VISCHER

Genügt eine Cloud-Lösung den Anforderungen einer Schweizer Bank[1]?

von David Rosenthal (drosenthal@vischer.com)

Anforderung	CID (Berufsgeheimnis)	Personendaten (DSG)	Relevanter Faktor für TIA[2]	Wesentliches Outsourcing[3]	Operative Kerndaten[4]	Kernanwendung	Nebenanwendung	Typ / No. Anforderung
Data at-rest in der Schweiz Die Inhaltsdaten[5] werden (nur) auf Servern in der Schweiz gespeichert. Dies sagt noch nichts über den Bearbeitungsort aus.	P		✓			P		**A01**
Data at-rest in Europa Die Inhaltsdaten werden (nur) auf Servern in Europa gespeichert. Dies sagt noch nichts über den Bearbeitungsort aus.		X	✓			X		**A02**
Bearbeitung nur in der Schweiz Die Inhaltsdaten bearbeitet der Provider grundsätzlich nur in der Schweiz, d.h. es kommt weder automatisiert noch manuell zu einem Zugriff von ausserhalb; vorbehalten sind ausserordentliche Situationen.			✓			P		**A03**
Bearbeitung nur in Europa Die Inhaltsdaten bearbeitet der Provider grundsätzlich nur in Europa (aber nicht zwingend in der Schweiz), d.h. es kommt weder automatisiert noch manuell zu einem Zugriff von ausserhalb; vorbehalten sind ausserordentliche Situationen.			✓			P		**A04**
Data at-rest verschlüsselt Im ruhenden Zustand (d.h. bei ihrer Speicherung) sind die Inhaltsdaten nach dem Stand der Technik verschlüsselt.	X	X	✓					**K01**
Zugriff auf Schlüssel von Bank kontrolliert Der für die Entschlüsselung der ruhenden Inhaltsdaten erforderliche Schlüssel steht grundsätzlich nur für jene Benutzer oder Anwendungen/Prozesse zur Verfügung, die der Kunde autorisiert hat. Er kann die Berechtigungen überwachen.	X	P	✓					**K02**

---

1 Ähnliche Anforderungen gelten auch für andere regulierte Finanzinstitute und Berufsgeheimnisträger.

2 Transfer Impact Assessment (um das Risiko eines ausländischen Behördenzugriffs zu ermitteln).

3 Gemäss FINMA-Rundschreiben 2018/3 ("Outsourcing"), Rz. 4 ("Wesentlich sind jene Funktionen, von denen die Einhaltung der Ziele und Vorschriften der Finanzmarktaufsichtsgesetzgebung signifikant abhängt.").

4 Für die Sanierung oder Abwicklung der Bank benötigte Daten (Outsourcing-Rundschreiben, Rz. 31)

5 Gemeint sind die Nutzdaten der jeweiligen Anwendung, also z.B. die mit einer Anwendung walteten Kundendaten der Bank. Nicht gemeint sind die Randdaten der Nutzung der Anwendung oder Kontodaten der Nutzer der Anwendung.

Schlüssel beim Provider, aber von Bank verwaltet Der für die Entschlüsselung der ruhenden Inhaltsdaten erforderliche Schlüssel wird beim Provider aufbewahrt (Schlüsselspeicher), aber das Schlüsselmanagement betreibt (aus der Distanz) die Bank. Sie kann mittels ihrer Instruktion Schlüssel generieren, ersetzen und revozieren.	P		✓					**K03**
Schlüssel nur bei Bank Der für die Entschlüsselung der ruhenden Inhaltsdaten erforderliche Schlüssel ist in einem Schlüsselspeicher in den Händen der Bank und nicht des Providers gespeichert. Sie betreibt auch das Schlüsselmanagement.			✓					**K04**
Data in-transit verschlüsselt Die Übermittlung von Daten im Rahmen von Zugriffen auf die Lösung in der Cloud ist verschlüsselt.	X	X	✓					**K05**
Angemessene Datensicherheit nach dem Stand der Technik Die vom Provider zur Gewährleistung der Datensicherheit der Lösung in der Cloud entspricht dem Stand der Technik und ist angemessen im Hinblick auf den Schutzbedarf im konkreten Fall. Die Massnahmen zur Datensicherheit sind in einem Sicherheitsdispositiv geregelt (mindestens "TOMS"). Es wurde eine Risikoanalyse durchgeführt, die keine inakzeptabel hohen Risiken aufweist.	X	X	✓	X	X	X	X	**S01**
Zugriff für Benutzer nur mit MFA Der Zugriff auf die Lösung in der Cloud, ob mit oder ohne Zugriff auf den Inhaltsdaten, ist mit einer Multi-Faktor-Authentisierung abgesichert.	X	X						**S02**
Datensicherheit nach SSAE 18/ISAE 3402 SOC 1 & 2 Typ II geprüft und dokumentiert Es liegen für alle die Lösung betreffenden Systeme und Prozesse Prüfberichte nach SSAE 18/ISAE 3402 vor, welche auch die Effektivität der Controls bestätigen (Typ II). Der Provider verpflichtet sich, dieses zu liefern.	X	X	✓	X	X	X	X	**S03**
Provider meldet Cyberangriffe sofort Sollte es zu einem Cyberangriff auf die Lösung kommen, welcher die Datensicherheit der Inhaltsdaten tangiert, so ist der Provider verpflichtet, diesen der Bank umgehend zu melden und sie bei der Erfüllung ihrer Meldepflicht gegenüber der FINMA[6] zu unterstützen.				X		X	X	**S04**
Zugriff auf Kundendaten und Lösung durch Bank jederzeit möglich Der Provider verpflichtet sich, der Bank jederzeit Zugang zu seinen Inhaltsdaten und der von der Lösung abgedeckten Funktionalität zu bieten. Es besteht ein angemessenes Service Level Agreement.				X	X			**B01**
Kopie der operativen Kerndaten in der Schweiz Die Lösung stellt auf die eine oder andere Weise sicher, dass eine Kopie der mit Lösung bearbeiteten Daten auf Schweizer Boden aufbewahrt werden. Dies gilt sowohl für Daten, welche die Bank für die Abwicklung ihres Ge-					X			**B02**

[6] Aufsichtsmitteilung 5/2020 der FINMA zur Konkretisierung von Art. 29 Abs. 2 FINMAG.

schäfts zwingend benötigt wie auch die Daten und Software, die erforderlich ist, um auf die Daten in nützlicher Form zuzugreifen.								
Sicherung (Backups) der Daten sichergestellt Es ist sichergestellt, dass die für den Betrieb der Lösung erforderlichen Daten eine Datensicherung besteht, sollte das für den Betrieb der Lösung benutzte System ausfallen oder zerstört werden oder die Daten gelöscht oder in ihrer Integrität verletzt werden. Dies kann mittels Backups, aber auch Mirrors erfolgen.		X		X	X	X		**B03**
Fortführung des Geschäfts auch beim Ausfall der Lösung sichergestellt Es ist im Sinne eines Business Continuity Managements sichergestellt, dass im Falle eines Ausfalls des für den Betrieb der Lösung benutzten Systems die Fortführung der Lösung oder sonst die Geschäftsfortführung der Bank gewährleistet ist. Dies kann z.B. mittels Mirror erfolgen. Es wurde eine Risikoanalyse durchgeführt, die keine inakzeptabel hohen Risiken aufweist.		X		X	X	X		**B04**
Geordnete Rückführung des ausgelagerten Bereichs innert Kündigungsfrist möglich Es ist möglich, dass der Bereich oder die Funktion der Bank, welcher durch die Lösung abgedeckt ist, innert der ordentlichen Kündigungsfrist zu einem anderen Provider oder zurück zur Bank transferiert werden kann.				X	X	X		**B05**
Weiterführung der Dienstleistung bei fehlgeschlagener Rückführung zugesichert Der Provider verpflichtet sich, die Lösung während mindestens zwölf Monaten weiterzubetreiben, falls die Rückführung aus irgendwelchen Gründen scheitern sollte.				X				**B06**
Weiterführung der Dienstleistung im Falle eines Konkurses der Bank Der Provider verpflichtet sich, im Falle eines Konkurses oder der Zahlungsunfähigkeit der Bank den Vertrag auf einen Dritten zu übertragen, welcher das Geschäft der Bank übernimmt, sofern dieser für die Kosten aufkommt.		X		X	X	X		**B07**
Zugang zu den Inhaltsdaten im Falle eines Konkurses des Providers Der Zugang zu ihren Inhaltsdaten ist der Bank auch im Falle eines Konkurses des Providers grundsätzlich zugesichert.				X		X		**B08**
Schriftlicher Vertrag Die Rechte und Pflichten der Parteien und deren Verantwortlichkeiten sind in einem Vertrag dokumentiert. The Vertrag muss den Nachweis durch Text ermöglichen, darf aber elektronisch sein.	X	X	✓	X		X		**C01**
Bank hat ein Weisungsrecht gegenüber Provider Der Provider räumt der Bank ein Weisungsrecht ein, das allerdings auch "standardisiert" sein kann, indem sich die Weisungen aus dem Inhalt des Vertrags und der Kundenkonfiguration ergeben. Im Falle eines ADV gemäss Art. 28 DSGVO ist das Weisungsrecht mit Bezug auf die Bearbeitung von Personendaten enthalten.			✓	X		X		**C02**
ADV gemäss Art. 28 DSGVO Der Provider schliesst mit der Bank einen Auftragsbearbeitungsvertrag gemäss den Vorgaben von Art. 28 DSGVO ab.	X	X	✓	X				**C02**
ADV verweist auf DSG		X	✓	X				**C03**

Der vom Provider vorgesehene Auftragsbearbeitungsvertrag (und die weiteren Bestimmungen zum Datenschutz) verweisen auf das Schweizer DSG (nicht nur die DSGVO) und gelten auch dort, wo nur das DSG zur Anwendung kommt.								
ADV gilt auch für CID (nicht nur Personendaten) Die vorgesehenen Regelungen zur Auftragsbearbeitung gelten nicht nur für Personendaten (d.h. Daten natürlicher Personen), sondern für alle Inhaltsdaten bzw. CID (auch solchen juristischer Personen).	X		✓	X				**C04**
Bank hat ein Widerspruchsrecht gegen den Beizug von wesentlichen Subunternehmern Soweit der Provider Subunternehmer beizieht, die keine Personendaten bearbeiten (dort gilt der ADV) räumt er der Bank ein Widerspruchsrecht ein, falls diese wesentliche Teile der Leistung erbringen sollen. Soweit Subunternehmer sowieso immer (auch) Personendaten bearbeiten, ist dies schon im ADV gemäss Art. 28 DSGVO enthalten.			✓	X				**C05**
Keine Bearbeitung von Inhaltsdaten für Providerzwecke oder analog geschützt wie mit ADV Soweit sich der Provider vorbehält, Inhaltsdaten auch für eigene Zwecke zu bearbeiten (z.B. Abrechnung, Statistik), kommen sinngemäss dieselben Massnahmen (Datensicherheit, Regelung zum Beizug Dritter, Auditrecht, etc.) zur Anwendung, wie sie auch der Auftragsbearbeitungsvertrag vorsieht. Der Zugriff auf CID (im Klartext) durch Mitarbeiter des Providers für eigene Zwecke des Providers, die nicht für die Vertragsabwicklung nötig sind, ist untersagt.	X		✓	X				**C06**
Unbefristete Geheimhaltungspflicht des Providers von Inhaltsdaten Der Provider verpflichtet sich und seine Mitarbeiter zur Geheimhaltung sämtlicher Inhaltsdaten. Diese Geheimhaltungspflicht ist zeitlich unbefristet. Ausnahmen beschränken sich auf gesetzliche Offenlegungspflichten.	X	X	✓	X				**C07**
EU-Standardvertragsklauseln bei Zugriff von ausserhalb Europas Soweit der Provider aus einem Land ohne angemessenen Datenschutz auf Personendaten zugreift, verpflichtet er sich zur Unterzeichnung der Standardvertragsklauseln der Europäischen Kommission (oder nach DSG/DSGVO genehmigten BCR). Falls es der Unterauftragsbearbeiter einen solchen Zugriff aus einem unsicheren Drittland hat, so müssen die Standardvertragsklauseln zwischen dem Provider und dem Unterauftragsbearbeiter abgeschlossen werden (aber nicht notwendigerweise der Bank).		X	✓	X				**C08**
Soweit der Provider Mitarbeiterdaten für eigene Zwecke bearbeitet, hält er sich an den Datenschutz Soweit der Provider Mitarbeiterdaten für eigene Zwecke bearbeitet, verpflichtet er sich einen angemessenen Datenschutz einzuhalten und deren Daten soweit möglich nur pseudonymisiert, verhältnismässig und für nicht personenbezogene Zwecke zu bearbeiten (z.B. kein Direktmarketing). Die Angemessenheit beurteilt sich nach dem Standard in Europa.		X	✓					**C09**
"Defend your Data"-Pflicht bei ausländischem Lawful Access	X	X	✓	X				**C10**

Ist der Provider in Bezug auf Inhaltsdaten mit Herausgabebefehlen von ausländischen Behörden oder Gerichten konfrontiert, so wird er sich gegen diese soweit vernünftig möglich rechtlich zur Wehr setzen. Dies gilt auch bei Behörden des EWR, nicht nur aussereuropäische Behörden.								
Provider muss für Vertragsverletzung angemessen haften Der Vertrag mit dem Provider sieht eine angemessene Haftung des Providers vor (mindestens unmittelbare Schäden bis zur Höhe einer Jahresgebühr). Kein Ausschluss oder Beschränkung der Haftung bei grober Fahrlässigkeit oder Vorsatz des Providers und seiner Hilfspersonen, insbesondere dort nicht, wo das anwendbare Recht solches zulässt (z.B. irisches Recht).	X	X	✓	X	X	X	P	**C11**
Keine unkontrollierten Vertragsänderungen Die vertraglichen Bestimmungen zum Schutz der mit der Lösung bearbeiteten Daten und zur Erfüllung der aufsichtsrechtlichen Vorgaben dürfen vom Provider nicht einseitig angepasst werden können (soweit sie den Schutz schwächen), oder die Bank hat die Möglichkeit, aus der Lösung auszusteigen.	X	X	✓			X		**C12**
Anspruch auf Vertragsanpassung (oder Exit) aus rechtlichen Gründen Sollte eine Rechtsentwicklung eine Anpassung des Vertrags mit dem Provider erforderlich machen, wird dieser darüber mit der Bank in guten Treuen verhandeln. Können sie sich nicht einigen, kann die Bank aus der Lösung aussteigen.				X		X		**C13**
Es besteht kein relevantes Risiko eines ausländischen Behördenzugriffs Die Wahrscheinlichkeit eines ausländischen Behördenzugriffs mit und ohne Rechtsweggarantie wird für eine bestimmte Anwendung und einen bestimmten Zeitraum mit einer Transfer Impact Analysis (TIA) ermittelt. Es existiert hierzu eine statistische Methode zur Ermittlung dieser Wahrscheinlichkeit.[7] Die Wahrscheinlichkeit sollte unter zehn Prozent liegen; ein Zugriff muss für den konkreten Fall der Auslagerung "höchst unwahrscheinlich" sein.	X	X	n.a.	P	P	P		**C14**
Es ist keine Zusicherungen der Bank an ihre Kunden verletzt Ausführungen in AGB, Datenschutzerklärungen und Verträgen dürfen keine Versprechungen oder Aussagen enthalten, welche der Auslagerung entgegenstehen.[8]	X	X						**C15**
Auslagerung ist intern geregelt Aus Inanspruchnahme der Lösung ist durch die internen Regelungen für Outsourcing-Projekte geregelt und es bestehen entsprechende Zuständigkeiten.				X				**C16**
Regelmässige Überprüfung der Datensicherheit (mindestens delegiert) Die Datensicherheit der Lösung wird regelmässig von einer unabhängigen, qualifizierten Prüfstelle überprüft. Deren Prüfbericht (nicht nur Zertifizierung oder Prüfbestätigung) steht der Bank in einer aussagekräftigen Form zur Verfügung. Mängel werden adressiert.	X	X	✓	X		X		**P01**

[7] https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

[8] Gemeint sind Aussagen wie etwa, dass keine Kundendaten im Klartext aus dem Ausland zugänglich sind, wenn dies in Tat und Wahrheit möglich ist.

Prüfung des ausgelagerten Bereichs, inklusive Zugriff auf Daten (uneingeschränkt, auch vor Ort) Die Bank, ihre externe Prüfgesellschaft und die FINMA kann den ausgelagerten Bereich jederzeit, ungehindert und vollumfänglich überprüfen, auch vor Ort.				X				**P02**
Provider gibt der FINMA sämtliche benötigten Auskünfte und Unterlagen Der Provider, der selbst nicht der FINMA untersteht, muss vertraglich verpflichtet sein, ihr für die Aufsicht nötigen Auskünfte zu erteilen und Unterlagen zu geben				X				**P03**
FINMA und externe Prüfgesellschaft können Prüf- und Auskunftsrechte vertraglich direkt durchsetzen Die Prüfgesellschaft und die FINMA können ihre Prüf- und Auskunftsrechte gegen den Provider vertraglich (als Drittbegünstigte) direkt durchsetzen, auch im Ausland und unter dem gewählten Recht. Sie haben einen eigenen Zugang zu etwaigen Prüfberichten, die im Auftrag des Providers erstellt wurden.				X				**P04**
Jede Konzerngesellschaft kann Erfüllungsanspruch, Prüf- und Zugriffsrechte vertraglich direkt durchsetzen Konzerngesellschaften, welche mit dem Provider zwar keinen direkten Vertrag haben, aber die Lösung trotzdem mitnutzen, können den Erfüllungsanspruch sowie ihre Prüf-, Auskunfts- und Zugriffsrechte vertraglich (als Drittbegünstigte) direkt gegen den Provider durchsetzen, auch im Ausland und unter dem gewählten Recht.				X				**P05**

X = Erfordernis P = Psychologisches Erfordernis (= Geschäftsentscheid)

Anforderungskategorie:

A = Architektur K = Kryptographie S = Security

B = BCM C = Compliance P = Prüfrechte

Hinweis: Für eine rechtskonforme Auslagerung müssen noch weitere Voraussetzungen innerhalb des Instituts erfüllt werden (wie die korrekte Einbindung in das IKS, die Inventarisierung, die Überwachung des Providers, die richtige Konfiguration der Lösung etc.). Diese sind hier nicht aufgeführt.