● Whitepaper

SBVg-Cloud-Leitfaden 3.0

Was Banken jetzt wissen müssen

eraneos

Management Summary

Synopsis

Die Schweizerische Bankiervereinigung (SBVg) hat im November 2025 die dritte Auflage ihres Cloud-Leitfadens veröffentlicht. Der vorliegende Beitrag analysiert die wesentlichen Neuerungen und ordnet sie regulatorisch ein. Im Zentrum steht der risikobasierte Ansatz, wonach nicht sämtliche theoretisch denkbaren Risikoszenarien abgesichert werden müssen, sondern nur die im konkreten Einzelfall voraussehbaren und mit verhältnismässigem Aufwand vermeidbaren. Die dritte Auflage berücksichtigt insbesondere die Anforderungen aus dem FINMA-Rundschreiben 2023/01 zu operationellen Risiken und Resilienz. Der Beitrag beleuchtet die vier Schwerpunktthemen des Leitfadens – Governance, Datenbearbeitung mit Fokus auf Bankkundendaten, behördliche Herausgabeanfragen sowie Audit-Anforderungen – und zeigt auf, wie der Leitfaden den Umgang mit Cloud-Diensten im regulierten Umfeld vereinfacht, ohne sämtliche Umsetzungsfragen abschliessend zu klären. Abschliessend wird der schweizerische Ansatz dem EU-Recht, namentlich DORA, gegenübergestellt.

Wie Eraneos Kunden unterstützt

Eraneos begleitet Finanzinstitute und andere regulierte Organisationen bei der Entwicklung und Umsetzung ihrer Cloud-Strategien – von der ersten Standortbestimmung bis zur nachhaltigen Verankerung im Betrieb. Mit einem bewährten Cloud-Strategierahmen und umfassender Branchenerfahrung im Finanz- und Versicherungssektor unterstützt Eraneos bei der Analyse regulatorischer Anforderungen, der Entwicklung individueller Zielbilder sowie der Auswahl und Integration geeigneter Cloud-Lösungen.

Unsere Kundinnen und Kunden profitieren von:

- Strategischer Beratung zur Verankerung einer Cloud-Strategie, die regulatorische, technische und wirtschaftliche Aspekte integriert
- Umsetzung von Best Practices für Governance, Datenklassifizierung, Schutzmassnahmen und Auditierung gemäss den Anforderungen von FINMA und SBVg
- Begleitung bei Auswahl, Verhandlung und Integration von Cloud-Providern sowie bei der Entwicklung individueller Betriebsmodelle
- Workshops zum Aufbau von Know-how und zur Stärkung der Akzeptanz für Cloud-Initiativen
- Laufende Unterstützung bei der Weiterentwicklung der Cloud-Strategie im Hinblick auf regulatorische und technologische Veränderungen

Mit diesem Ansatz ermöglicht Eraneos seinen Kunden, die Cloud-Transformation im regulierten Umfeld sicher, effizient und zukunftsgerichtet zu nutzen.

Inhalt

Hintergründe, Entwicklung und Schwerpunkte 04

Risikobasierter Ansatz als Schlüsselelement 05

Wichtige Neuerungen der dritten Auflage 06

Vier Schwerpunktthemen 07

1. Steuerung (Governance mit Risk Management) 07

2. Datenbearbeitung mit Fokus auf Bankkundendaten 08

3. Behörden und Verfahren 11

4. Audit der Cloud-Dienstleistungen 14

Internationaler Kontext und Vergleich mit EU-Recht 15

Fazit | Teilweise aber nicht restlose Klärung offener Umsetzungsfragen 16

Hintergründe, Entwicklung und Schwerpunkte

Die Schweizerische Bankiervereinigung (SBVg) hat im November 2025 die dritte Auflage ihres Cloud-Leitfadens veröffentlicht. Der überarbeitete «Rechtliche und regulatorische Leitfaden für den Einsatz von Cloud-Dienstleistungen durch Banken und Wertpapierhäuser» ersetzt die Version von Februar 2020 und berücksichtigt die zwischenzeitlichen rechtlichen und regulatorischen Entwicklungen. Die mit RS-FINMA 2023/01 erfolgte «Totalrevision» der FINMA-Regulierung im Bereich der operationellen Risiken bildet den Hauptanlass für die Aktualisierung des Cloud-Leitfadens und erklärt dessen wichtigste Neuerungen gegenüber der Vorgängerversion. Bspw. wurde das Konzept der «Operationellen Resilienz» aus RS-FINMA 2023/01 im Cloud-Leitfaden übernommen.

Vorab ist anzumerken, dass der Leitfaden selbst kein verbindliches Recht setzt, sondern als Auslegungshilfe dient. Gleichwohl orientiert sich die Aufsichtsbehörde FINMA in ihrer Praxis an solchen Branchenstandards. Die FINMA wird grundsätzlich bei der Entwicklung solcher Leitfäden konsultiert, wobei der genaue Umfang ihrer Mitwirkung bei diesem spezifischen Leitfaden nicht öffentlich dokumentiert ist. In der Regel erfolgt jedoch ein Austausch zu den wesentlichen Punkten, um sicherzustellen, dass die Branchenleitlinien mit den aufsichtsrechtlichen Erwartungen übereinstimmen. Während die erste Leitfaden-Version von 2019 hauptsächlich grundlegende rechtliche Fragen adressierte, stehen heute vermehrt die konkreten technischen und organisatorischen Massnahmen im Fokus. Die anfänglichen grundsätzlichen, rechtlichen Bedenken – insbesondere bezüglich Bankkundengeheimnis und Datenschutz – wurden aufgrund der zusehend detaillierteren FINMA-Regulierung sowie der sich dahingehend entwickelten Behörden und Branchenpraxis weitgehend geklärt. Damit hat sich die Diskussion von der grundsätzlichen Zulässigkeit zur praktischen Umsetzung verlagert.

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.

Mithin bilden insbesondere Fragen um technische und organisatorische Massnahmen (zur Umsetzung der Vorgaben von RS-FINMA 2023/01) die Schwerpunkte des revidierten Cloud-Leitfadens, wobei rechtliche Fragen im engeren Sinn, nach wie vor relevant sind (Stichwort: «Foreign Lawful Access»).

Risikobasierter Ansatz als Schlüsselelement

Ein zentrales Konzept des Leitfadens ist der risikobasierte Ansatz bei der Definition und Implementierung technischer, organisatorischer und vertraglicher Massnahmen.
Diese müssen nicht sämtliche theoretisch denkbaren Risikoszenarien adressieren, sondern fokussieren auf diejenigen, die im konkreten Einzelfall nach dem gewöhnlichen Lauf der Dinge voraussehbar und bei pflichtgemässem Verhalten vermeidbar sind.

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.

INFOBOX

Primäre Risiken und Schutzmassnahmen

Primäre Risiken

Risiken für Vertraulichkeit
- Datenzugriff Cloud-Anbieter
- Datenzugriff externer Dritter (Angreifer)
- Datenabfluss aufgrund technischer Fehler
- Lawful Access

Risiken für Verfügbarkeit
- Technischer Ausfall Cloud-Anbieter oder Infrastruktur
- Sperrung aufgrund hoheitlicher Anordnung (bspw. Sanktionen)
- Sperrung durch externe Dritte (insb. Ransomware)

Risikobasierter Ansatz: Voraussehbare Risiken müssen mit Massnahmen abgesichert werden

Technische Massnahmen
- → Anonymisierung
- → Pseudonymisierung
- → Verschlüsselung
- → Redundante Datenhaltung

Organisat. Massnahmen
- → Kontinuierliche Überwachung der Dienstleister
- → Regelmässige Prüfung der Sicherheitsstandards
- → Zugriffs- und Berechtigungs-konzept (auch techn. Mass.)
- → Dokumentation und Aufzeichnung
- → Exit-Strategie definieren
- → Mehrere Cloud-Anbieter

Vertragliche Massnahmen
- → Verfahren bei Behördenanfragen regeln
- → Informationspflichten
- → Prüfungs- und Anfechtungspflichten
- → Verfahrensführungsrechte für Institut
- → Vertraulichkeitsverpflichtung
- → Audit-Rechte

Vertraulichkeit Verfügbarkeit

Wichtige Neuerungen der dritten Auflage

Im Vergleich zur zweiten Auflage aus dem Jahr 2020 enthält die neue Version folgende wesentliche Änderungen:

- Stärkerer Fokus auf Resilienz: Die dritte Auflage berücksichtigt die Anforderungen aus dem FINMA-Rundschreiben 2023/01 zu operationellen Risiken und Resilienz, das nach der zweiten Auflage in Kraft getreten ist.

- Konkretisierung des risikobasierten Ansatzes:
  Die neue Version betont stärker, dass angemessene techni sche, organisatorische und vertragliche Massnahmen nicht sämtliche theoretisch denkbaren Risikoszenarien adressieren müssen, sondern auf diejenigen fokussieren sollen, die im konkreten Einzelfall voraussehbar und vermeidbar sind.

- Aktualisierte Begriffsdefinitionen: Die dritte Auflage ergänzt und präzisiert Begriffe und nimmt neu bspw. den Begriff der «kritischen Daten» gemäss FINMA-RS 2023/01 auf.

- Erweiterte Governance-Anforderungen: Der Leitfaden unterstreicht die Notwendigkeit einer verbindlichen Governance mit klaren Aufgaben, Kompetenzen und Verantwortlichkeiten für den ordnungsgemässen Betrieb nach Projektabschluss.

- Klarere Regelungen zu behördlichen Anfragen: Die Ausführungen zum Umgang mit «Foreign Lawful Access» - dem Zugriff ausländischer Behörden auf Daten - wurden präzisiert und erweitert.

- Praktische Anwendungsorientierung: Die neue Fassung ist stärker auf die konkrete Umsetzung der Cloud-Strategie in verschiedenen Instituten ausgerichtet und berücksichtigt die unterschiedlichen Geschäfts- und Betriebsmodelle.

Der Cloud-Leitfaden des SBVg gliedert sich auch in seiner dritten Auflage in die bekannten Kapitel mit den vier inhaltlichen Schwerpunkten Steuerung (Governance mit Risk Management), Daten, Behörden sowie Audit.

Vier Schwerpunkt-themen

1. Steuerung (Governance mit Risk Management)

PRAXISBOX: Cloud-Governance nach Projektabschluss

Die dritte Auflage betont die Notwendigkeit einer **verbindlichen Governance mit klaren Aufgaben, Kompetenzen und Verantwortlichkeiten** – insbesondere für den laufenden Betrieb nach Projektabschluss:

- **Laufende Überwachung** der Cloud-Dienstleistungen
- **Regelmässige Überprüfung** der Risikobeurteilung
- **Rechtzeitige Erkennung und Bewertung** von Änderungen beim Anbieter oder in dessen Lieferkette

→ Beispiel: Anpassung der Cloud-Governance

Eine Regionalbank nutzt Microsoft 365 für die interne Kommunikation. Die Governance-Überwachung ergibt, dass Microsoft einen neuen Unterakkordanten für Support in einem Drittstaat beigezogen hat.

Erforderliche Governance-Massnahmen:

- Aktualisierung der Risikobeurteilung bezüglich des neuen Auslandsbezugs
- Prüfung der vertraglichen Absicherung (Informationspflichten, Datenschutzgarantien)
- Bewertung, ob zusätzliche technische Massnahmen erforderlich sind
- Dokumentation der Entscheidung und ggf. Eskalation an zuständige Gremien

Die dritte Auflage unterstreicht die Notwendigkeit einer verbindlichen Governance mit klaren Aufgaben, Kompetenzen und Verantwortlichkeiten – nicht nur während der Projektphase, sondern insbesondere für den ordnungsgemässen Betrieb nach Projektabschluss. Dies umfasst die laufende Überwachung der Cloud-Dienstleistungen, die regelmässige Überprüfung der Risikobeurteilung sowie die Sicherstellung, dass Änderungen beim Cloud-Anbieter oder in dessen Lieferkette rechtzeitig erkannt und bewertet werden. Die Auswahl des Cloud-Anbieters und seiner Unterakkordanten sowie die Zustimmung bei einem Wechsel der Zulieferer erfordern einen strukturierten Prozess. Bei der Auswahl müssen Finanzinstitute besonders folgende Kriterien berücksichtigen:

- Fähigkeit zur Erfüllung vertraglicher Pflichten mittels angemessener technischer und organisatorischer Massnahmen
- Wirtschaftliche Stabilität des Anbieters
- Anwendbare Rechtsordnung

Der Leitfaden empfiehlt darüber hinaus die Prüfung der Bereitschaft des Cloud-Anbieters zur Übernahme finanzmarkt- und datenschutzrechtlicher Pflichten.

Wesentliche Änderungen wie der Wechsel eines Zulieferers muss der Cloud-Anbieter dem Institut vorgängig mitteilen (FINMA-RS 18/3 Rz 33). Zudem sollten geeignete Vorkehrungen für eine allfällige Rückführung der ausgelagerten Funktionen und Daten getroffen werden (Exit-Strategie). Der Leitfaden betont, dass solche Exit-Szenarien nicht nur konzeptionell durchdacht, sondern auch praktisch umsetzbar sein müssen, ein Aspekt, der im Kontext der operationellen Resilienz besondere Bedeutung erlangt (vgl. FINMA-RS 23/01, insb. Rz 87 ff.).

Aus praktischer Sicht empfiehlt der Leitfaden schliesslich, bei Dienstleistungsverträgen, in denen über Links auf Anhänge verwiesen wird, die zum Zeitpunkt des Vertragsschlusses gültigen Anhänge herunterzuladen und abzulegen, um die Nachvollziehbarkeit und Beweissicherung zu gewährleisten.

INFOBOX

Zu schützende Bankdaten

Bankkundendaten
Sämtliche bankkundengeheimnisrelevante Daten (Art. 47 BankG) –

Schutz der Vertraulichkeit im Vordergrund

Personendaten
Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 lit. a DSG) –

Schutz der Vertraulichkeit im Vordergrund

Kritische Daten
Daten, die für die erfolgreiche und nachhaltige Erbringung der Dienstleistungen des Instituts oder für regulatorische Zwecke wesentlich sind (FINMA-RS 23/01 Rz 7, FINMA-RS 18/03 RZ 31) –
Schutz der Verfügbarkeit im Vordergrund

2. Datenbearbeitung mit Fokus auf Bankkundendaten

Die Behandlung von Bankkundendaten (definiert als: sämtliche bankkundengeheimnisrelevante Daten) stellt eines der zentralen Themen des revidierten Cloud-Leitfadens dar. Die dritte Auflage präzisiert die Anforderungen und berücksichtigt Erfahrungswerte aus der Praxis der vergangenen Jahre.

Eine wesentliche Neuerung ist die differenziertere Kategorisierung von Daten. Neben «Bankkundendaten» nimmt der Leitfaden nun auch Bezug auf «Personendaten» gemäss Datenschutzgesetz (DSG) und «Kritische Daten» gemäss FINMA-RS 2023/1. Die Klassifizierung der Daten dient als massgeblicher Anknüpfungspunkt für die risikoadäquate Differenzierung der Schutzmassnahmen.

Der Leitfaden beschreibt und präzisiert verschiedene technische, organisatorische und vertragliche Massnahmen zum Schutz von Bankkundendaten:

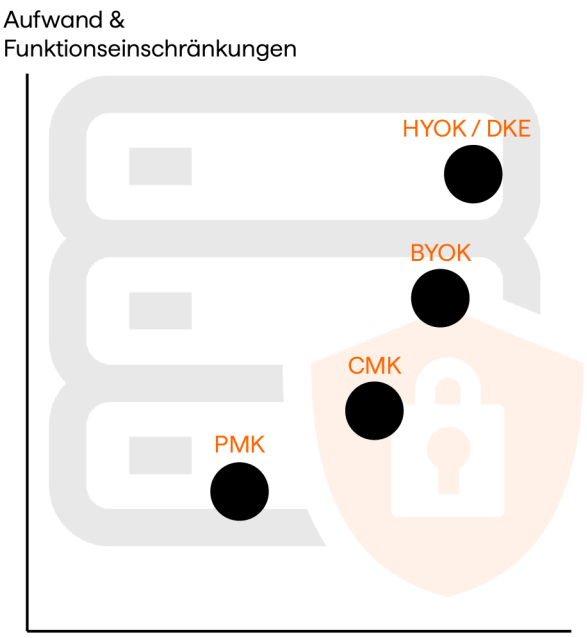
Technische Massnahmen:

- Anonymisierung: Bei der Anonymisierung werden personenbezogene Attribute mit an Sicherheit grenzender Wahrscheinlichkeit irreversibel verändert, sodass niemand mehr auf die betroffene Person schliessen kann. Solche Daten gelten nicht mehr als Bankkunden- oder Personendaten.

- Pseudonymisierung: Bei der Pseudonymisierung werden personenbezogene Attribute durch ein Kennzeichen ersetzt, wobei die Zuordnungsregel unter Kontrolle des Instituts bleiben muss.

- Verschlüsselung: Die dritte Auflage beschreibt Verschlüsselung als «Hauptanwendungsfall der Pseudonymisierung» und konkretisiert die Anforderungen an aktuell gültige Sicherheitsstandards.

INFOBOX: Verwaltungstypen Verschlüssungsschlüssel



→ Provider-Managed Keys (PMK) / Service-Managed Keys
- Die Cloud-Plattform generiert, verwaltet und hält alle Schlüssel vollständig selbst.
- Die Institute haben keinen Zugriff auf die Schlüssel, profitieren aber von automatischer Schlüsselrotation und -verwaltung.

→ Customer-Managed Keys (CMK)
- Das Institut erstellt, besitzt und verwaltet die Schlüssel im Cloud-eigenen Key Management Service.
- Die Schlüssel verbleiben in der Cloud, das Institut steuert jedoch Lebenszyklus, Rotation, Zugriff, etc.

→ Bring Your Own Key (BYOK) / Institut-eigene Schlüssel
- Das Institut generiert die Schlüssel in einer eigenen Infrastruktur (z.B. in einem eigenen Hardware-Sicherheitsmodul) und importiert diese dann in den Cloud Key Management Service.

→ Hold Your Own Key (HYOK) / Double Key Encryption (DKE)
- Das Institut behält die vollständige Kontrolle über die Verschlüsselungsschlüssel; diese verlassen die eigene Infrastruktur nie.
- Die Daten können nur in der On-Premises-Umgebung des Instituts entschlüsselt werden.

Datenverschlüsselung, Stärke und Kontrolle des Verschlüsselungsschlüssels sollen gemäss den aktuellen Sicherheitsstandards und auf Grundlage einer Risikobeurteilung erfolgen. Die Cloud-Anbieter stellen unterschiedliche Varianten zur Verfügung, die sich im Wesentlichen hinsichtlich der Kontrolle der Schlüsselverwaltung und der dafür benötigten technischen und organisatorischen Fähigkeiten unterscheiden.

Im Sinne eines Stufenmodells lassen sich die Varianten wie folgt gruppieren:

1. **Provider-Managed Keys / Service-Managed Keys**
   - Die Cloud-Plattform generiert, verwaltet und hält alle Schlüssel vollständig selbst.
   - Die Institute haben keinen Zugriff auf die Schlüssel, profitieren aber von automatischer Schlüsselrotation und -verwaltung.
   - Bsp. Cloud-Services: Azure-Standardverschlüsselung für gespeicherte Daten (z.B., Azure Storage Service Encryption), SSE-S3 von AWS (Server Side Encryption mit S3 Managed Keys) und Standard Data-at-Rest Encryption in Microsoft 365
2. **Customer-Managed Keys (CMK)**
   - Das Institut erstellt, besitzt und verwaltet die Schlüssel im Cloud-eigenen Key Management Service
   - Die Schlüssel verbleiben in der Cloud, das Institut steuert jedoch Lebenszyklus, Rotation, Zugriff, etc.
   - Bsp. Cloud-Services dafür sind: Customer Managed Keys im Azure Key Vault, Customer Master Keys in AWS KMS und Kundengesteuerte Verschlüsselung in Microsoft 365
3. **Bring Your Own Key (BYOK) / Institut-eigene Schlüssel**
   - Das Institut generiert die Schlüssel in einer eigenen Infrastruktur (z.B. in einem eigenen Hardware-Sicherheitsmodul) und importiert diese dann in den Cloud Key Management Service.
   - Bsp. Cloud-Services: Azure Key Vault BYOK, AWS KMS Import Key Material und Microsoft 365 BYOK-Funktionalität (nur für bestimmte Dienste verfügbar)
4. **Hold Your Own Key (HYOK) / Double Key Encryption (DKE)**
   - Das Institut behält die vollständige Kontrolle über die Verschlüsselungsschlüssel; diese verlassen die eigene Infrastruktur nie.
   - Die Daten können nur in der On-Premises-Umgebung des Instituts entschlüsselt werden.
   - Diese Variante bietet den höchsten Schutz vor unberechtigten Zugriffen, ist jedoch für die meisten Cloud-Services im grossflächigen Einsatz nicht praktikabel, da wesentliche Cloud-Funktionalitäten eingeschränkt werden.
   - Bsp. Umsetzungen: Microsoft DKE, AWS XKS

Die mögliche Einflussnahme des Instituts, beispielsweise zum Entzug des Schlüssels in einem Cloud-Service, nimmt über die Stufen hinweg zu. Parallel dazu steigen allerdings auch die Anforderungen und Aufwände des Instituts bezüglich der Verwaltung der Schlüssel entlang der fortschreitenden Stufen. Insbesondere bei der BYOK-Variante können die Anforderungen erheblich zunehmen.

Organisatorische Massnahmen:

- Überwachung der Dienstleister: Kontinuierliche Kontrolle der vom Cloud-Anbieter und seinen Unterakkordanten durchgeführten operativen Massnahmen.
- Prüfung der Sicherheitsstandards: Regelmässige Beurteilung der Sicherheits- und Vertraulichkeitsstandards des Anbieters anhand unabhängiger Berichte nach anerkannten Prüfstandards.
- Zugriffs-/Berechtigungskonzept: Definition und Überwachung der Zugriffe auf Bankkundendaten unter Beachtung der Zweckbindung mit Aufzeichnung und regelmässiger Überprüfung.

Vertragliche Massnahmen:

- Definition der Schutzmassnahmen: Vertragliche Festlegung konkreter technischer und organisatorischer Massnahmen zwischen Institut und Anbieter sowie Überbindung auf Unterakkordanten.
- Vertraulichkeitsverpflichtungen: Bindende Vereinbarungen zur Wahrung der Vertraulichkeit mit definierten Umsetzungsvorgaben.
- Datensensitivität: Klare Regelung der anbieterseitigen Verantwortlichkeiten je nach Schutzbedarf der Daten.
- Audit-Rechte: Vertraglich gesicherte Möglichkeiten zur Überwachung und Prüfung durch unabhängige Prüfgesellschaften.
- Behördliche Anfragen: Festgelegte Prozesse für den Umgang mit Behördenanfragen bezüglich Bankkundendaten.
- Sicherheitsvorfälle: Prozeduren für die Erkennung, Meldung und Bearbeitung von Vertraulichkeits- und Sicherheitsverletzungen.

Im Ergebnis ist ein wesentlicher Zusatz der dritten Auflage die explizite Betonung des risikobasierten Ansatzes. Der neue Leitfaden stellt klar, dass nicht alle theoretisch denkbaren Szenarien abgesichert werden müssen, sondern nur jene, die «im konkreten Einzelfall nach dem gewöhnlichen Lauf der Dinge voraussehbar und bei pflichtgemässem Verhalten vermeidbar sind.» Dies erlaubt eine institutsspezifische, verhältnismässige Umsetzung von Schutzmassnahmen.

Diese Klarstellungen sind für Schweizer Banken von Bedeutung, da das Bankkundengeheimnis nicht mehr als grundsätzliches Hindernis für Cloud-Lösungen betrachtet werden muss. Institute können datenschutzkonforme Cloud-Strategien entwickeln, ohne bei jedem Kundenkontakt separate Einwilligungen einholen zu müssen.

3. Behörden und Verfahren

PRAXISBOX: Foreign Lawful Access & US CLOUD Act

→ Das Risiko
Der US CLOUD Act ermöglicht US-Behörden seit 2018, von Cloud-Anbietern Daten unabhängig vom Speicherort zu verlangen. Ähnliche Regelungen bestehen in weiteren Ländern (z.B. China). Eine solche Herausgabe kann aus schweizerischer Sicht unzulässig sein, selbst wenn sie nach ausländischem Recht rechtmässig wäre.

→ Vertragliche Massnahmen zur Risikoreduktion
Das Restrisiko lässt sich durch vertragliche Vereinbarungen weiter reduzieren:

- **Rechtzeitige Information** des Instituts bei Behördenanfragen (soweit zulässig)
- **Selbständige Prüfung** und ggfs. Anfechtung Ersuche bei Benachrichtigungsverbot
- **Erwirkung einstweiliger Massnahmen** zur Aussetzung der Wirkung des Ersuchens
- **Einräumung der Verfahrensführungsrechte** für das Institut
- **Regelmässige Berichterstattung** über Anzahl und Art ausländischer Verfahren

→ Die praktische Konsequenz
Angesichts der geringen Eintrittswahrscheinlichkeit und der vertraglichen Absicherung stufen viele Institute das CLOUD Act-Risiko als nicht «im gewöhnlichen Lauf der Dinge» liegend ein – und verzichten auf restriktive Massnahmen wie HYOK oder DKE zugunsten voller Cloud-Funktionalität.

Anfragen von Behörden oder Verfahren können die Herausgabe oder die Übermittlung von geschützten Informationen, welche in der Cloud bearbeitet werden, zum Gegenstand haben. Der Leitfaden unterscheidet zwischen rechtmässigen Zugriffen durch Schweizer Behörden («Lawful Access») und rechtmässigen Zugriffen durch ausländische Behörden («Foreign Lawful Access»).

Ein Zugriff gilt als rechtmässig («lawful»), wenn er auf einer gesetzlichen Grundlage basiert und im Einklang mit dem anwendbaren Recht erfolgt.

Lawful Access
Stützt sich eine zuständige Schweizer Behörde beim Ersuchen auf Herausgabe der Bankkundendaten auf eine schweizerische Rechtsgrundlage, ist von einem «Lawful Access» die Rede. Das betroffene Finanzinstitut muss im Einzelfall prüfen, ob die Herausgabe von der jeweiligen Rechtsgrundlage tatsächlich abgedeckt ist. Es ist verpflichtet:

- Die rechtliche Grundlage des Ersuchens zu prüfen.
- Sicherzustellen, dass nur die vom Ersuchen tatsächlich erfassten Daten offengelegt werden.
- Die Herausgabe im Einklang mit den gesetzlichen Vorgaben vorzunehmen.

Foreign Lawful Access
Stützt sich eine ausländische Behörde auf eine eigene Rechtsgrundlage, liegt ein «Foreign Lawful Access» vor. Eine Herausgabe von Bankkundendaten kann aus Sicht der schweizerischen Rechtsordnung unzulässig sein (bspw., wenn die betroffenen Informationen durch das Bankkundengeheimnis geschützt sind) – auch dann, wenn die ausländische Rechtsgrundlage die Herausgabe rechtmässig vorsieht.

Diesfalls gilt es, die Herausgabe der Bankkundendaten mittels angemessener, vorgängig implementierter technischer, organisatorischer und vertraglicher Massnahmen entweder mit an Sicherheit grenzender Wahrscheinlichkeit zu vermeiden oder aber nur Informationen herauszugeben, die keinen direkten oder indirekten Rückschluss durch, aus Sicht des schweizerischen Rechts, unberechtigte Dritte auf die Identität der geschützten Person vorsehen.

Falls das nicht möglich sein sollte, muss das Finanzinstitut überprüfen, ob die fragliche Herausgabe bzw. Übermittlung mit einer Einwilligung des Instituts, einer Einwilligung der betroffenen Personen, dem Entscheid eines zuständigen Schweizer Gerichts oder der Bewilligung der zuständigen Schweizer Behörde an ausländische Behörden gerechtfertigt werden kann.
Ist auch das nicht möglich, muss das Finanzinstitut die Herausgabe verweigern.

Pflichten des Cloud-Anbieters
Der Cloud-Anbieter sowie allfällige Unterakkordanten und Konzerngesellschaften dürfen geschützte Informationen nur bei Herausgabeanfragen, die «lawful» sind, und alternativ mit (i) vorgängiger schriftlicher Zustimmung des Instituts, (ii) aufgrund eines Entscheids des zuständigen Schweizer Gerichts oder (iii) aufgrund einer Genehmigung der zuständigen Schweizer Behörde an ausländische Behörden bekanntgeben.

Der Cloud-Anbieter muss, soweit rechtlich zulässig, das Institut rechtzeitig über Herausgabeanfragen informieren. Ist ihm dies untersagt, soll er selbständig die Rechtmässigkeit des Offenlegungsersuchens überprüfen und gegebenenfalls anfechten. Er hat dabei soweit möglich die Wirkung des Gesuches aufzuschieben, bspw. durch das Verlangen einstweiliger Massnahmen. Er legt die angeforderten Bankkundendaten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist.

Der Cloud-Anbieter muss das Institut rechtzeitig vor Herausgabe der geschützten Daten informieren, ihm soweit möglich die Rechte zur Verfahrensführung einräumen und es bei der Behandlung von Anfragen ausländischer Behörden unterstützen.

Überdies soll der Anbieter das Finanzinstitut in genereller Art über Anzahl, Gegenstand und Vorgehen von Verfahren informieren, welche nach auf den Anbieter sowie auf seine Unterakkordanten anwendbaren ausländischen Vorschriften eine Bekanntgabe von geschützten Informationen verlangen oder verlangen könnten.

Digitale Souveränität und der US CLOUD Act
Eine in der Praxis besonders häufig diskutierte, aber im Leitfaden nicht direkt angesprochene Quelle für einen «Foreign Lawful Access» ist der US CLOUD Act (Clarifying Lawful Overseas Use of Data Act), der es US-Behörden seit 2018 unter bestimmten Voraussetzungen ermöglicht, von Cloud-Anbietern die Herausgabe von Daten zu verlangen – unabhängig von deren physischem Speicherort. Ähnliche Rechtsgrundlagen bestehen auch in anderen Ländern, beispielsweise im Cyber Security Law in China.

Bei näherer Betrachtung relativiert sich jedoch die praktische Relevanz: Seit dem Inkrafttreten des CLOUD Act sind keine Fälle von behördlich durchgesetzten Zugriffen auf in der Schweiz gespeicherte Daten öffentlich bekannt geworden.

Der «Law Enforcement Requests Report» von Microsoft dokumentiert für das erste Halbjahr 2024 weltweit lediglich einen einzigen Fall, in dem US-Behörden Zugriff auf ausserhalb der USA gespeicherte Daten gewährt wurde. Zudem sehen die grossen Cloud-Anbieter in ihren Verträgen regelmässig Klauseln vor, mit denen sie sich zur Information bei Anfragen sowie gegebenenfalls zur Beschreitung des Rechtswegs verpflichten. Obwohl ein unerwünschter Datenzugriff nicht ausgeschlossen werden kann, erweist sich die Eintrittswahrscheinlichkeit als äusserst gering.

Gleichwohl wird in der Praxis diskutiert, ob über die vertraglichen und organisatorischen Massnahmen hinaus zusätzliche technische Restriktionen erforderlich sind. Erwogen werden etwa End-to-End-Verschlüsselungslösungen, bei denen sich Daten ausschliesslich in der On-Premises-Umgebung des Unternehmens entschlüsseln lassen (Double Key Encryption). Solche Massnahmen schränken allerdings die Cloud-Funktionalitäten erheblich ein.

Im Sinne des risikobasierten Ansatzes obliegt es jedem Institut, eine individuelle Risikoeinschätzung vorzunehmen. Angesichts der dokumentiert geringen Eintrittswahrscheinlichkeit stufen viele Unternehmen das Risiko eines «Foreign Lawful Access» auf Grundlage des US CLOUD Acts als nicht «im gewöhnlichen Lauf der Dinge» liegend ein und verzichten zugunsten der Cloud-Funktionalitäten auf restriktive technische Massnahmen.

Vertragliche Vereinbarungen betreffend Umgang mit Herausgabeanfragen
Der Umgang mit Herausgabeanfragen ist zwischen dem Institut und dem Cloud-Anbieter vertraglich zu regeln. Die Vereinbarungen sollten mindestens folgende Aspekte abdecken:

- Abgestimmtes Verfahren für den Umgang mit Anfragen, die eine Herausgabe von Bankkundendaten zum Gegenstand haben
- Verpflichtung zur rechtzeitigen Information des Instituts bei Anfragen ausländischer Behörden
- Verfahren bei nicht möglicher vorgängiger Information (Prüfungs- und Anfechtungspflichten)
- Einräumung der Verfahrensführungsrechte für das Institut
- Regelung der Unterstützungspflichten des Anbieters
- Verpflichtung zu regelmässiger Berichterstattung über ausländische Verfahren
- Klare Regelung der zulässigen Herausgabegründe (Einwilligung, Gerichtsentscheid, Behördenbewilligung)

4. Audit der Cloud-Dienst-leistungen

Die Einhaltung der regulatorischen und vertraglichen Anforderungen muss regelmässig geprüft werden. Der Leitfaden sieht hierfür verschiedene Möglichkeiten vor:

- Prüfungen können vom Institut selbst, dessen Prüfgesellschaft oder der FINMA durchgeführt werden
- Pool-Audits durch mehrere Institute und indirekte Audits sind zulässig
- Ein logischer Zugriff auf die Cloud-Infrastruktur für die Prüfung ist ausreichend, physische Vor-Ort-Prüfungen sind nicht zwingend erforderlich

Insoweit die Cloud-Dienstleistung «kritische Daten» umfasst, sind die Institute insbesondere verpflichtet die Punkte gemäss FINMA-RS 2023/1 Randziffer 71-82 zu überprüfen. Weiter enthält der Leitfaden einen umfangreichen ergänzenden Anhang, der spezifische Orientierungshilfen für die Prüfung von Cloud-Dienstleistungen bietet. Dieser Anhang erläutert unter anderem internationale Zertifizierungen und Attestierungen und gibt praktische Hinweise, wie diese im Rahmen des Auditprozesses berücksichtigt werden können. Für Finanzinstitute bedeutet dies eine Vereinfachung der Prüfanforderungen.

Die Möglichkeit von Pool-Audits ermöglicht Kostenteilung, während die Akzeptanz logischer Zugriffsrechte anstelle physischer vor-Ort-Prüfungen den Prüfaufwand unter Umständen beträchtlich reduziert und die Zusammenarbeit mit internationalen Cloud-Anbietern erleichtert. ländischer Behörden unterstützen.

Der Anhang I zum Cloud-Leitfaden liefert eine detaillierte Orientierungshilfe zur Prüfung von Cloud-Dienstleistungen und erläutert verschiedene internationale Audit-Standards wie ISAE 3402, ISAE 3000, SSAE 18 und SOC 2. Er definiert klare Kriterien für die Beurteilung von Prüfberichten und gibt Hinweise, wie Lücken identifiziert und adressiert werden können. Besonders wichtig sind dabei:

- Die Bewertung des Prüfumfangs und der Prüftiefe
- Das Zusammenwirken von Prüfungen beim Cloud-Anbieter und beim Institut
- Die Berücksichtigung der Unabhängigkeit und Qualifikation des Prüfers
- Die Abdeckung wesentlicher Unterakkordanten im Prüfbericht
- Die Identifikation und Behebung von Lücken im Audit
- Das Betriebsmodell des Cloud-Anbieters und in welcher Form die Zugriffe von Administratoren/Operatoren des Cloud-Anbieters auf die Cloud-Plattformen erfolgen und wie sichergestellt wird, dass dabei Zugriffe auf Kundendaten verhindert oder grösstmöglich minimiert werden.

Internationaler Kontext und EU-Vergleich

Der überarbeitete Cloud-Leitfaden der SBVg weist Parallelen zur europäischen Regulierungslandschaft auf. Die begriffliche Annäherung an das EU-Recht zeigt sich beispielhaft am Konzept der «Operationellen Resilienz», das aus dem FINMA-Rundschreiben 2023/01 in den Leitfaden übernommen wurde und dem Ansatz des EU Digital Operational Resilience Act (DORA) entspricht. Auch die differenzierte Betrachtung von Auslagerungsrisiken folgt europäischen Regulierungsmustern, wie sie in den ESMA/EBA-Leitlinien zum Outsourcing verankert sind. Die Behandlung des grenzüberschreitenden Behördenzugriffs («Foreign Lawful Access») im Schweizer Leitfaden adressiert ähnliche Fragestellungen wie die EU-Diskussion um Datensouveränität und den Schutz vor extraterritorialen Zugriffen, wobei insbesondere der US CLOUD Act beide Rechtsräume vor vergleichbare Herausforderungen stellt.
Die materiellen Schutzziele – Datensicherheit, Vertraulichkeit und operationelle Resilienz – sind sodann in beiden Rechtsräumen Hauptzwecke der Regulierung.

Die wesentlichen Unterschiede ergeben sich primär aus den unterschiedlichen Regelungstechniken: Während die EU mit DORA ab Januar 2025 detaillierte, verbindliche Vorgaben für alle Finanzunternehmen einführt, verfolgt die Schweiz auch im Bereich der operationellen Resilienz bei Cloud-Dienstleistungen ihren bewährten Regulierungsansatz: Prinzipienbasierte Vorgaben durch Gesetz- und Verordnungsgeber bilden den Rahmen, FINMA-Rundschreiben konkretisieren die aufsichtsrechtlichen Erwartungen, und (echte oder unechte) Selbstregulierung durch Branchenleitlinien wie den Cloud-Leitfaden der SBVg ergänzt diese mit praxisorientierten Standards. Der in der Schweiz verfolgte Ansatz, nach dem nicht alle theoretisch denkbaren Risiken adressiert werden müssen, sondern nur die im konkreten Einzelfall voraussehbaren und vermeidbaren, unterscheidet sich zudem von den teilweise äusserst detaillierten EU-/mitgliedstaatlichen Vorgaben.

Teilweise aber nicht restlose Klärung offener Umsetzungsfragen

Fazit

Der aktualisierte Cloud-Leitfaden der SBVg vervollständigt die regulatorischen Grundlagen für Cloud-Dienste im Finanzsektor. Mit dem risikobasierten Ansatz, bei dem nur die im konkreten Einzelfall voraussehbaren und vermeidbaren Risiken adressiert werden müssen, wird eine weiterhin praktikable Umsetzung ermöglicht. Die dritte Auflage dokumentiert einen veränderten Fokus: Standen anfänglich rechtliche Grundsatzfragen im Vordergrund, konzentriert sich der Leitfaden nun auf konkrete technische und organisatorische Massnahmen zur Gewährleistung der operationellen Resilienz.

Für Finanzinstitute ergeben sich daraus konkrete Umsetzungserleichterungen. Der Leitfaden schafft Rechtssicherheit bei der Cloud-Nutzung und reduziert durch Instrumente wie Pool-Audits und die Akzeptanz logischer Zugriffsrechte den Prüfaufwand. Die ausführlichen Orientierungshilfen zu Bankkundendaten und zur Anbieterauswahl sowie die hilfreichen, aber lückenhaften Ausführungen zu Foreign Lawful Access ermöglichen eine strukturiertere Herangehensweise an Cloud-Projekte.

Der Leitfaden bestätigt den schweizerischen Regulierungsansatz für Cloud-Dienste. Die Kombination aus prinzipienbasierten Vorgaben, FINMA-Rundschreiben und Selbstregulierung erlaubt institutsspezifische Lösungen. Allerdings zeigt sich darin auch die Kehrseite der häufig als Vorzug des schweizerischen Regulierungsansatzes gelobten prinzipienbasierten und risikoorientierten Regulierung: mangelnde Verbindlichkeit und Rechtssicherheit. So erhalten Praktiker bei zentralen Anwenderfragen, etwa zur konkreten Handhabung von Foreign Lawful Access oder zur Wahl zwischen Verschlüsselungsschlüsselvariante (CMK vs. BYOK oder HYOK), durch den neuen Cloud-Leitfaden kaum die erhoffte Klarheit.

Der Leitfaden präzisiert somit die Rahmenbedingungen für Cloud-Technologien im Finanzsektor, kann jedoch wichtige Fragen der praktischen Umsetzung nicht auflösen. Die betroffenen Personen und Institute müssen weiterhin erhebliche Interpretations- und Entscheidungsleistungen erbringen.

Kontakt aufnehmen

Miro von Mutzenbecher
Analyst, Financial Services

+41 58 123 99 11
miro.vonmutzenbecher@eraneos.com

Eraneos Switzerland
Andreasstrasse 11
8050 Zürich