
f) «**bearbeiten**» wie er gemäss Datenschutzgesetz definiert wird. Der Begriff «bearbeiten» umfasst auch den Begriff «verarbeiten» oder ähnliche Begriffe, wie sie in den anwendbaren Datenschutzgesetzen definiert werden.
g) «**BEHG**» das Bundesgesetz über die Börsen und den Effektenhandel (Börsengesetz, BEHG), SR 954.1.
h) «**BEHV**» die Verordnung über die Börsen und den Effektenhandel (Börsenverordnung, BEHV), SR 954.11.
i) «**CID**» Kundenidentifikationsdaten gemäss Ziffer 52 des Anhang 3 RS 08/21.
j) «**Cloud**» oder «Cloud Computing» wie es vom National Institute of Standard and Technology (NIST)[1] oder von der European Union Agency for Network and Information Security (ENISA)[2] 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.
k) «**Cloud-Dienstleistungen**» die Service-Modelle des Anbieters im Bereich Cloud Computing im Auftrag des Instituts.
l) «**DSG**» das Bundesgesetz über den Datenschutz, SR 235.1.

1 https://csrc.nist.gov/publications/detail/sp/800-145/final
2 https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

m) «**FINMA-RS 18/3**» das Rundschreiben der Eidgenössischen Finanzmarktaufsicht 2018/3, Outsourcing – Banken und Versicherer, Auslagerungen bei Banken und Versicherungsunternehmen, Datum des Erlasses: 21. September 2017, in der jeweils geltenden Fassung.

n) «**FINMA-RS 08/21**» das Rundschreiben der Eidgenössischen Finanzmarktaufsicht 2008/21, Operationelle Risiken – Banken, Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken, Datum des Erlasses: 20. November 2008, in der jeweils geltenden Fassung.

o) «**FINMA-RS 08/10**» das Rundschreiben 2008/10, Selbstregulierung als Mindeststandard, Datum des Erlasses: 20. November 2008, in der jeweils geltenden Fassung.

p) «**geschützte Informationen**» sind CID, Personendaten sowie vom Institut als vertraulich zu behandelnde bezeichnete weiteren Informationen und Daten.

q) «**Institut**» Banken und Effektenhändler gemäss Ziffer 5 des FINMA-RS 18/3.

r) «**Kunden**» die Kunden eines Instituts.

s) «**Leitfaden**» die in dem vorliegenden Dokument festgehaltenen Grundsätze und Empfehlungen.

t) «**Massen-CID**» Massen-CID gemäss Ziffer 53 des Anhang 3 FINMA-RS 08/21.

u) «**Personendaten**» wie er in den jeweils anwendbaren Datenschutzgesetzen definiert wird. Der Begriff «Personendaten» umfasst auch den Begriff «personenbezogene Daten» oder ähnliche Begriffe, wie sie in den anwendbaren Datenschutzgesetzen definiert werden.

v) «**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.

Kapitel II: Steuerung (Governance)

Rechtliche Grundlagen

- Art. 3 und 47 BankG, Art. 12 BankV
- Art. 10 und 43 BEHG sowie Art. 19 f. BEHV
- DSG
- FINMA-RS 08/21 und insbesondere Anhang 3 FINMA-RS 08/21
- 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[3], sollten neben den mit dem Beziehen der Cloud-Dienstleistungen verbundenen Chancen und Risiken die Wesentlichkeit der Cloud-Dienstleistungen im Sinne von FINMA-RS 18/3, sowie die Qualifikation der im Rahmen der Cloud-Dienstleistungen bearbeiteten geschützten Informationen, insbesondere CID, Rechnung getragen werden.

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

3 Beispielsweise wären Risiken zu bewerten, welche im Zusammenhang mit der Datensicherheit oder dem anwendbaren Recht stehen.

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.

4 Verantwortlichkeiten und Rollen

9 Aufgrund der Regulierung des Instituts sind gegebenenfalls finanzmarktrechtliche Vorschriften und, sofern im Rahmen der Cloud-Dienstleistungen CID oder Personendaten bearbeitet werden, das Bankkundengeheimnis und die Datenschutzgesetze 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 vertraglichen Pflichten, die wirtschaftliche Stabilität, die Jurisdiktion, der der Anbieter untersteht, und weitere massgebliche Punkte bei Auswahl des geeigneten Anbieters berücksichtigt werden. 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.

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[4] und datenschutzrechtlichen Vorgaben und die Ausgestaltung des Betriebsmodells berücksichtigt werden. Bei der Auswahl eines Anbieters und dessen Unterakkordanten, welche CID des Instituts oder sonstige Personendaten bearbeiten, sollte die Vertraulichkeit und Sicherheit der Daten ein ausschlaggebendes Kriterium sowie integraler Bestandteil der zugrunde liegenden Sorgfaltsprüfung (Due Diligence) sein. Dies gilt insbesondere für alle Arten von Aktivitäten, die einen Zugriff auf Massen-CID[5] beinhalten.

17 Ein Wechsel des Anbieters 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 Jurisdiktion, 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.

4 Einschliesslich Bankkundengeheimnis.
5 Siehe die Anforderungen gemäss FINMA Rundschreiben 08/21 Operationelle Risiken – Banken, insbesondere Anhang 3.

18 Der Einbezug neuer wesentlicher Unterakkordanten oder deren Wechsel muss den im FINMA RS 03/18 festgelegten Grundsätzen folgen[6]. Die vertragliche Vereinbarung von Kriterien für den Einbezug wesentlicher Unterakkordanten, deren Einhaltung der Anbieter sicher zu stellen 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 des Vertrags mit dem 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, sodass die ausgelagerten Funktionen und Dienstleistungen sowie die geschützten Informationen 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 geschützten Informationen berücksichtigt werden.

6 Datenzentren und Betriebszentren

19 Zuweilen bestehen Bedenken, wonach mit der Nutzung von Cloud-Dienstleistungen ein Kontrollverlust über die bearbeiteten Daten einhergehe und dass eine Lokalisierung der Orte, wo Daten gespeichert sind und bearbeitet werden, nicht mehr möglich sei (Ubiquität der Daten). Aus Sicht der Institute ist das Vertrauen ihrer 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.

6 FINMA RS 03/18 Randnummer 33.

21 Eine Verlegung von Standorten während der Vertragslaufzeit in eine andere Jurisdiktion sollte bei geschützten Informationen einem vertraglich definierten Änderungsverfahren unterstehen und, abhängig vom individuellen Schutzbedürfnis, der vorgängigen Zustimmung des Instituts unterliegen. 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 Eine solche vorgängige Zustimmung sollte ohne weitere Angaben der Gründe verweigert werden können. Das Institut sollte andernfalls die geeigneten Vorkehrungen treffen, insbesondere sich eine genügend lange Kündigungsfrist und eine geeignete Beendigungsunterstützung des Anbieters ausbedingen, gegebenenfalls auch Verlängerungsoptionen unter Aufrechterhaltung des bisherigen Betriebsmodells, sodass die ausgelagerten Funktionen und Dienstleistungen sowie die geschützten Informationen zurückgeführt oder auf einen neuen Anbieter transferiert werden können. Dabei sollten auch sogenannte Lock-In-Effekte, und Menge, Anzahl sowie Kritikalität der ausgelagerten Funktionen und Dienstleistungen sowie der geschützten Informationen berücksichtigt werden. Weitere sich aus einem Datenzugriff durch Dritte ergebende Anforderungen werden in den folgenden Kapiteln beschrieben.

Kapitel III: Daten und Datensicherheit

Rechtliche Grundlagen

- Art. 47 BankG
- Art. 43 BEHG
- Anhang 3 FINMA-RS 08/21
- 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, sollte eine Klassifizierung der mittels der Cloud-Dienstleistungen bearbeiteten geschützten Informationen durch das Institut vorgenommen werden.

24 Eine solche Klassifizierung 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 Kontrollen zu beurteilen und zu definieren.

25 Dabei sollte in Betracht gezogen werden, ob und wieweit Kunden über eine Auslagerung der Bearbeitung von CID an einen Anbieter von Cloud-Dienstleistungen in der Schweiz oder im Ausland, informiert wurden oder, sofern und soweit notwendig, einer solchen Auslagerung zugestimmt haben[7].

7 Dazu Kapitel III: 10 Bankgeheimnis und Sicherheitsmassnahmen.

26 Massgebliche Änderungen der Klassifizierung der ausgelagerten geschützten Informationen während der Vertragslaufzeit sollten erfasst und notwendige Massnahmen vor solchen Auslagerungen umgesetzt werden.

8 Speicherorte und Datenflüsse, Zugriffskonzept

27 Der Anbieter sollte es dem Institut ermöglichen, die Zulässigkeit der Orte der Bearbeitung von CID und gegebenenfalls anderer geschützter Informationen zu prüfen und diese Orte der Bearbeitung zu kontrollieren. Auch sollte das Institut in der Lage sein, seinen Pflichten gegenüber den Kunden bezüglich Transparenz nachzukommen und entsprechend die Orte der Bearbeitung, insbesondere der Speicherorte der geschützten Informationen, in dem für diese Zwecke erforderlichen Detaillierungsgrad, zu kennen.

28 Auch geschützte Informationen 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 vertraglich festgelegt werden.

29 Zu Letzterem gehört auch die Definition und Umsetzung eines Zugriffskonzepts[8] durch den Anbieter. Erteilte Zugriffsberechtigungen[9] sollten vom Anbieter auf Nachfrage offengelegt werden und Zugriffe auf geschützte Informationen, insbesondere CID, 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 geschützte Informationen verarbeitet 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.

8 Hinsichtlich Zugriffe auf geschützte Informationen.
9 Siehe Fussnote 7.

9 Allgemeine technische und organisatorische Massnahmen der Datensicherheit

31 Im Allgemeinen sollten vom Anbieter angemessene technische und organisatorische Massnahmen zum Schutz der bearbeiteten geschützten Informationen des Instituts angeboten und vereinbarungsgemäss ergriffen werden. Dabei sollten internationale und lokale Standards berücksichtigt werden. Die Einhaltung solcher Massnahmen sollte, soweit anwendbar[10], auf die Unterakkordanten und auf die vom Anbieter und den Unterakkordanten eingesetzten Mitarbeitenden überbunden werden.

32 Der Anbieter sollte sicherstellen, dass seine Mitarbeitenden und diejenigen der Unterakkordanten, welche Zugriff auf geschützte Informationen, einschliesslich CID, haben, sich nachweislich zur Geheimhaltung und vertraulichen Behandlung verpflichten und entsprechend informiert und geschult werden. 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 weiter als ausreichend erachtet, wenn in einer solchen Verpflichtung die Geheimhaltung den datenschutzrechtlichen Vorgaben entspricht, auch wenn eine Verpflichtung auf das Bankkundengeheimnis nicht explizit vorgenommen wird. Es ist jedoch den Anbietern zu empfehlen, die in der Schweiz tätigen Mitarbeitenden ausdrücklich auf das Bankkundengeheimnis und die Strafandrohung bei dessen Verletzung hinzuweisen. Gleiches gilt mit Bezug auf die Verletzung von Geschäftsgeheimnissen samt Strafandrohung bei dessen Verletzung[11].

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 durch den Kunden notwendig ist. Dieses wäre der Fall, wenn das Institut durch die Inanspruchnahme der Cloud-Dienstleistungen das Bankkundengeheimnis vorsätzlich oder fahrlässig verletzen würde.

10 Dabei sollte die Wesentlichkeit eines Unterakkordanten berücksichtigt werden.
11 Art. 162 StGB.

34 Vorliegend wird vertreten, dass eine Entbindung vom Bankkundengeheimnis durch den Kunden nicht notwendig ist, wenn das Institut angemessene Sicherheitsmassnahmen hinsichtlich der im Rahmen der Cloud-Dienstleistungen bearbeiteten CID vorgesehen hat.

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

10.2 Technische, organisatorische und vertragliche Sicherheitsmassnahmen

35 Eine Verletzung des Bankkundengeheimnisses besteht in einer durch das Institut vorsätzlich oder fahrlässig verursachten Offenbarung von CID an Unbefugte[12]. Art. 47 Abs. 1 BankG ist ein Erfolgsdelikt, allein die Möglichkeit einer Kenntnisnahme von CID durch Unbefugte stellt keine Verletzung des Bankkundengeheimnisses dar.

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

37 Die jeweils zu berücksichtigenden Massnahmen ergeben sich aus Anhang 3 FINMA-RS 08/21 und den anwendbaren datenschutzrechtlichen Bestimmungen. Die Beurteilung der Angemessenheit dieser Massnahmen sollte unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Bearbeitung der CID sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte der betroffenen Kunden erfolgen.

Im Folgenden werden einige Massnahmen beispielhaft aufgeführt.

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

38 Technische Massnahmen zum Schutz von CID:

Technische Massnahmen können bewirken, dass die in der Cloud bearbeiteten Daten nicht mehr als CID zu qualifizieren sind. Die Definition des Begriffs CID[13] orientiert sich am datenschutzrechtlichen Personendatenbegriff. Demensprechend sind gemäss der in der Schweiz anerkannten Rechtspraxis weder anonymisierte noch pseudonymisierte oder verschlüsselte Daten, die der Empfänger mangels Konkordanztabelle oder Verschlüsselungsschlüssel keiner Person zuordnen kann, als Personendaten bzw. CID zu qualifizieren.

Als geeignete technischen Verfahren zum angemessenen Schutz von CID werden insbesondere die nachfolgend aufgeführten Sicherheitsmassnahmen betrachtet[14].

39 **Anonymisierung**: Anonymisierte Daten (irreversible Methodik) sind nicht mehr als CID beziehungsweise Personendaten zu qualifizieren[15]. Die in diesem Abschnitt aufgeführten Anforderungen gelten daher nicht für anonymisierte Daten.

40 **Pseudonymisierung**: Sofern es sich um CID handelt, sollte die jeweilige Zuordnungsregel unter Kontrolle des Instituts in der Schweiz 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 Verschlüsselung von CID, 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 CID im Rahmen der Cloud-Dienstleistung verwendet wird. Das Institut sollte auf der Grundlage einer Beurteilung der Risiken insbesondere im Hinblick der Klassifizierung der CID abwägen, welche Verfahren zur Ausprägung der Kontrolle des Verschlüsselungsschlüssels angemessen sind.

13 Anhang 3 FINMA-RS 08/21, Randziffer 52.
14 Siehe dazu FINMA-RS 08/21, Anhang 3, Randziffer 20 sowie die Definitionen in Randziffern 61 bis 65.
15 Siehe dazu FINMA-RS 08/21, Anhang 3, Randziffer 64.

Das Verschlüsselungsverfahren wie auch die Stärke des Verschlüsselungsschlüssels müssen den gegenwärtigen Sicherheitsstandards Rechnung tragen, sodass die Verschlüsselung als kryptographisch sicher betrachtet werden kann.

Eine Übermittlung von CID sollte stets 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 CID:

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

Die erforderliche[16] Prüfung der Sicherheits- und Vertraulichkeitsstandards des Anbieters sollte anhand von unabhängigen Berichten auf der Grundlage anerkannter Berichtsstandards[17] erfolgen.

43 Vertragliche Massnahmen zum Schutz von CID:

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 Überbindung der massgeblichen organisatorischen und technischen Massnahmen auf Unterakkordanten des Anbieters, sofern diese CID bearbeiten;
- die Vereinbarung der Wahrung der Vertraulichkeit durch den Anbieter;
- die Berücksichtigung der Sensitivität der Daten und die diesbezügliche Verantwortlichkeit des Anbieters;
- die Überwachung der Umsetzung und Einhaltung der technischen, organisatorischen und vertraglichen Massnahmen;
- die Vereinbarungen gemäss Kapitel IV (Behörden und Verfahren).

16 Die Prüfung hat nach den Vorgaben von FINMA-RS 08/21, Anhang 3, Grundsatz 9, zu erfolgen.
17 Beispielsweise Prüfungsstandards der Berichterstattungsoptionen nach ISAE 3000 oder SOC2.

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 CID im Klartext, d.h. weder verschlüsselt noch 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 Vorliegend wird vertreten, dass der Anbieter und seine Unterakkordanten keine Unbefugten im Sinne des Art. 47 Abs. 1 BankG sind. 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[18]. Ausserdem hat das Institut regelmässig Weisungsbefugnis[19] 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. Dieses entspricht dem Sinn und Zweck des Art. 47 Abs. 1 BankG und ist dem Wortlaut nach nicht ausgeschlossen[20]. Darüber hinaus können die im Ausland geltenden rechtlichen und regulatorischen Bestimmungen ebenfalls wirksame Schutzmechanismen vorsehen.

18 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».
19 FINMA-RS 03/18, Randziffer 21.
20 Die Notwendigkeit eines ausdrücklichen Ausschlusses folgt aus dem Legalitätsprinzips des Art. 1 StGB.

47 Die Risikoerhöhung durch eine Klartext-Datenbearbeitung im Ausland ist allerdings im Rahmen der anwendbaren Sicherheitsmassnahmen zu berücksichtigen. Ausschlaggebend für die Beurteilung der Angemessenheit sind unter anderem auch die länderspezifischen Risiken, 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 Anhang 3 FINMA-RS 08/21 und den anwendbaren datenschutzrechtlichen Bestimmungen.

49 Die im Folgenden aufgeführten zusätzlichen 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 des 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 CID durch Mitarbeitende des Anbieters und seiner Unterakkordanten grundsätzlich keine Verletzung des Bankkundengeheimnisses durch das Institut dar.

51 Eine Offenbarung von CID 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 durch das Institut Kenntnis von CID erlangen. Sofern die angemessenen technischen, organisatorischen und vertraglichen Massnahmen zum Schutz der CID ergriffen wurden, stellt

sich in einem solchen Fall allerdings die Frage, ob dem Institut überhaupt ein ursächliches und vorsätzliches oder fahrlässiges Tun oder Unterlassen zur Last gelegt werden kann[21].

10.4 Datenschutzrechtliche Informationspflichten

ANPASSUNG JUNI 2020

52 Soweit im Rahmen der Cloud-Dienstleistungen Personendaten bearbeitet werden, besteht eine datenschutzrechtliche Informationspflicht, 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.

10.5 Weitere Informationspflichten

ANPASSUNG JUNI 2020

53 Weitere Informationspflichten, die sich aus Gründen ausserhalb des Datenschutzrechts ergeben können, sind im Einzelfall zu beurteilen. Zu berücksichtigen sind zum Beispiel der Erwartungshorizont 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 geschützte Informationen, 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.

21 Damit scheidet im Fall der blossen Möglichkeit eines Zugriffs auf CID auch die Annahme eines strafbaren Versuchs der Offenbarung an Unbefugte aus, da es sich um ein Vorsatzdelikt handelt.

55 Der Anbieter sollte sich dazu verpflichten, die geschützten Informationen 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 zurück zu führen, sofern dem Anbieter die dazu notwendigen Mittel[22] und Kenntnisse[23] vorliegen. Der Anbieter sollte diesfalls die geschützten Informationen in einem standardisierten, maschinell lesbaren Format zurück übertragen.

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.

22 Etwa Verschlüsselungsschlüssel.

23 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.

Kapitel IV: Behörden und Verfahren

Rechtliche Grundlagen

- Art. 271 StGB
- Art. 273 StGB
- Art. 47 BankG
- Art. 6 DSG
- Staatsverträge für internationale Rechtshilfe
- FINMA-RS 08/21 Anhang 3, Randziffer 20

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 geschützten Informationen zum Gegenstand haben. Sofern und soweit kein zwingendes gesetzliches Recht entgegensteht, hat sich der Anbieter gegenüber dem Institut zu den nachfolgend in den Randziffern 57 bis 60 genannten Punkten vertraglich zu verpflichten:

58 Der Anbieter, sowie die Unterakkordanten und Konzerngesellschaften des Anbieters dürfen nur im Einklang mit anwendbaren gesetzlichen und regulatorischen Bestimmungen und mit (i) einer vorgängigen schriftlichen Zustimmung des Instituts, (ii) aufgrund eines Entscheids des zuständigen Schweizer Gerichts, oder (iii) aufgrund einer Bewilligung der zuständigen Schweizer Behörde, geschützte Informationen, 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 geschützten Daten 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 geschützten Informationen 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 Kunden die angemessenen Rechts- oder Schutzmassnahmen ergreifen.[24]

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 geschützten Informationen zum Gegenstand haben oder haben könnten und auf den Anbieter sowie auf die Unterakkordanten[25] oder Konzerngesellschaften des Anbieters[26] anwendbar sind.

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

24 Siehe Kapitel II und III, insbesondere die Ausführungen zum Bankkundengeheimnis und der datenschutzrechtlichen Transparenz.
25 Unterakkordanten, welche Zugriff auf geschützte Informationen, insbesondere CID, haben.
26 Siehe Fussnote 22.

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

Rechtliche Grundlagen

- Art. 18 und 23 ff. BankG sowie Ausführungsbestimmungen BankV
- Art. 17 BEHG
- FINMA-RS 08/21
- FINMA-RS 18/3

63 Cloud-Dienstleistungen werden von den Anbietern regelmässig aus hochsicheren Rechenzentren gegenüber einer grossen Anzahl von Kunden[27] erbracht. Die Prüfung (Auditierung) der von den Anbietern eingesetzten Infrastrukturen erfordert eine hohe Spezialisierung; dabei sollten die Vertraulichkeitsverpflichtungen des Anbieters gegenüber seinen anderen Kunden beachtet werden.

64 Die Einhaltung der auf den Anbieter anwendbaren oder mittels Vertrag überbundenen Anforderungen, die sich aus dem gesetzlichen 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, deren interner und externer Prüfgesellschaft oder von der FINMA durchgeführt und veranlasst werden können. 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.

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 Auslandbezug 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 Vertrag 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.

27 Public Cloud.

•SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.org