LAUX LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
A Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

RECHTSANWÄLTE
Z Dr. Christian Laux · LLM
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

In den zuständigen
Anwaltsregistern eingetragen

Rechtsgutachten

# Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG

zugleich ein Diskussionsbeitrag aus Anlass der Publikation
eines Cloud-Leitfadens der Schweizerischen Bankiervereinigung (SBVg)
zum Einsatz von Cloud-Dienstleistungen
durch Banken und Effektenhändler

Autoren:
Dr. Christian Laux
Alexander Hofmann
Mark Schieweck
Dr. Jürg Hess

Zürich, 14. Februar 2019

## MANAGEMENT SUMMARY

**Gegenstand**: Das vorliegende Rechtsgutachten erörtert, inwiefern und unter welchen Bedingungen eine Bank[1] Cloud-Angebote[2] nutzen darf. Die Analyse beschränkt sich auf den strafrechtlichen Gesichtspunkt des Bankgeheimnisses und orientiert sich an drei konkreten Fragen:

- Frage 1: (a) Darf eine Schweizer Bank im Lichte von Art. 47 des Bundesgesetzes über die Banken und Sparkassen (Bankengesetz, **BankG**) Cloud-Angebote nutzen? (b) Fällt die Antwort anders aus für Cloud-Angebote mit Auslandsbezug[3]?
- Frage 2: (a) Kann ein Cloud-Anbieter[4] als "Beauftragter" im Sinne von Art. 47 BankG beigezogen werden und ist eine Bekanntgabe von Bankkundendaten an den Cloud-Anbieter dann nach Art. 47 BankG straflos? (b) Fällt die Antwort anders aus für Cloud-Angebote mit Auslandsbezug?
- Frage 3: Ist es nach Art. 47 BankG zulässig, dass ein nicht als Beauftragter bestellter Cloud-Anbieter auf geheimnisbewehrte Informationen zugreift, solange dies rein zu Betriebszwecken (insbesondere IT Maintenance- oder Supportzwecken) erfolgt?

**Resultat vorab**: Nach der hier vertretenen Auffassung stehen reife Cloud-Lösungen im In- und Ausland auch Banken zur Nutzung offen. Die Bank als Nutzerin muss den Cloud-Anbieter sorgfältig auswählen und mittels geeigneter Massnahmen veranlassen, dass die migrierten Daten auch in den IT-Infrastrukturen[5] des Cloud-Anbieters geschützt sind. Ziel dieser Massnahmen ist es, strafrechtlich relevante Offenbarungen im Normalbetrieb[6] zu vermeiden. Um dies dauerhaft gewährleisten zu können, muss die Bank verstehen, wie der um das Cloud-Angebot erweiterte Perimeter funktioniert. Mittels vertraglicher Massnahmen ist dieser Zustand abzusichern. Dies ergibt sich aus dem Folgenden:

**Frage 1**: Wenn die Bank Cloud-Anbieter auswählt, die in technischer, organisatorischer und vertraglicher Hinsicht sicherstellen können, dass im Normalbetrieb keinerlei Offenbarungen an unbefugte Dritte erfolgen, darf die Bank deren Cloud-Angebote nutzen. Die Erfahrung zeigt, dass dies heute für reife Cloud-Anbieter bereits bestätigt werden kann. Die Migration von Daten in die IT-Infrastrukturen solcher Cloud-Anbieter erfüllt das Tatbestandsmerkmal der Offenbarung nicht. Es liegt somit von vornherein kein strafrechtlich sanktioniertes Verhalten vor, ungeachtet dessen, wie die Antwort auf die Fragen 2 und 3 ausfällt (Teilfrage 1a). Die Frage des Auslandsbezugs ist für solche Cloud-Angebote ohne Bedeutung (Teilfrage 1b).

**Frage 2**: Ein Cloud-Anbieter kann als Beauftragter im Sinne von Art. 47 Abs. 1 lit. a BankG bestellt werden. Der personelle Perimeter der Bank wird dadurch erweitert. Die Bank muss darauf achten, dass beim Cloud-Anbieter schützende Massnahmen technischer, organisatorischer und vertraglicher Art umgesetzt sind. Die Migration von Daten in die IT-Infrastrukturen des Cloud-Anbieters stellt keine Offenbarung dar (**Privilegierungswirkung** zu Gunsten der für die Bank handelnden Personen in strafrechtlicher Hinsicht).

---

1 Zum Begriff "Bank" siehe Anhang.
2 Zum Begriff "Cloud-Angebot" siehe Anhang.
3 Zum Begriff "Auslandsbezug" siehe Anhang.
4 Zum Begriff "Cloud-Anbieter" siehe Anhang.
5 Zum Begriff "IT-Infrastrukturen" siehe Anhang.
6 Zum Begriff "Normalbetrieb" siehe Anhang.

Dies gilt auch dann, wenn Mitarbeitende des Cloud-Anbieters Klartext-Zugriff[7] auf Daten der Bank erhalten. Umgekehrt ist die Privilegierungswirkung kein Automatismus. Ein Cloud-Anbieter kann sich dagegen wehren, in die Risikosphäre der Bank eingebunden zu werden. Wenn der Cloud-Anbieter den unter Frage 1 angesprochenen Reifegrad aufweist, kann die Bank das Cloud-Angebot dennoch nutzen.

Die Privilegierungswirkung kann auch bei Migration von Daten in IT-Infrastrukturen eines Cloud-Anbieters mit Auslandsbezug bejaht werden. Massgeblich für dieses Resultat ist der Wortlaut der Regelung in Art. 47 Abs. 1 lit. a BankG. Die Nutzung von Beauftragten mit Auslandsbezug ist darin nicht ausgeschlossen. Art. 1 StGB ("keine Strafe ohne Gesetz") schliesst eine unterschiedliche Behandlung von Cloud-Angeboten mit Auslandsbezug aus. Dieses Resultat muss durch ergänzende Auslegung der Strafnorm in Art. 47 BankG gestützt werden. Die Auslegung führt dabei zum Resultat, dass eine Strafbarkeit bei Beizug von Beauftragten mit Auslandsbezug heute nicht aufrechterhalten werden kann.

Die Privilegierungswirkung erlaubt es der Bank, Cloud-Anbieter selbst dann zu nutzen, wenn es im Rahmen des Normalbetriebs beim Cloud-Anbieter (bzw. seinen Mitarbeitenden oder Sub-Akkordanten) in kontrollierter Weise zu Klartext-Zugriffen auf die geheimnisgeschützte Information kommen kann (Teilfrage 2a). Dies gilt auch für Cloud-Anbieter mit Auslandsbezug (Teilfrage 2b).

**Frage 3**: Für die zuletzt gestellte Frage 3 verbleibt nach Beantwortung der Fragen 1 und 2 nur noch wenig Raum. Soweit der Cloud-Anbieter als Beauftragter bestellt wurde, stellt sich die Problematik per se nicht (privilegierter Informationsaustausch ohne Straffolgen möglich). Auch sonst wird man für viele der unter Frage 3 zu diskutierenden Betriebsmassnahmen in Bezug auf reife Cloud-Anbieter bestätigen können, dass keine Offenbarungen stattfinden (dann gilt von vornherein die Analyse zu Frage 1). Führt Support durch Mitarbeitende eines Cloud-Anbieters, der nicht als Beauftragter bestellt wurde, zu Klartext-Zugriffen auf Informationen von Bankkunden, muss die Bank ein rechtfertigendes Kontrolldispositiv aufsetzen (beispielsweise: Nur "*just in time access*", d.h. Zugriffe nur im Einzelfall; Einsichtnahme nur bei ausgewiesenem Bedürfnis, "*need to know*"; jeweils unter Kontrolle durch die Bank, "*4 eyeballs principle*"; grundsätzlich ohne Übertragung von Steuerungskompetenzen durch den fremden Supportmitarbeitenden, "*least privilege*"). Wird dies in angemessenem Umfang so umgesetzt, kann die Strafbarkeit der Bank unbesehen der Frage der Beauftragtenstellung abgewendet werden.

**Zusammenfassend**: Eine Cloud-Nutzung durch Banken kann ausgehend vom heutigen Stand der Technik, Lehre und Rechtsprechung als rechtmässig bestätigt werden. Reife Cloud-Anbieter kann die Bank auch nutzen, wenn der Cloud-Anbieter der Einbindung in den personellen Perimeter der Bank nicht zustimmt, solange im Sinne der Antworten auf Frage 1 und 3 die Cloud-Lösung gegen Offenbarungen mittels technischer, organisatorischer und vertraglicher Massnahmen ausreichend geschützt ist. So oder so muss die Bank für die Umsetzung von technischen, organisatorischen und vertraglichen Massnahmen sorgen und vom Cloud-Anbieter Transparenz darüber verlangen. Die Bank muss sich mit dem technisch-organisatorischen Reifegrad des Cloud-Anbieters auseinandersetzen und verstehen, wie der Cloud-Anbieter mit Daten umgeht, welche die Bank in dessen IT-Infrastrukturen migriert.

---

[7] Zum Begriff "Klartext-Zugriff" siehe Anhang.

# TEIL 1 GRUNDLAGEN

## I. Anlass und Gegenstand

### A. Anlass für das vorliegende Rechtsgutachten

1 Die Schweizerische Bankiervereinigung (SBVg) hat einen Cloud-Leitfaden zum Einsatz von Cloud-Dienstleistungen durch Banken und Effektenhändler im Entwurf vorliegen. Mit Bezug auf das Bankkundengeheimnis stellt sich die SBVg die folgenden konkreten Fragen:

a. Frage 1: (a) Darf eine Schweizer Bank im Lichte von Art. 47 BankG Cloud-Angebote nutzen? (b) Fällt die Antwort anders aus für Cloud-Angebote mit Auslandsbezug?

b. Frage 2: (a) Kann ein Cloud-Anbieter als "Beauftragter" im Sinne von Art. 47 BankG beigezogen werden und ist eine Bekanntgabe von Bankkundendaten an den Cloud-Anbieter dann nach Art. 47 BankG straflos? (b) Fällt die Antwort anders aus für Cloud-Angebote mit Auslandsbezug?

c. Frage 3: Ist es nach Art. 47 BankG zulässig, dass ein nicht als Beauftragter bestellter Cloud-Anbieter auf geheimnisbewehrte Informationen zugreift, solange dies rein zu Betriebszwecken (insbesondere IT Maintenance- oder Supportzwecken) erfolgt?

2 LAUX LAWYERS AG möchte sich an der Diskussion im Rahmen der Bankiervereinigung beteiligen und bringt zu diesem Zweck das vorliegende Rechtsgutachten in die Diskussion ein. Dieses Rechtsgutachten stellt keine Beurteilung des im Entwurf vorliegenden Cloud-Leitfadens dar.

3 LAUX LAWYERS AG ist eine Anwaltskanzlei mit spezialisierter Fachkompetenz an der Schnittstelle zwischen Recht und Informationstechnologie. Die Anwälte von LAUX LAWYERS AG verfügen über langjährige Erfahrungen in der Finanzbranche (u.a. als Inhouse Counsels bei Schweizerischen Grossbanken und globalen IT-Outsourcingprovidern). LAUX LAWYERS AG berät sowohl Klienten aus der Finanzbranche in IT-rechtlichen Fragen als auch in- und ausländische Cloud-Anbieter im Umgang mit Banken.

### B. Gegenstand

4 Das vorliegende Rechtsgutachten erörtert, inwiefern und unter welchen Bedingungen eine Bank Cloud-Angebote nutzen darf. Die Analyse beschränkt sich auf den strafrechtlichen Gesichtspunkt des Bankgeheimnisses (Art. 47 BankG) und orientiert sich an den genannten drei Fragen der SBVg. Andere Themenkomplexe sind nicht Gegenstand dieses Rechtsgutachtens.[8] Die in diesem Rechtsgutachten verwendeten Begrifflichkeiten finden sich in Anhang 1.

---

8 Namentlich enthält dieses Rechtsgutachten keine Erörterung der FINMA-Rundschreiben (RS 2018/3 "Outsourcing - Banken und Versicherungen" sowie RS 2008/21 "Operationelle Risiken"), von datenschutzrechtlichen Aspekten, von Beschränkungen, die sich eine Bank im Rahmen von internen Richtlinien selber auferlegt haben könnte oder zu denen sich die Bank im

### C. Geheimnisschutz heisst Perimeterschutz

5 Wer für einen Dritten ein Geheimnis wahrt, hat zu kontrollieren, dass das Geheimnis keinem unbefugten Dritten offengelegt wird. Der Geheimnisträger erreicht dieses Ziel, indem er seine Einfluss- und Risikosphäre gegen Lecks absichert, durch welche das Geheimnis Dritten bekannt werden könnte. Diese Absicherungspflicht bezeichnen wir in diesem Rechtsgutachten als Pflicht, den eigenen Perimeter zu sichern. Es geht u.a. um Zutrittskontrolle und Zugriffskontrolle. Perimeterschutz hat mindestens die drei folgenden Ausprägungen:

- Der **physische Perimeter** ist zu schützen: Gebäude etc. sind vor Zutritt durch Unbefugte zu schützen; dies geschieht massgeblich mit baulichen Massnahmen.

- Der **logische Perimeter** ist zu schützen: Netzwerk und andere IT-Infrastrukturen sind vor dem logischen Zugriff durch unbefugte Dritte (Hacker, etc.) zu schützen.

- Der **personelle Perimeter** ist zu schützen: In der arbeitsteiligen Wirtschaft arbeitet niemand mehr allein. Eine Bank z.B. muss aber gleichwohl jederzeit in der Lage sein zu beantworten, "wo die Bank anfängt und wo sie aufhört". Dies geschieht durch angemessene Verträge mit jenen Personen und Unternehmen, welche die Bank in ihrer Aufgabe unterstützen.

6 Aus der Sicht des Bankkunden verhält sich das Vorstehende wie folgt: Der Bankkunde schliesst einen Vertrag mit der Bank als Institution und vertraut auf Geheimhaltung gegenüber bankfremden Personen. Innerhalb der Bank erwartet er griffige Massnahmen zum Schutz seiner Informationen.

## II. Allgemeines zum Bankkundengeheimnis

### A. Rechtsgrundlagen

#### 1. Grundlage im Vertrag

7 Vertragliche Grundlagen: Die Beziehung zwischen einer Bank und ihren Kunden ist primär vertragsrechtlicher Natur. Eine Bank führt für einen Kunden auf Basis einer spezifischen Vereinbarung mindestens ein Konto und ist abrechnungspflichtig. Im Rahmen dieser Vereinbarungen übernimmt die Bank zudem die Verpflichtung, die über den Kunden erlangten Informationen zu schützen. Meist ändert die Bank die nachfolgend kurz zusammengefassten Bestimmungen des Schweizerischen Obligationenrechts (OR) ab. In der Regel wird die Geschäftsbeziehung zum Kunden massgeblich in Allgemeinen Geschäftsbedingungen (**AGB**) umschrieben und geregelt.

8 Ergänzende Grundlagen: Vertraulichkeit wäre auch dann eine Nebenpflicht der Bank gegenüber dem Bankkunden, wenn die konkrete vertragliche Einigung (Rz. 7) sich zu diesem Aspekt nicht

---

Rahmen von Verträgen mit Bankkunden oder Dritten verpflichtet hat; von Aspekten des Behördenzugriffs (z.B. BÜPF oder weitere Spezialthemen wie CLOUD-Act, Behördenzugriff, etc.); von Bestimmungen des Schweizerischen Strafgesetzbuches (Art. 273 StGB etc.). Praktische Ausführungen zur Umsetzung (z.B. umfassende Beschriebe einer konkreten Lösung, Besprechung einzelner technischer, organisatorischer oder vertraglicher Massnahmen oder Kombinationen davon; Hinweise zur Vorgehensplanung einer Cloud-Migration durch die Bank; Anforderungskataloge, welche eine Bank sich geben sollte, um die Cloud-Migration organisatorisch umzusetzen; Anforderungskataloge, um Compliance-Anforderungen abzudecken; Informationsschritte gegenüber Bankkunden) werden nur am Rand behandelt.

äussern würde. Gemäss Art. 398 Abs. 2 OR haftet eine Auftragnehmerin gegenüber dem Auftraggeber für die sorgfältige und treue Besorgung des ihr anvertrauten Geschäfts. In diesem Zusammenhang ist die Bank die Auftragnehmerin, die ein Geschäft des Bankkunden (des Auftraggebers) ausführt. Art. 398 Abs. 2 OR verpflichtet die Bank ausserdem, die sogenannten "Integritätsinteressen" des Bankkunden zu wahren. Dies umfasst das Interesse des Bankkunden an der Wahrung seiner Persönlichkeitsrechte gemäss Art. 28 des Schweizerischen Zivilgesetzbuches (**ZGB**). Angaben über das Bestehen der Bankbeziehung ebenso wie weitere Angaben sind von der Bank auch im Hinblick auf Art. 28 ZGB zu schützen.

## 2. Verstärkung des vertraglichen Schutzes durch Art. 47 BankG

9 Das so abgesteckte Bankkundengeheimnis erhält einen zusätzlichen Schutz durch verschiedene Bestimmungen der öffentlich-rechtlichen Finanzmarktgesetzgebung, von denen die bedeutendste und praktisch relevanteste Art. 47 BankG ist.[9]

10 Daneben verstärken auch das Datenschutzrecht und das Verwaltungsrecht das Bankgeheimnis (z.B. Anhang 3 des Rundschreibens 2008/21 der FINMA). Darauf wird hier jedoch nicht weiter eingegangen.

## 3. Ergänzende Überlegungen

11 Die vorstehende Darstellung der Rechtsgrundlagen in Bezug auf das Bankgeheimnis zeigt, dass das Bankkundengeheimnis in erster Linie privatrechtlich zu denken ist (siehe vorne Rz. 7 ff.). Der Erwartungshorizont des Bankkunden ist somit von Bedeutung (**Integritäts- und Persönlichkeitsschutzinteressen**). Der Bankkunde erwartet von der Bank, *dass* sie ihren Perimeter mit etablierten Mitteln schützt (dazu Rz. 5). Unter dieser Voraussetzung ist der Bankkunde einverstanden mit der Verarbeitung der für ihn besonders sensiblen finanziellen Informationen. Der Bankkunde braucht aber nicht zu wissen, *mit welchen Massnahmen* die Bank ihren Perimeter schützt.

12 Aus Sicht der Bank ist das Bankgeschäft von der **Eigentumsgarantie und Wirtschaftsfreiheit** geschützt. Die Bank darf autonom darüber entscheiden, welches Geschäft und welche Geschäftspolitik sie verfolgen möchte und auch mit welchen (rechtmässigen) Mitteln sie dies tun will. Dazu gehört insbesondere auch der Entscheid darüber, welche IT-Infrastrukturen und welche IT-Organisation die Bank nutzen möchte. Es ist nicht Sache des Bankkunden zu entscheiden, wie die Bank sich organisiert. Die Wahl der Mittel ist der Bank vorbehalten und die Bank muss darüber nicht informieren, *solange sie im Rahmen des Erwarteten und Angemessenen bleibt*.

---

9 Ähnliche Strafbestimmungen finden sich unter anderem in einigen anderen für den Schweizer Finanzmarkt relevanten Gesetzen (Artikel 43 des Bundesgesetzes über die Börsen und den Effektenhandel (BEHG), Artikel 147 des Bundesgesetzes über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (FINFRAG) und Art. 148 Abs. 1 lit k des Bundesgesetzes über die kollektiven Kapitalanlagen (KAG)). Diese Regeln werden in diesem Rechtsgutachten nicht weiter beleuchtet.

13 Die Bank darf auch darauf vertrauen, dass der Bankkunde ihrer internen Organisation nicht widersprechen wird, solange die Bank angemessene Massnahmen zur Sicherung ihres Perimeters aufrechterhält. Insofern greift das **Vertrauensprinzip**. *Solange die Bank angemessene Schutzmassnahmen ergreift, darf sie somit auch die implizite Einwilligung des Bankkunden voraussetzen*.

14 Ergänzend sind die jüngsten gesetzgeberischen Entwicklungen von grosser Bedeutung: Das Bankgeheimnis bietet dem Bankkunden keinen absoluten Schutz vor Offenbarung seiner Daten gegenüber Aussenstehenden.[10] Der Erwartungshorizont des Bankkunden ist somit nicht allein ausschlaggebend. Tatsächlich kann das Bankgeheimnis ohne Zustimmung und sogar wider die Interessen des Bankkunden aufgehoben werden, beispielsweise in Steuerangelegenheiten[11]. Das öffentliche **Interesse an einem international integrierten Finanzsystem** ("Level Playing Field")[12] kann dem Integritäts- und Persönlichkeitsschutzinteresse vorgehen. Diese jüngste gesetzgeberische Gewichtung fällt für das Strafverfolgungsinteresse des Staats in Bezug auf Art. 47 BankG stark ins Gewicht.

## B. Objektiver Tatbestand

### 1. Vorbemerkung

15 Art. 47 BankG stellt die Offenbarung des Bankgeheimnisses unter Strafe. "Offenbaren" ist dabei der zentrale Begriff der Strafregel, und im Rahmen des vorliegenden Rechtsgutachtens hat sich die Betrachtung auf diesen zu beschränken. Die weiteren Tatbestandsmerkmale – insb. der Geheimnisbegriff – sind in der Standardliteratur ausreichend beschrieben.

16 Es gibt soweit ersichtlich in der Schweiz keine Rechtsprechung, die den Begriff der Offenbarung im Zusammenhang mit Cloud Computing im Allgemeinen bzw. mit Cloud-Angeboten im Speziellen klarstellen oder auch nur behandeln würde. Es ist demnach zu untersuchen und zu schärfen, ob das Übertragen von Daten in die IT-Infrastrukturen eines Cloud-Anbieters eine Offenbarungshandlung im Sinne von Art. 47 BankG darstellt.

### 2. Zum Begriff der "Offenbarung" in Lehre und Rechtsprechung

17 Das Bundesgericht hat kürzlich entschieden, dass eine Offenbarung erst dann vorliegt, wenn der Aussenstehende die zu schützende Information tatsächlich wahrgenommen hat.[13] Dieses tatsächliche Wahrnehmen bezeichnen wir hier als Klartext-Zugriff[14]:

> *In dem von der Vorinstanz erwähnten BGE 142 IV 65 E. 5.1 hat das Bundesgericht erwogen, dass ein Geheimnis offenbart, wer es einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht. Es handelt sich hierbei um eine blosse Umschreibung des*

---

10 BBl 1970 I 1144 ff., 1161: "*Es muss hier gleich mit allem Nachdruck betont werden, dass das Bankgeheimnis nicht unbeschränkt gilt und keinen Deckmantel für Delikte darstellt. Artikel 47 des Bankengesetzes bestraft bloss die widerrechtliche Verletzung des Bankgeheimnisses*."

11 Seit 2017 werden bspw. Bankdaten automatisch zwischen Ländern erhoben und ausgetauscht, welche sich zur Anwendung des globalen Standards für den internationalen automatischen Informationsaustausch (AIA) verpflichtet haben. Dazu im Einzelnen hinten, Rz. 47.

12 BBl 2017 4913 ff., 4935.

13 BGer 6B_1403/2017 vom 8. August 2018, E. 1.2.2; SJZ 114/2018 S. 453.

14 Zum Begriff "Klartext-Zugriff" siehe auch die Begriffsdefinition im Anhang.

*strafbaren Verhaltens, woraus – entgegen der Meinung der Vorinstanz – nichts zum Zeitpunkt der Vollendung der Tat abgeleitet werden kann. Vielmehr ist in dieser Frage der Lehre zu folgen, wonach die Tat vollendet ist, sobald ein Aussenstehender dank dem Verhalten des Täters Kenntnis vom betreffenden Geheimnis erhält. Strafbarer Versuch wäre insbesondere dann anzunehmen, wenn der Täter Informationen für einen Dritten zugänglich gemacht hat, dieser aber vom Geheimnis noch keine Kenntnis genommen hat (DONATSCH/THOMMEN/WOHLERS, Strafrecht IV, 5. Aufl. 2017, S. 580 f.; siehe auch NIGGLI/HAGENSTEIN, in: Basler Kommentar, Strafrecht II, 3. Aufl. 2014, N. 36 zu Art. 162 StGB). Keiner der Mitarbeiter der B._____ Sagl nahm von den Zeichnungen, welche sich im Altpapier befanden, Kenntnis. Ein Schuldspruch wegen einer vollendeten Verletzung des Fabrikations- oder Geschäftsgeheimnisses ist damit von vornherein ausgeschlossen. Der angefochtene Entscheid ist bereits aus diesem Grund aufzuheben.*

18 Damit kann das Bankgeheimnis als **Erfolgsdelikt** qualifiziert werden. Offenbaren bedeutet damit "Zugänglichmachen" von Informationen, d.h. von Angaben, die per se sprechend[15] sind *und* konkret eingesehen werden[16]. Kommt es nicht zu Klartext-Zugriff, ist auch der objektive Tatbestand von Art. 47 BankG nicht erfüllt. Wenn es nicht zu Klartext-Zugriff kommt, ist der Grund dafür irrelevant (ob der Zugriff absolut unmöglich ist oder nachweislich nicht stattgefunden hat). Keine Offenbarung liegt zum Beispiel vor, wenn ein Unbefugter zwar vorübergehend physische Kontrolle über einen Datenträger hat, aber kein Hilfsmittel zur Verfügung hat, die auf dem Datenträger gespeicherten Angaben zu lesen.

19 Die Qualifikation als Erfolgsdelikt entspricht nicht der überwiegenden Lehre[17] und Rechtsprechung[18], ist aber gleichwohl richtig. Man muss, wie das Bundesgericht es festhält, die *Aktivitäten bzw. Tathandlungen*, die eine Offenbarung herbeiführen oder herbeiführen können, unterscheiden von deren Wirkung (sprich dem *Eintritt des Erfolgs*, respektive der *Offenbarung* als solcher[19]). Jedenfalls die moderne Welt macht diese Unterscheidung notwendig.[20]

---

15 Nicht "sprechend" sind Informationen, die verschlüsselt sind, anonymisiert sind oder zu deren Einsichtnahme es erst noch eines technischen Hilfsmittels bedarf.

16 Beispiel: Hält der Geheimnisträger ein mit einem Geheimnis beschriebenes Blatt Papier in 5m Abstand einem Unbefugten hin, findet keine Offenbarung statt, wenn der Unbefugte auf diese Distanz den Text nicht lesen kann; hat der Unbefugte aber ein Teleobjektiv vor den Augen, durch das er den Text lesen kann, findet eine Offenbarung statt.

17 Statt vieler: DAMIAN K. GRAF, Zu den Anwendungsgrenzen des schweizerischen Strafrechts bei Geschäftsgeheimnisverletzungen, SJZ 112 (2016) 19 ff., 197: *"Zunächst ist festzuhalten, dass es sich bei den Geheimnisverratsdelikten um schlichte Tätigkeitsdelikte handelt, ..."*, m.w.H.; ANDREAS DONATSCH, Strafrecht III, Delikte gegen den Einzelnen, 10. Ausgabe, Zürich 2013, S. 336; OLIVIER WENIGER, La protection des secrets économiques et du savoir-faire [Know-how], Diss. Lausanne, Geneva 1994, S. 256; GEORGES BINDSCHEDLER, Der strafrechtliche Schutz wirtschaftlicher Geheimnisse, Diss. Bern, Bern 1981, 57 ff. und 72; für die Qualifikation als Erfolgsdelikt im Kontext des anwaltlichen Berufsgeheimnisses: CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands (SAV), S. 13 ff.

18 BStGer SK.2017.52 vom 4. April 2018, E. 4.2.2.: "*Umstritten ist, ob die Tat erst mit der Kenntnisnahme durch den Geheimnisempfänger oder bereits mit der Übergabe oder der Einräumung der Möglichkeit der Kenntnisnahme des Geheimnisses an Dritte vollendet wird (vgl. auch Urteil des Bundesstrafgerichts SK. 2016.14 vom 16. Mai 2017 E. 2.2.2). Das Bundesgericht hat sich dazu bislang, soweit ersichtlich, nicht direkt geäussert.*"

19 Mindestens unklar: GIUSEPPE MUSCHIETTI, Wirtschaftlicher Nachrichtendienst – eine richterliche Perspektive, EIZ - Europa Institut Zürich Band/Nr. 157, Zürich 2015, 113 ff., 135 ff.: "*Die Straftat ist vollendet, sobald der Destinatär in der Lage ist, das Geheimnis - auch nur teilweise - zur Kenntnis zu nehmen.*"

20 Dazu MARC AMSTUTZ unter https://www.rechtimkontext.de/en/events/event/rechte-an-daten (besucht am 14.02.2019): "*Und was sind eigentlich Daten? Die meisten JuristInnen begreifen Daten von ihrem Inhalt (content) her, d.h. als Information. Sie denken semiotisch. Nur: die Digitalität kennt keine Semiotik. Sinnieren sie über Digitalität, tun sie das in den Kategorien der Hermeneutik. So wurden sie ausgebildet. Nur: die Digitalität kennt keine Hermeneutik. Verpassen sie die Idiosynkrasien der Digitalität? Lavieren bringt hier nichts: JA, vollends. Nicht einmal die Schlüsselfrage der Digitalität vermögen sie heuristisch zu fassen. Kein Wunder.*" Marc Amstutz schreibt dies als Einleitung zu einer Präsentation, die im Kontext zu seiner Forschung zum Eigentum an Informationen steht (MARC AMSTUTZ, Dateneigentum – Funktion und Form, AcP 218 [2018], 438 ff.). Dieselbe Diskrepanz diskutiert Amstutz auch in einem Artikel mit dem Titel "Dateneigentum – Eckstein der kommenden Digitalordnung", in Neue Zürcher Zeitung, September 2018, 10.

20 Zusätzlich muss – auf der Ebene der *Tathandlung*, die eine Offenbarung herbeiführt – weiter differenziert werden. Im Fokus von Lehre und Rechtsprechung stand in der Vergangenheit stets die *aktive Begehung* der Tat, etwa durch Folgendes:

- **Der Täter verschafft einem unbefugten Dritten direkten Klartext-Zugriff auf geschützte Informationen**. Beispiel: Unterrichtung eines Sachverständigen über Tatsachen in einem Rechtsstreit.[21] Soweit es zum Lesen oder zur Einsichtnahme noch eines technischen Vorgangs bedarf, stellt das blosse Zugänglichsein der Daten für "Aussenstehende" per se noch keinen Klartext-Zugriff unter diesem Spiegelstrich dar.[22]

- **Herbeiführen einer Situation, in der Aussenstehende Klartext-Zugriff auf geschützte Informationen erhalten können**.[23] Beispiel: Senden einer CD-ROM an einen Empfänger, der den Inhalt der CD lesen kann.[24] In diesem Szenario kann der Umstand, dass ein Unbefugter Zugriff auf Daten hat, welche die geschützten Informationen verkörpern, bereits sanktionierbar sein[25] (nach der hier vertretenen Meinung jedoch nur, wenn der Aussenseiter später die Daten "öffnet" und den Inhalt liest; dazu sogleich).

21 Auch das Bundesgericht räumt ein, dass in der zweiten Variante noch immer eine Bestrafung wegen Versuchs möglich ist (der Täter wird bestraft nach der Vorstellung, die er im subjektiven Tatbestand gebildet hat). Vorausgesetzt ist dabei Wissen und Wollen der handelnden Person in Bezug auf die Offenbarung (Art. 22 Abs. 1 StGB; fahrlässiger Versuch ist denkunmöglich). Solche Szenarien sind zwar vorstellbar, stehen aber nicht im Fokus des vorliegenden Rechtsgutachtens. Zu klären ist vielmehr, ob eine Bank sich so aufstellen kann, dass sie sich bei Nutzung von Cloud-Angeboten *gerade nicht strafbar macht*. Konkret: Was darf die Bank nicht ausser Acht lassen, um der Strafbarkeit zu entgehen? Es geht im Folgenden also ausschliesslich um Art. 47 BankG als *unechtes Unterlassungsdelikt, und zwar in der Form des Fahrlässigkeitsdelikts*.

## 3. Tatbegehung durch Unterlassung

22 Bank als Garantin: Art. 47 Abs. 1 BankG ist sowohl im Grundtatbestand (Vorsatzdelikt) als auch in Absatz 3 (Fahrlässigkeitsdelikt) als Vergehen ausgestaltet (Art. 10 Abs. 3 StGB) und kann demnach auch durch pflichtwidriges Untätigbleiben begangen werden (Art. 11 Abs. 1 StGB). Der Bankkunde vertraut der Bank im Rahmen der Geschäftsbeziehung Angaben über seine persönliche Situation an und vertraut darauf, dass die Bank diese Angaben durch angemessene Massnahmen schützt (Rz. 11). Die Pflicht zur Vornahme von Schutzmassnahmen ergibt sich aus Vertrag. Die

---

21 OGer ZH UE140317 vom 9. Juli 2015: *"Offenlegung von allfälligen Bankgeheimnissen gegenüber einem externen Privatgutachter [kann] tatbestandsmässig sein (...)".*

22 Ein solches Ereignis muss jedoch unter dem zweiten Aspekt der Regel überprüft werden ("Herbeiführen einer Situation, in der Aussenstehende Informationen über geschützte Informationen erhalten können").

23 WOLFGANG WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), digma Schriften zum Datenrecht, Band 9, Zürich 2016, S. 17 m.w.H.

24 OGer ZH SB110200 vom 19. August 2016: "*Durch den Versand der CD an die Steuerbehörden und die Zeitschrift "Cash" hat der Beschuldigte dieses Geheimnis offenbart*".

25 In Bezug auf Art. 321 StGB: BezGer Uster vom 20. März 1996 (ZR 96/1997, 289, 294); STEFAN TRECHSEL, Schweizerisches Strafgesetzbuch, Kurzkommentar, Zürich 1997, StGB 320 N 8.

Bank ist in dieser Hinsicht *Garantin* für den Schutz der Integritätsinteressen (Rz. 8) des Bankkunden.

23 Schutzpflichten: Speichert die Bank Daten in IT-Infrastrukturen von Dritten, ist dies nicht ohne Weiteres ein Vertragsbruch. Die Bank schuldet ausreichenden Perimeterschutz (dazu vorn, Rz. 5). Dies bedeutet, dass die Bank **ausreichende Schutzmassnahmen** vorkehren muss, die nach dem gewöhnlichen Lauf der Dinge (d.h. im Normalbetrieb) normalerweise verhindern, dass Unbefugte den Inhalt des Geheimnisses wahrnehmen, d.h. Klartext-Zugriff erhalten. Trifft die Bank solche Massnahmen, verhält sie sich aus der Optik des Bankkunden erwartungsgemäss (Rz. 5, Rz. 11). Unterlässt sie solche, verhält sie sich pflichtwidrig.

24 Tatmacht: Die Bank hat es in der Hand, solche Sicherungsmassnahmen durchzusetzen oder, bei Fehlen von solchen, auf die Nutzung der Cloud-Lösung zu verzichten (*Tatmacht*). Die Bank kann sich vom Cloud-Anbieter darüber aufklären lassen, wie dieser Daten schützt, welche die Bank in seine IT-Infrastrukturen migriert. Die Dokumentation muss das ganze Cloud-Angebot abdecken und in einer genügenden Tiefe beschreiben, wie der Cloud-Anbieter sich zum Schutz der von der Bank migrierten Daten einsetzt und sicherstellt, dass keine Offenbarungen erfolgen. Die Bank muss aufgrund der Dokumentation nachvollziehen können, ob die auf die fremden IT-Infrastrukturen migrierten Daten weiterhin angemessen geschützt bleiben. Die Dokumentation hat diesem zentralen Zweck zu dienen. Die Bank hat diese Dokumentation nicht selbst zu erstellen; der Cloud-Anbieter hat sie bereitzustellen. Mit anderen Worten hat es die Bank in der Hand, sich vor Vollzug der Datenmigration in die IT-Infrastrukturen des Cloud-Anbieters zu vergewissern, wie die transferierten Daten dannzumal geschützt sein werden. Sie kann übermässige Gefährdungen der Integritätsinteressen somit im Voraus erkennen und nötigenfalls vermeiden. Sie hat somit strafrechtlich relevante Tatmacht.

25 Hypothetische Kausalität: Die technischen Möglichkeiten der Cloud-Industrie sind heute weit vorangeschritten. Wie solcher Schutz aussehen kann, wird in Teil 2 beschrieben (Teil 2, Rz. 65 ff.). Auch wenn solche Schutzmassnahmen aus technischen Gründen eine theoretische Restmöglichkeit belassen, dass Dritte unbefugt Klartext-Zugriff auf die in die IT-Infrastrukturen des Cloud-Anbieters migrierten Daten nehmen, bedeutet dies nicht, dass im Normalbetrieb solche Zugriffe stattfinden. Je nach dem ausgewählten Cloud-Angebot lässt sich sogar zeigen, dass Klartext-Zugriff auf geheime Information im Normalbetrieb vollständig ausgeschlossen ist. Mit anderen Worten kann die Bank durch sorgfältige Auswahl der zum Einsatz gelangenden Cloud-Angebote steuern, welche Daten sie wie schützt. Unterlässt sie die ihr zur Verfügung stehenden Massnahmen und kommt es anschliessend zu einer verbotenen Offenbarung, stellt sich die Frage, ob die Offenbarung durch sorgfältige Abklärungen beim Cloud-Anbieter hätten vermieden werden können. Soweit dies zu bejahen ist, ist ihre Unterlassung im strafrechtlich relevanten Sinn hypothetisch kausal für die Offenbarung. Die Bank muss jedoch nicht einstehen für Ereignisse, die sie nicht mit genügender Sicherheit antizipieren kann. Entsprechend ist der Bank widerrechtlicher Zugriff von Dritten auf das Cloud-Angebot nicht anzulasten, wenn es mittels hochstehender Massnahmen gegen solche Zugriffe geschützt war. Ebensowenig fällt ein allfälliger Konkurs des Cloud-Anbieters unter Art. 47 BankG zu ihren Lasten, wenn es im Zuge der Konkursabwicklung zu gewissen Offenbarungen kommt, die nicht vermeidbar waren. Gleichermassen steht auch der Zugriff von Seiten einer bestimmten Behörde ausserhalb des Einflussbereichs der Bank. Diese Beispiele zeigen, dass die

Bank nur für das einstehen muss, was sie nach dem allgemeinen Lauf der Dinge, d.h. für den Normalbetrieb beim Cloud-Anbieter, erwarten musste.

26 Zumutbarkeit: Die von der Bank zu treffenden Massnahmen zum Schutz des Perimeters müssen der Bank *zumutbar* sein. In der Lehre wird kaum diskutiert, welches Niveau und welche Qualität Massnahmen erreichen müssen, damit sie als ausreichender Schutz vor Zugriffen von Aussenstehenden auf die geheime Information akzeptiert werden. Nicht zumutbar wäre es, von der Bank eine Garantie zu verlangen, dass Klartext-Zugriffe absolut ausgeschlossen sind. Art. 47 BankG wird nicht bereits deshalb verletzt, weil aus rein technischer Sicht noch eine theoretische Möglichkeit besteht, dass jemand anderes als die Bank auf das Geheimnis zugreifen kann – solange Massnahmen in Kraft sind, die unbefugte Dritte normalerweise daran hindern, Klartext-Zugriff auf die geheimzuhaltende Information zu nehmen. Eine solche Pflicht hätte die Bank auch nicht in Bezug auf Daten, die sie auf eigenen IT-Infrastrukturen gespeichert hält. Die eingesetzten Massnahmen müssen nur, aber immerhin dem *aktuellen Stand der Technik*[26] entsprechen. Soweit sich die Bank nicht dafür einsetzt, solche Massnahmen zu veranlassen, setzt sie sich bzw. ihre Organe oder die bestimmenden Angestellten einem strafrechtlich relevanten Risiko aus.

27 Fazit: *Die vorstehenden Ausführungen bedeuten, dass eine Bank (d.h. die für sie handelnden Personen), die für ausreichenden technischen und organisatorischen Schutz gegen unbefugte Zugriffe sorgt, sich nicht nach Art. 47 BankG strafbar macht*. Die Nutzung von solchen Cloud-Angeboten ist einer Bank nach Art. 47 BankG erlaubt. Unterlässt die Bank demgegenüber angemessene Massnahmen zum Schutz und tritt infolgedessen der Erfolg (Klartext-Zugriff, d.h. eine Offenbarung) ein, können die bestimmenden Personen strafbar werden – vorbehalten ist die Bestellung des Cloud-Anbieters als Beauftragter im Sinne von Art. 47 Abs. 1 BankG, was mit Zustimmung beider Parteien eine jederzeit zur Verfügung stehende Gestaltungsmöglichkeit darstellt (dazu Teil 1, Ziffer III, Rz. 31).

## C. Subjektiver Tatbestand

28 Das Bankgeheimnis kann vorsätzlich oder fahrlässig verletzt werden. Weder vorsätzliche noch fahrlässige Tatbegehung liegen vor, wenn die Organe der Bank zum Schluss kommen, dass die von ihnen gewählte technische IT-Infrastruktur wirksam gegen Offenbarungen an unbefugte Dritte schützt.

29 Keine IT-Infrastruktur schützt vollständig gegen unbefugte Zugriffe. Wenn Organen und Angestellten einer Bank bewusst ist, dass in geringem Umfang Restrisiken zu unbefugten Offenbarungen bestehen, machen sie sich keiner pflichtwidrigen Unsorgfalt schuldig, solange sie gegenüber dem Cloud-Anbieter für schützende Massnahmen gesorgt haben.

30 Die für die Bank handelnden Personen machen sich nur dann fahrlässig strafbar, wenn sie die von der Bank geschuldete Sorgfalt pflichtwidrig unterlassen. Auch hier ist entscheidend, mit welchen Massnahmen technischer und organisatorischer Art die Bank die geheim zu haltenden Angaben gegenüber Dritten sichert oder sichern lässt. Die Organe einer Bank, die es unterlässt, schützende Massnahmen einzurichten, verhalten sich pflichtwidrig, wenn die Bank die Vorsicht nicht beachtet,

---

26 Nur dieser ist relevant, siehe etwa MUSCHIETTI (Fn. 19) 113 ff., 137 ff.

zu der sie nach den Umständen und nach ihren persönlichen Verhältnissen verpflichtet ist (Art. 12 Abs. 3 StGB). Die Bank muss sich von den zum Einsatz kommenden Sicherheitsmassnahmen mittels aussagekräftiger Dokumentation überzeugen und wirksame Kontrollen vorsehen.

## III. Zur Funktion des "Beauftragten" nach Art. 47 Abs. 1 BankG

### A. Vorbemerkungen

31 Art. 47 BankG ist ein echtes Sonderdelikt, d.h. Täter sind nur die explizit und abschliessend aufgezählten Personengruppen, die der Risikosphäre der Bank zuzurechnen sind (z.B. Organe und Angestellte). Art. 47 BankG nennt seit dem Jahr 1971 ausdrücklich auch Beauftragte; damit sollte den Banken das Outsourcing im betriebswirtschaftlich sinnvollen Rahmen ermöglicht werden.[27] Die Materialien stellen klar, dass mit der damaligen Änderung insbesondere Anbieter von Rechenzentrumsleistungen für Banken der Strafbarkeit unterstellt werden sollten.[28] Da auch Beauftragte zum Kreis der strafbaren Personen gehören, gilt die "Preisgabe von Kundenbeziehungen an Beauftragte"[29] durch die Bank als erlaubt.[30] Ist der Beauftragte eine juristische Person, können die für den Beauftragten handelnden Personen zumeist gemäss Art. 47 Abs. 1 lit. c BankG ins Recht gefasst werden.

32 Cloud-Anbieter setzen für ihre Leistungen ebenfalls IT-Infrastrukturen wie Rechenzentren ein und kommen als Beauftragte ohne Weiteres in Frage. Durch Auslegung ist im Folgenden zu bestimmen, ob Cloud-Anbieter "Beauftragte" im Sinne von Art. 47 Abs. 1 lit. a BankG sein können.

### B. Cloud-Anbieter als Beauftragte im Allgemeinen

#### 1. Auslegung nach dem Wortlaut und nach der Gesetzgebungshistorie

33 Der Beauftragtenbegriff ist vom Gesetzgeber bewusst offen gehalten worden. Insbesondere die historische Auslegung zeigt, dass der Begriff "Auftrag" bzw. "Beauftragter" keine besondere gesetzgeberische Wertung enthält, zumal auch die Anbieter von reinen Rechenzentrumsleistungen explizit erfasst sein sollten (dazu vorn, Rz. 31). Der Gesetzgeber wollte ermöglichen, dass in einer zunehmend arbeitsteiligen Welt externe Dritte der Risikosphäre der Bank zugerechnet werden können, obwohl diese Stellung für den Bankkunden nicht unbedingt im Voraus erkennbar war. Die

---

27 BSK BankG-STRATENWERTH, Art. 47 N 7: "*Das wird man dahin verallgemeinern dürfen, dass die Bank Dritte jedenfalls dann in den Kreis der Geheimnisträger einbeziehen darf, wenn dies einem ernstzunehmenden Interesse an der Optimierung ihrer Leistungen oder an der Senkung ihrer Kosten entspricht. Die in solchem Rahmen erfolgende Weitergabe personenbezogener Daten dürfte in aller Regel auch im wohlverstandenen Interesse des Bankkunden liegen, um dessen Schutz es geht.*"

28 BBl 1970 I 1144 ff., 1182: *"Mit der Unterstellung des Beauftragten sollen insbesondere auch Rechenzentren erfasst werden, die von Banken mit der elektronischen Datenverarbeitung betraut werden."*

29 BEAT KLEINER/RENATE SCHWOB/CHRISTOPH WINZELER, in: Zobl/Schwob/Geiger/Winzeler/Kaufmann/Weber/Kramer (Hrsg.), Kommentar zum Bundesgesetz über die Banken und Sparkassen, 23. Auflage, Zürich etc. 2015, Art. 47 N 369: "*Die Preisgabe von Kundenbeziehungen an Beauftragte ist somit i.S.v. Art. 32 StGB grundsätzlich erlaubt. Die Erläuterung in der Botschaft ("insbesondere") lässt erkennen, dass der Wortlaut von Art. 47 Abs. 1 BankG insoweit für Entwicklungen der Zukunft nicht nur offen gehalten, sondern auch mit Absicht so formuliert wurde.*"

30 BEAT KLEINER/RENATE SCHWOB, in: Bodmer/Kleiner/Lutz (Hrsg.), Kommentar zum schweizerischen Bankengesetz, Zürich 1996, BankG 47 N 102; URS ZULAUF, Bankgeheimnis und historische Forschung, ZSR 113 I (1994), 115; PETER HONEGGER/THOMAS A. FRICK, Das Bankgeheimnis im Konzern und bei Übernahmen, SZW 1996 6.

Nähe eines Cloud-Anbieters zu einem Anbieter von Rechenzentrumsleistungen ist augenfällig, bietet ein Cloud-Anbieter doch IT-Infrastrukturen zur Nutzung an. Wortlaut und Historie sind klar: Cloud-Anbieter können nach der wortlautgetreuen Auslegung unter den Beauftragtenbegriff subsumiert werden. Dieses Auslegungsresultat erscheint auch heute noch zeitgemäss und bedarf keiner Korrektur.

### 2. Systematische Auslegung

34 Die Tathandlung nach Art. 47 BankG liegt im Offenbaren von an sich geheimzuhaltenden Informationen (dazu vorn, Rz. 17 ff.). Es liegt auf der Hand, dass innerhalb der Bank viele Personen arbeiten, die im Einzelfall Zugriff auf kundenbezogene Daten haben und in diesem Rahmen den gespeicherten Bedeutungsgehalt dessen, was die Daten ausdrücken, wahrnehmen können (Klartextzugriff). Die Geheimhaltungspflicht erfasst alle in einer Bank oder für sie vertraglich tätigen Personen.[31] Andere Strafnormen zum Schutz von Geheimnissen im schweizerischen Recht mit derselben Stossrichtung operieren mit dem Begriff der "Hilfsperson". Auch wenn das BankG andere Begrifflichkeiten wählt ("Angestellter" sowie "Beauftragter"), geht es im Kern doch darum, die von der Bank im Rahmen des Üblichen beigezogenen Hilfskräfte der Strafbarkeit zu unterstellen. Gleich wie der Hilfspersonenbegriff im schweizerischen Berufsgeheimnisschutz (Art. 321 StGB) beruht auch die Definition der strafbaren Personen in Art. 47 BankG auf einem funktionalen Verständnis. Strafbar soll sein, wer im Rahmen des heute Üblichen, des sozial Akzeptierten und des vom Bankkunden auch Erwartbaren (Rz. 11) in oder mit einer Bank arbeitet und in diesem Rahmen an der Banktätigkeit in einer Weise mitwirkt, dass er grundsätzlich von geschützten Geheimnissen Kenntnis erhalten kann.

35 Auf dieser Basis kann die Bank eine geheimnisrelevante Tätigkeit an jene übertragen, die ebenfalls derselben Strafdrohung unterstehen (vorn, Rz. 31). Die Geheimnisschutzrechte, die den Hilfspersonenbegriff oder den Begriff des Beauftragten kennen, sind grundsätzlich darauf ausgelegt, eine betriebswirtschaftlich sinnvolle arbeitsteilige Organisation der Arbeit zu ermöglichen. Sachlich begründete Formen der Arbeitsteilung entsprechen dem im schweizerischen Recht inhärenten Regelungsziel[32] der Geheimnisdeliktstatbestände ebenso wie sonstige Regeln im schweizerischen Recht (Art. 101 OR, Art. 398 Abs. 3 und Art. 399 Abs. 1 OR).

### 3. Teleologische Auslegung

36 Die teleologische Auslegung geht über die historische nicht wesentlich hinaus: Der Gesetzgeber wollte den Banken ermöglichen, in sachlich begründeten Fällen externe Anbieter zur Befriedigung von IT-Bedürfnissen beizuziehen. Auch mit Blick auf das teleologische Element können Cloud-Anbieter als Beauftragte bestellt werden.

---

31 KLEINER/SCHWOB/WINZELER (Fn. 29) Art. 47 N 360.

32 Auch das Amtsgeheimnis, dem bislang eine Hilfspersonenklausel fehlte, soll im Rahmen der Gesetzgebungsarbeiten zum Informationsschutzgesetz um eine Hilfspersonenklausel ergänzt werden, siehe BBl 2017 2953 ff., 3077 f.

## 4. Weitere Überlegungen zur Auslegung: funktionaler Hilfspersonenbegriff und Zusammenhang zur impliziten Einwilligung des Bankkunden

37 Wer die Bank in ihrem regulierten geschäftlichen Wirkungskreis und unmittelbar unterstützt, ist ihr *bei funktionaler Betrachtung* unter Umständen gleichzustellen. Wenn diese Gleichstellung möglich ist, *offenbart* der Geheimnisträger in der Bank kein Geheimnis, wenn er die geheime Information mit einem anderen Mitarbeitenden, einem Organ oder einem Beauftragten teilt. Bei funktionaler Betrachtung werden alle im Straftatbestand genannten Personen Angehörige derselben Risikosphäre[33] (nämlich jener der Bank, der sie zugehörig sind oder für die sie als Beauftragte Leistungen erbringen). Innerhalb dieser Risikosphäre müssen sich alle, die arbeitsteilig zusammenwirken, vertrauen können.[34] Dieses Nebeneinander von Haupt-Geheimnisträgern ist in der arbeitsteiligen Wirtschaft nicht nur notwendig, sondern auch sozial akzeptiert (siehe Rz. 5 f. und Rz. 13).

38 Man kann im Umfang, in dem ein solches Nebeneinander von Geheimnisträgern dem Erwarteten entspricht, jeweils auch von einer impliziten Einwilligung des Bankkunden ausgehen (Rz. 13).[35] Die implizite Einwilligung des Bankkunden kann stillschweigend erteilt worden sein oder als offensichtlich mitumfasst von der Bank vorausgesetzt und angenommen werden. So oder so misst sich der Umfang der Einwilligung am Erwartungshorizont des Bankkunden. Eine solche Einwilligung deckt Verhaltensweisen, die der Bankkunde erwarten konnte und musste.

## 5. Fazit: Cloud-Anbieter können als Beauftragte im Sinne von Art. 47 Abs. 1 lit. a BankG bestellt werden

39 Die Auslegung mittels verschiedener Auslegungsmethoden führt zum Resultat, dass Cloud-Anbieter als Beauftragte im Sinne von Art. 47 Abs. 1 lit. a BankG bestellt werden können. Das bedeutet, dass die Bank mit einem Cloud-Anbieter auch geheimnisgeschützte Informationen im Klartext austauschen darf, wenn sie ihn korrekt als Beauftragten bestellt. Dieses Resultat kann als Privilegierung des Informationsaustausches zwischen Bank und Cloud-Anbieter bezeichnet werden.

---

33 Es kommt zu einer Ausdehnung des personellen Perimeters auf den Beauftragten (dazu Rz. 5).

34 CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands (SAV), 1. November 2018, S. 21.

35 Für das Patientenrecht ausdrücklich: BezGer ZH GG150233 vom 18. November 2015, E. II.2.5.3.

## C. Bestellung von Beauftragten mit Auslandsbezug

### 1. Einleitung mit Problemstellung

40 Die bisher wohl vorherrschende Lehre[36] ist der Ansicht, dass die privilegierende Wirkung (siehe Rz. 39) in Bezug auf einen Cloud-Anbieter mit Auslandsbezug nicht gilt.[37] Wie es sich damit verhält, ist im Folgenden zu klären.

41 Die Diskussion ist zu führen vor dem Hintergrund, dass die beigezogenen Personen, die entgegen den Weisungen der Bank eine relevante Offenbarung vornehmen, im Ausland verfolgt werden müssten. Art. 47 BankG ist zwar mit der neusten bundesgerichtlichen Rechtsprechung als Erfolgsdelikt zu qualifizieren. Gleichwohl herrscht aber wenig Einigkeit in der Lehre, ob die Auslandstat in jedem Fall nach schweizerischem Recht strafbar ist. Massgeblich ist Art. 8 Abs. 1 StGB.[38] So oder so: Wenn sich der im Ausland handelnde Täter nicht freiwillig in die Schweiz begibt bzw. die Auslieferung durch den ausländischen Staat scheitert, müsste zudem auf die Strafverfolgung im Ausland zurückgegriffen werden. Womöglich ist die Offenbarung dort aber nicht strafbar oder der Täter kann aufgrund der konkreten Umstände im Ausland damit rechnen, dass es zu keiner Bestrafung im Ausland kommen wird.[39] Diese summarischen Ausführungen zeigen bereits, dass der strafrechtliche Schutz der diesen Personen offengelegten Bankkundengeheimnisse unter Umständen also reduziert wird oder womöglich ganz entfällt.

42 Es geht somit im Folgenden um die juristische Bewertung, ob trotz des reduzierten oder entfallenden strafrechtlichen Schutzes noch immer von genügender Kontrolle der Bank über den Cloud-Anbieter gesprochen werden kann. Wenn eine genügende Kontrolle bejaht wird, darf konsequenterweise auch die privilegierende Wirkung (dazu Rz. 39) nicht entfallen.

43 Nun, diese Argumentation wäre schon seit dem Jahr 1971 möglich gewesen. Und dennoch hat in der Praxis soweit ersichtlich noch keine Bank darauf abgestellt, mit dieser Begründung bankgeheimnisrelevante Daten beispielsweise in ein Rechenzentrum in Indien zu migrieren. Lohnt es sich

---

36 KLEINER/SCHWOB/WINZELER (Fn. 29), BankG 47 N 371: "*Da im Ausland domizilierte Beauftragte trotz theoretischer Strafbarkeit dem Arm der schweizerischen Strafbehörden praktisch entzogen sind ("Over the border means out of control"), darf die Bank Aufträge, die zur Preisgabe von Kundenbeziehungen führen, nur dann ins Ausland erteilen, wenn dafür gewichtige Gründe sprechen wie z.B. beim Anschluss an ein internationales Zahlungssystem.*"; gl.M.: DAVID SCHWANINGER / STEPHANIE S. LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11. März 2013, N 31; URSULA WIDMER, Kurzgutachten für die Schweizerische Informatikkonferenz SIK betreffend die Nutzung von Cloud Services mit Rechtswahl von irischem Recht und Gerichtsstand Dublin durch die schweizerische öffentliche Verwaltung, 2012, 7.

37 Anders: SCHWARZENEGGER/THOUVENIN/STILLER, (Fn. 34) S. 21, Fn. 50, mit Verweis auf BezGer ZH GG150233 vom 18. November 2015, E. II.2.5.3. für das Arztgeheimnis nach Art. 321 StGB: Bei einem durch eine kleine Arztpraxis ohne Sekretariat beigezogenen auswärtigen Schreibbüro handle es sich um eine Hilfsperson, ***woran auch der Umstand nichts ändere, dass das Schreibbüro seine Arbeiten nicht in der Schweiz, sondern in Deutschland verrichtete.***

38 Siehe ausführlich zum Strafanwendungsrecht bei digitalen Offenbarungshandlungen DAMIAN K. GRAF, Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext, SJZ 112/2016, 193; SCHWARZENEGGER/THOUVENIN/STILLER, (Fn. 34) S. 35 f.;

39 Siehe z.B. GRAF (Fn. 17) 19 ff.: "*Angesichts des wenig verbreiteten Schutzes von Bankkundeninformationen im Ausland steht die Voraussetzung der Reziprozität einer Verfolgung und Verurteilung wegen der Verletzung von Art. 47 BankG regelmässig entgegen.*"*;* mit Verweis auf: JÖRG SCHWARZ, in: Jürg-Beat Ackermann/Günter Heine, Wirtschaftsstrafrecht der Schweiz, 2013, §19 N 112.

also, den seit 1971 unveränderten Wortlaut von Art. 47 BankG und seine Rezeption über die vergangenen 50 Jahre hinweg zu hinterfragen? Die Antwort lautet ja. Zwar hat sich nicht die Gesetzesbestimmung geändert, aber das Umfeld.

## 2. Auslegung von Art. 47 Abs. 1 lit. a BankG

### a) Auslegung nach dem Wortlaut

44 Der Wortlaut von Art. 47 BankG unterscheidet nicht zwischen in- oder ausländischen Angestellten, Organen oder Beauftragten etc. einer Bank. Nach grammatikalischer Auslegung muss der Beauftragte mit Auslandsbezug gleich behandelt werden wie der schweizerische Beauftragte.[40] Ein anderes Resultat würde gegen Art. 1 StGB ("nulla poena sine lege") verstossen.

### b) Auslegung nach der Gesetzgebungshistorie

45 Als die Figur des Beauftragten 1971 in Art. 47 BankG eingeführt wurde, wurde die Frage des Auslandsbezugs im Zusammenhang mit Beauftragten (oder Rechenzentrumsdienstleistungen) nicht besonders erörtert. Im Rahmen der Gesetzgebung im Jahr 1934 war es das erklärte Ziel der Gesetzgebung zum Bankgeheimnis, dass es Daten auch vor dem Zugriff anderer Staaten schützen wollte. Der Bundesrat hat zur Stossrichtung dieser Bestimmung in seiner Botschaft zur Revision des Bankgesetzes (1970) Folgendes festgehalten[41]:

> *1934 hat der schweizerische Gesetzgeber es für notwendig gehalten, die privatrechtliche Pflicht des Bankiers zur Verschwiegenheit durch eine Strafandrohung in Artikel 47 des Bankengesetzes zu verstärken. Bei den Beratungen über diese Bestimmung wurde erwähnt, dass sie sich nicht nur gegen die eigentlichen Verletzer des Bankgeheimnisses, sondern auch gegen "ausländische Spionage" richte. Es ging in der Tat darum, wirksam gegen die mannigfachen Versuche der totalitären Regime jener Zeit anzukämpfen, ihre Devisengesetzgebung, die oft auf Enteignung hinauslief, in der Schweiz zur Anwendung zu bringen und die Hand auf das in unsern Banken deponierte Vermögen der aus politischen oder rassischen Gründen verfolgten Personen zu legen. Der schweizerische Gesetzgeber wollte daher den Schutz der Persönlichkeit gegen Massnahmen verstärken, die unsere öffentliche Ordnung verletzen. Bankmoral und Bankrecht, wie die Schweizer sie für sich selbst entwickelt hatten, sollten auch für die Ausländer gelten.*

46 Die historische Betrachtung des gesetzgeberischen Willens indiziert somit zunächst anders als der Wortlaut eine unterschiedliche Behandlung von Beauftragten mit Auslandsbezug. Seither wurde das BankG mehrfach revidiert und gerade in jüngster Zeit dem öffentlichen Interesse an einem international integrierten Finanzplatz angepasst. Diese geltungszeitliche Auslegung ist im Rahmen der systematischen Betrachtung zu vertiefen. Sie führt dazu, dass der gesetzgeberische Wille vor 80 Jahren aus heutiger Warte verblasst.

### c) Systematische Auslegung

47 Die Schweiz hat sich durch die neuste Gesetzgebung von den Überlegungen des Gesetzgebers aus dem Jahr 1934 erheblich distanziert:

---

40 ADRIAN ANDERMATT, Die Konzerninterne Bekanntgabe von geschützten Bankkundendaten ins Ausland - Eine strafrechtlich relevante Offenbarung im Sinne von Art. 47 BankG?, GesKR 2007, 405, 409.

41 BBl 1970 I 1144 ff., 1161.

48 Durch Beteiligung namentlich am globalen Standard über den automatischen Informationsaustausch über Finanzkonten (AIA) melden schweizerische Banken den schweizerischen Behörden seit 2017 relativ detaillierte Informationen über ausländische Bankkunden, damit diese Informationen von der Schweiz anschliessend ins Ausland übermittelt werden können. Die Schweiz will sich damit den internationalen Finanzmarkt offenhalten ("Level Playing Field", Rz. 14). Der Bundesrat hat im Rahmen von mehreren Iterationen von 2015 – 2018 die Grundlagen hierfür dem Parlament zur Beratung vorgelegt. Seit 2017 ist das erste AIA-Gesetz in Kraft. Die Schweiz tauscht seit 2018 unter dem AIA Informationen über Finanzkonten mit Partnerstaaten aus.

49 Mit den USA hat die Schweiz einen Staatsvertrag abgeschlossen, um die Umsetzung von FATCA ("US Foreign Account Tax Compliance Act") zu erleichtern und ein entsprechendes Schweizer FATCA-Gesetz wurde erlassen. Im Rahmen des FATCA-Abkommens melden Schweizer Banken Konteninformationen mit Zustimmung der betroffenen Kunden direkt den US-Steuerbehörden. Wenn keine Zustimmung erteilt wurde, erfolgt stattdessen eine anonyme, aggregierte Meldung gewisser Kontoinformationen. Auf dieser Grundlage können US-Steuerbehörden dann die Offenlegung bestimmter Kunden- und Kontoinformationen verlangen, sofern dies im Doppelbesteuerungsabkommen zwischen den USA und der Schweiz vorgesehen ist.

50 Diese jüngsten Entwicklungen relativieren die Bedeutung der historischen gesetzgeberischen Absicht deutlich. Im Rahmen eines Systems wie des AIA werden die von Banken standardisiert zu meldenden Angaben über Bankkunden *voraussetzungslos* und in der *gesamten Breite* an ausländische Staaten übermittelt, was in mehrfacher Hinsicht von Bedeutung ist für die hier zu beurteilende Frage, ob ein Beauftragter mit Auslandsbezug von einer schweizerischen Bank ausgewählt werden darf: Das noch 1934 vom Gesetzgeber verfolgte Schutzinteresse ist jedenfalls durch den AIA übersteuert worden, gibt es doch für einen ausländischen Staat, der sich am AIA beteiligt, kein Bedürfnis mehr, über den Umweg des Beauftragten (und nach Durchlaufen von grundsätzlich restriktiven Verfahren) auf dieselbe Information zugreifen zu können. Sollten für den ausländischen Staat weitere als die im Rahmen des AIA ausgetauschten Informationen von Bedeutung werden, könnte sich der ausländische Staat direkt an den Beauftragten wenden, um über Strafverfolgungsbehörden auf solche weitere Information zu greifen. Das Bankgeheimnis schützt aber auch in der Schweiz nicht vor Zugriffen der Strafverfolgungsbehörden, die Straftaten einer gewissen Intensität verfolgen. Die Schweiz würde dem ausländischen Staat für solche weitergehenden Untersuchungen auch jederzeit Rechtshilfe leisten. Würden Mitarbeitende des Beauftragten das Geheimnis brechen, könnten sie im Ausland (abhängig von der dortigen Gesetzgebung) nach dem dortigen Recht verfolgt werden; je nach Auffassung kann die Auslandstat auch in der Schweiz verfolgt werden.[42]

51 Diese Überlegungen sind gerade für die Würdigung von Art. 47 BankG als Strafnorm von erheblicher Bedeutung. Art. 47 BankG stellt eine gesetzliche Verstärkung des vertraglichen Geheimnisschutzes dar (Rz. 9). Art. 47 BankG ist ein Offizialdelikt, darin kommt der Strafverfolgungsanspruch des Staats zum Ausdruck. Es wäre widersprüchlich, wenn derselbe Staat, der im Rahmen des AIA voraussetzungslos und im vollen Querschnitt über die gesamte Bankenlandschaft (bzw. deren Kunden) Daten ans Ausland übermittelt, Datenübermittlungen in sachlich viel engerem Umfang, die

---

42 Siehe vorne Rz. 41 m.w.H.

restriktiv auf technisch gesicherte IT-Infrastrukturen gespeichert werden, der Strafbarkeit unterstellen würde (ohne dies im objektiven Tatbestand konkret zum Ausdruck zu bringen). Im Resultat führen diese Entwicklungen dazu, dass das subjektiv-historische Auslegungselement (Rz. 46) für das Auslegungsresultat nicht mehr bestimmend sein kann.

52 Im Rahmen der systematischen Auslegung ist auch anzumerken, dass jüngst auch für den Bereich des Anwaltsgeheimnisses die Meinung vertreten wurde, dass Hilfspersonen im Ausland rechtmässig in die Risikosphäre des Anwalts eingebunden werden könnten und dass es keine Verletzung des Anwaltsgeheimnisses darstelle, wenn diesen ausländischen Hilfspersonen Klartext-Zugriff auf geheimnisbewehrte Information gegeben werde.[43]

### d) Teleologische Auslegung

53 Für die teleologische Auslegung kann auf die Ausführungen in Rz. 36 verwiesen werden. Art. 47 BankG soll es einer Bank ermöglichen, sich in der arbeitsteiligen Wirtschaft so aufzustellen, wie dies aus sachlichen Gründen erforderlich ist. Zu diesem Zweck soll die Bank Dienstleistende in ihre Risikosphäre einbinden können. Da der Markt für Cloud-Angebote heutzutage international geprägt ist, führt das teleologische Argument in konsequenter Weiterführung dazu, den Beizug von ausländischen Beauftragten eher zuzulassen.

54 Klar ist jedenfalls, dass Art. 47 BankG keine Bestimmung zum Schutz von inländischen Cloud-Anbietern sein soll. Dazu wäre die Regelung als Strafnorm nicht geeignet, eine entsprechende Konnotation müsste im Rahmen der Auslegung verworfen werden.

### e) Fazit

55 Die Würdigung der vorstehenden Auslegungselemente ergibt eine doch deutliche Tendenz zum Schluss, dass Banken auch Dienstleistende mit Auslandsbezug als Beauftragte im Sinne von Art. 47 BankG bestellen können.

---

43 SCHWARZENEGGER/THOUVENIN/STILLER, (Fn. 34), S. 21, 27f.

## TEIL 2 UMSETZUNG ANGEMESSENER SCHUTZMASSNAHMEN

### I. Ableitungen aus den Überlegungen zum objektiven und subjektiven Tatbestand

### A. Vorbemerkungen

56 Die Überlegungen zum objektiven und subjektiven Tatbestand (dazu vorn, Rz. 15 ff.) haben gezeigt, dass Art. 47 BankG als unechtes Unterlassungsdelikt bei fahrlässiger Tatbegehung zu prüfen ist (Rz. 22). Sowohl unter dem Aspekt der Garantenstellung als auch unter jenem der Fahrlässigkeit ist die Bank in der Pflicht, bei Auswahl des Cloud-Anbieters Sorgfalt walten zu lassen, voraussehbare Risiken zu antizipieren und sich vom Cloud-Anbieter aufzeigen zu lassen, mit welchen konkreten Massnahmen Bankkundendaten gegen Zugriff von unbefugten Dritten geschützt sind. Wenn die Bank dann nach sorgfältiger Prüfung zum Schluss gelangt, dass die ihr gegenüber dokumentierten Massnahmen nach dem voraussehbaren Lauf der Dinge im Normalbetrieb dazu führen, dass keine Offenbarungen stattfinden (auch nicht gegenüber Mitarbeitenden des Cloud-Anbieters), oder wenn sie den Cloud-Anbieter auf dieser Basis vertraglich als Beauftragten in ihre Risikosphäre einbindet (womit Klartext-Zugriffe auch durch Mitarbeitende des Cloud-Anbieters zulässig werden), verletzt die Bank weder ihre Garantenstellung noch können die Organe bzw. Angestellten der Bank wegen fahrlässiger Tatbegehung bestraft werden.

57 Die Bank, die für einen angemessenen technischen und organisatorischen Schutz sorgt, der nach dem gewöhnlichen Lauf der Dinge normalerweise verhindert, dass unbefugte Dritte das Geheimnis zur Kenntnis nehmen, kann das Bankgeheimnis dann aus wertender Sicht bereits im objektiven Tatbestand nicht verletzen. **Angemessener Schutz** bedeutet, dass **ausreichende Vorkehrungen** gegen den Zugriff durch Unbefugte wirksam getroffen werden müssen. Solche Vorkehrungen sind dann ausreichend, wenn sie im Rahmen des Normalbetriebs (gewöhnlicher Lauf der Dinge) normalerweise verhindern, dass Unberechtigte den Inhalt des Geheimnisses wahrnehmen ("Klartext-Zugriff").

58 Die Bank muss verstehen, inwiefern sie über die auf die fremden IT-Infrastrukturen migrierten Daten mittels dokumentierter Massnahmen die Kontrolle behält (Pflicht, den eigenen Perimeter zu schützen, Rz. 5); denn kontrollieren kann die Bank nur, was sie auch versteht.

59 Wenn die Bank so vorgeht, kann sie dokumentieren, dass sie ihrer *vertraglich begründeten Garantenstellung gerecht geworden* ist und *nicht fahrlässig* handelt.

60 Die Bank muss sowohl im Beschaffungsprozess als auch im laufenden Betrieb dafür sorgen, dass sie interne Strukturen und internes Personal bereithält, das den Austausch mit dem Cloud-Anbieter unter Kontrolle behält. Das kann bedeuten, dass internes Personal neue Aufgabenfelder besetzen muss und auf die dafür erforderlichen Kompetenzen umzuschulen ist ("Skill Shift").

### B. Ableitungen aus den Überlegungen zur Beauftragtenstellung

61 Das Gesetz äussert sich nicht konkret dazu, wie ein Beauftragter die Stellung eines solchen erwirbt – ob diese Stellung dem Beauftragten mit Abschluss des Vertrags von Gesetzes wegen zukommt oder ob die Bank ihn mittels Vertrags in ihre Risikosphäre einbinden muss. Unseres Erachtens ist

Letzteres der Fall. Gerade die Nähe des funktionalen Hilfspersonenbegriffs zur impliziten Einwilligung (Rz. 37 f.) zeigt deutlich, dass es nicht vollständig im Ermessen der Bank liegt, wie sie Dritte beizieht. Die Bank kann die Privilegierung (Rz. 39) nur erwirken, wenn sie den Cloud-Anbieter inhaltlich korrekt zum Beauftragten macht. Zudem dient eine formelle Bestellung des Beauftragten mittels Vertrags der Rechtssicherheit: Jeder soll grundsätzlich erkennen können, ob er einer Strafsanktion unterliegen könnte (oder ob er im Fall einer Geheimnisverletzung nur Ersatz für Schaden bzw. vertragliche Konventionalstrafen zu bezahlen hat).

62 Insbesondere sind die folgenden Leitlinien von Bedeutung und die Bank muss diese einhalten:

- Abgrenzung der Risikosphären: Den Geheimnisträger (d.h. die Bank) trifft ganz direkt die Pflicht, sich dafür einzusetzen, dass das Geheimnis nicht offenbart wird. Jede Disposition, welche das Geheimnis einer Gefährdung aussetzt, muss den Geheimnisträger zu schützenden Massnahmen veranlassen. Wenn die Bank so vorgeht, verhält sie sich aus der Warte des Bankkunden erwartungsgemäss. Es ist rechtmässig, innerhalb der eigenen Risikosphäre anderen Personen zu vertrauen[44], wozu auch Beauftragte gehören. Dazu muss die Risikosphäre aber definiert sein, was entsprechend klare Verträge erfordert.

- Ohne vertragliche Einbindung geht es nicht: Ein Vertrag, der Dritten genügende technische und organisatorische Massnahmen auferlegt sowie im Interesse der Durchsetzbarkeit über schützende vertragliche Instrumente verfügt, ist auf jeden Fall erforderlich.

- Berücksichtigung der betroffenen Informationen: Besonders heikle Informationen wird die Bank besser schützen müssen als andere. Bei besonders sensiblen Informationen ist der Kreis der einbezogenen Personen enger zu fassen als bei anderen Informationen.[45]

63 Aus der hier vertretenen Auffassung ergibt sich somit, dass nicht nur rein formale Kriterien[46], sondern vielmehr inhaltliche und funktionale Kriterien darüber entscheiden, ob ein Beauftragter rechtmässig als solcher bestellt wurde. Es würde nicht genügen, wenn die Bank den Beauftragten rein formal "der Strafbarkeit des Art. 47 BankG" unterstellt. Die Bank muss durch die getroffenen Massnahmen einen dem Bedürfnis entsprechenden Schutz umgesetzt sehen. Das bedingt auch auf Seiten der Bank ein tiefgreifendes Verständnis über die (vom Cloud-Anbieter zuzusichernden) Abläufe beim Cloud-Anbieter; denn kontrollieren kann nur, wer auch versteht, wie die Informationsverarbeitung beim Cloud-Anbieter aussehen wird. Der Cloud-Anbieter muss die Bank zu diesen Zwecken angemessen dokumentieren.

64 Wenn die Bank den Cloud-Anbieter auf diese Weise formell bestellt, können auf Seiten des Cloud-Anbieters Klartext-Zugriffe vorkommen, ohne dass eine Strafbarkeit der Bank bzw. ihrer Organe

---

44 SCHWARZENEGGER/THOUVENIN/STILLER, (Fn. 34) S. 21.

45 DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, OR 328b N 57.

46 Zu Recht insofern das OGer ZH UE140317 vom 9. Juli 2015 i.S., E 6: "*Allein die Tatsache, dass eine Person zur Bank ein Auftragsverhältnis unterhält, kann nicht genügen, um die Bank zur Weitergabe von Geheimnissen zu ermächtigen (vgl. Stratenwerth, a.a.O., N. 7 zu Art. 47 BankG)*.".

und Angestellten resultiert. Die Bank hat dann ihre vorn unter Rz. 22 ff. diskutierten Sorgfaltspflichten erfüllt.

## C. Szenarien ohne Klartext-Zugriff

### 1. Vorbemerkungen

65 Solange der Cloud-Anbieter nicht formell als Beauftragter eingebunden ist, gelten auch der Cloud-Anbieter und seine Mitarbeitenden als Unberechtigte. Dies hat jedoch, wie sogleich zu zeigen sein wird, nicht zwingend zur Folge, dass die Bank Cloud-Angebote nicht nutzen könnte. Cloud-Angebote, die mittels technischer und organisatorischer Massnahmen Offenbarungssituationen faktisch verhindern, stehen der Bank zur Nutzung frei. Insofern unterscheidet sich auch das unter dieser Ziffer I.C dargestellte Szenario nicht wesentlich von den sonstigen Resultaten unter diesem Teil 2.

66 Wenn Bankkundendaten auch auf den IT-Infrastrukturen des Cloud-Anbieters angemessen **gegen Zugriffe unbefugter Dritter** geschützt sind, findet keine strafrechtlich relevante Offenbarung statt. Aus wertender Sicht liegt keine Offenbarung vor, wenn die Bank als Geheimnisträgerin für Schutzmassnahmen sorgt, die dem aktuellen Stand der Technik entsprechen. Was dies im Kontext von Cloud-Angeboten bedeutet, ist im Folgenden darzustellen. Dabei ist auf Nutzungsszenarien einzugehen und darzulegen, inwiefern allfällige Variationen im Servicemodell (IaaS, PaaS, SaaS) zu rechtlichen Differenzierungen führen:

### 2. Analyse unter Differenzierung nach Service-Modellen

#### a) Analyse bei Nutzung von reinen IaaS-Angeboten

67 In einem reinen IaaS-Angebot nutzt die Bank IT-Infrastrukturen des Cloud-Anbieters, und zwar im Wesentlichen Gebäude, Server, Virtualisierungsschichten und Storagekomponenten. Diese Ressourcen werden allerdings nicht isoliert genutzt, sondern sind die Basiskomponenten, auf deren Grundlage der Bank virtuelle Server bzw. virtuelle Maschinen zur Verfügung gestellt werden.[47] Diese virtuellen Maschinen benutzt die Bank in ähnlicher Weise, wie sie früher physische Serverkomponenten mit Datenträgern in eigenen Räumlichkeiten gehalten und verwaltet hat. Das Nutzungserlebnis für die Bank unterscheidet sich vom früheren Nutzungserlebnis (IT-Infrastrukturen bei der Bank) nicht wesentlich.

68 Die vom Cloud-Anbieter eingesetzten Basiskomponenten werden vom Cloud-Anbieter automatisiert verwaltet. Dazu dienen Steuerungssysteme, die es dem Cloud-Anbieter ermöglichen, die in grosser Zahl bereitgestellten Ressourcen mit angemessenem Aufwand und einem überaus hohen Mass an Automatisierung für die Bank nach einheitlichen Methoden (also gleich wie für andere Kunden) zu verwalten. Eine kundenindividuelle Betreuung zu Gunsten der Bank findet grundsätzlich nicht statt. Der Cloud-Anbieter bedient die zentrale Automatisierungslösung in einer Weise, dass auf allen Ebenen der eingesetzten IT-Infrastrukturen Softwarekomponenten automatisiert aktualisiert werden oder die Aktualisierung für alle der eingesetzten Basiskomponenten (oder für eine nach abstrakten Kriterien definierte Auswahl der Basiskomponenten: Versionennummer, Alter der

---

47 Zum Begriff "Basiskomponenten" siehe Anhang.

Hardware, etc.) einheitlich vorgenommen werden kann. Das Steuerungssystem ermöglicht also eine effizientere Steuerung von Handlungen zur Aufrechterhaltung und Verbesserung des Gesamtsystems. Die für die rechtliche Analyse zentrale Charakteristik dieses Vorgehens besteht darin, dass die eingesetzten Ressourcen des Cloud-Anbieters nicht von menschlicher Hand und dediziert für die Bank verwaltet werden, sondern automatisiert und uniform für die gesamte Kundenbasis. Dieser Ansatz kann mit dem Schlagwort "Hyperscale" bezeichnet werden. Anders als in kleinen IT-Infrastrukturen sind Cloud-Angebote, die nach dem Hyperscaler-Ansatz aufgebaut sind, notwendigerweise anonym. Während zwar noch immer Menschen die zentrale Automatisierungslösung bedienen, steuern sie vielmehr die Verwaltungskriterien, als dass sie "für einen einzelnen Kunden" Management-Aufgaben übernehmen.

69 Die Verwaltung der IT-Infrastrukturen mit dem Hyperscaler-Ansatz kommt zum Ausdruck in Abläufen, die Anonymität fördern:

- Genehmigungsprozesse sorgen dafür, dass zu keinem Zeitpunkt ein einzelner Mitarbeitender unbegründet Zugriff auf eine Steuerungskomponente nehmen kann; der Zugriff auf die Steuerungskomponente muss von einem Manager genehmigt werden, der nur für diesen Zweck Approval-Funktionen hat, im Übrigen aber mit der zugriffsberechtigten Person nicht zusammenarbeitet. Solche Genehmigungsprozesse fördern auch innerhalb der Teams des Cloud-Anbieters die Anonymität, so dass Interessenkonflikte und Kollusion zum Nachteil eines bestimmten Kunden minimiert, wenn nicht ausgeschlossen werden.

- Wird einem Mitarbeitenden der Zugriff gewährt, erfolgt dies nur für die Dauer, die der Mitarbeitende für den in der Genehmigungsanfrage angegebenen Grund – der selbstverständlich plausibilisiert werden muss – benötigt. Man spricht von "Just in Time"-Access. Die erteilten Rechte sind limitiert und dem Zweck des Zugriffsgesuchs angemessen ("Just enough"-Access).

- Im IaaS-Modell wirken nicht nur organisatorische Massnahmen. Eine technische Limitierung der Zugriffsmöglichkeit von Personal des Cloud-Anbieters resultiert aus der Funktionalität der zentralen Steuerungssoftware. Diese ist dafür da, Softwaresysteme zu aktualisieren. Sie ist aber nicht dazu da, Zugriffe auf Virtuelle Maschinen einzelner Kunden zu eröffnen (wozu es andere Systeme benötigt und auch die softwaretechnisch abgebildete Zustimmung des Kunden erforderlich ist).

- Alle Massnahmen werden in Logs protokolliert.

70 Diese anonymisierte Methodik der Bereitstellung und Verwaltung limitiert gesamthaft die Wahrscheinlichkeit, dass im Normalbetrieb ein Mitarbeitender eines Cloud-Anbieters auf eine Virtuelle Maschine der Bank und die darauf sich befindlichen Daten zugreifen könnte. Die Virtuellen Maschinen sind durch softwaretechnische Massnahmen innerhalb der Virtualisierungsschicht vor unbefugten Zugriffen geschützt.

71 Die Bank ihrerseits ist im IaaS-Ansatz frei, das "Innenleben" der Virtuellen Maschine eigenständig zu definieren: Sie wählt die konkrete Softwarekonfiguration (Betriebssystem und Anwendungssoft-

ware) auf der Virtuellen Maschine aus und definiert die in diesem Rahmen gewünschten Datenmodelle. Verliert die Bank die Zugriffsdaten für die Virtuelle Maschine oder für die auf dieser laufenden Applikationen, kann der Cloud-Anbieter im Hyperscaler-Modell den Kunden nicht unterstützen, um Recovery-Massnahmen einzuleiten. Der Kunde muss diese Massnahmen dann selber treffen.

72 Ergänzend ist für das IaaS-Modell anzumerken, dass das Gesamtsystem selbstverständlich vom Cloud-Anbieter koordiniert wird. Der Cloud-Anbieter stellt den Administratoren der obersten Ebene.[48] Sollte ein Mitarbeitender des Cloud-Anbieters Zugriff nehmen müssen und bei diesem Zugriff Daten des Kunden einsehen können, muss er über den Administratoren des Kunden berechtigt werden (ein Ablauf, der mittels technischer sowie organisatorischer Massnahmen abgebildet und gesichert wird). Der Administrator des Kunden ist im Gesamtsystem gleichsam der Administrator der zweitobersten Ebene[49] (der situativ vom Kunden zusätzlich freigeschaltete Supportmitarbeitende hätte die Rolle eines kurzfristigen Benutzers oder subalternen Administratoren auf der dritten Ebene).[50]

73 Dies ist bei weitem keine vollständige Schilderung eines IaaS-Modells. Die Ausführungen sollen aber aufzeigen, dass je nach Service-Modell und mittels einer Vielzahl von ineinander hineingreifenden Massnahmen technischer und organisatorischer Natur die Wahrscheinlichkeit und in weitgehender Hinsicht auch die Möglichkeit reduziert oder gar ausgeschlossen wird, dass Mitarbeitende im Normalbetrieb auf Virtuelle Maschinen des Kunden und damit auf gespeicherte Daten überhaupt zugreifen können. Durch das dem Hyperscaler-Ansatz inhärente hohe Mass an Automatisierung und Anonymität ergibt sich somit für die Bank als Kundin ein natürlicher Schutz gegen unbefugte Klartext-Zugriffe einzelner Mitarbeitender des Cloud-Anbieters auf Bankkundendaten.

74 Wenn der Cloud-Anbieter einen derart wirkenden Mix an Massnahmen plausibel zu dokumentieren vermag, kann die Bank den Nachweis führen, dass ihre Wahl (z.B. "reines IaaS-Modell") in Verbindung mit den dokumentierten Massnahmen zu einem so verbindlich voraussehbaren Schutz gegen unbefugte Zugriffe führt, dass Klartext-Zugriffe im Normalbetrieb der Lösung nach menschlichem Ermessen ausgeschlossen werden können.

75 Dass der Cloud-Anbieter Direktzugriff auf die virtuelle Maschine des Kunden nimmt, kann technisch ausgeschlossen werden. Theoretisch betrachtet kann aber nicht ausgeschlossen werden, dass der Cloud-Anbieter auf die verschlüsselte Speicherdatei[51] für die Virtuelle Maschine zugreift (der Cloud-Anbieter stellt ja den Administratoren der obersten Ebene, Rz. 72). Dass er diese Datei mittels sog.

---

48 Administratorenrolle der obersten Ebene: Dieser Begriff wird aus Gründen der Verständlichkeit verwendet, ist aber aus technischer Sicht ungenau. Es geht eher um eine Aufgabentrennung, bei der der Cloud-Anbieter die zugrunde liegenden Basiskomponenten verwaltet und mit den virtuellen Maschinen nichts zu tun hat. Der Administrator des Cloud-Anbieters hätte die Möglichkeit, eine definierte virtuelle Maschine hoch- und herunterzufahren, ohne jedoch Zugriff auf die virtuelle Maschine zu erhalten. Die Möglichkeit, eine virtuelle Maschine herunterzufahren ist auf dringliche Fälle beschränkt, in welchen die betroffene virtuelle Maschine ausserhalb des Normalbetriebs läuft und dieser Zustand Auswirkungen auf die Stabilität der in derselben Umgebung ausgeführten virtuellen Maschinen hätte.

49 Die Terminologie ist wiederum technisch nicht präzise. Es geht um Segregation. Die Administratoren des Kunden könnten als VM-Administratoren oder IaaS-Administratoren bezeichnet werden.

50 Soweit der Cloud-Anbieter aus technischen Gründen, z.B. für das Patching der Softwareschicht gewisse Softwarepakete automatisiert in die Virtuelle Maschine des Kunden verteilen muss, kann dies mittels standardisierten Einträgen in das Berechtigungssystem des Kunden erreicht werden. Man kennt für solche Zugriffe ohne Dateneinsichtnahme z.B. das Konzept des Eligible Admins. Es würde jedoch zu weit gehen, dieses Konzept hier zu vertiefen.

51 Bei einer virtuellen Maschine werden die Daten in einem spezifischen Format (VHDX, VMDK, etc.) gespeichert und sind technisch gegen Klartext-Zugriffe geschützt.

"Brute Force" entschlüsselt, kann technisch gesehen zwar nicht zu hundert Prozent ausgeschlossen werden. Diese Möglichkeit ist jedoch so marginal, dass man sie nicht ernsthaft als realistische Gefahr bezeichnen kann. Da (und soweit) aber technische und organisatorische Massnahmen eingerichtet sind, die sicherstellen, dass ein solcher Zugriff im Normalbetrieb nicht stattfindet, resultiert im IaaS-Modell kein strafrechtlich sanktionierbares Verhalten, wenn eine Bank Daten in die IT-Infrastrukturen des Cloud-Anbieters migriert. Dieser Schluss stellt ab auf die jüngste Rechtsprechung des Bundesgerichts (wonach nur der tatsächliche Zugriff zählt, siehe vorn Rz. 17).

**b) Analyse bei Nutzung von reinen PaaS-Angeboten**

76 Ein PaaS-Angebot unterscheidet sich von einem IaaS-Angebot dadurch, dass der Kunde die virtuellen Maschinen nicht selber verwaltet. Der Cloud-Anbieter übernimmt die Verwaltung der virtuellen Maschinen, inklusive Betriebssystem und Plattformsoftware wie Datenbankensoftware und dergleichen, die ebenfalls vollständig durch den Cloud-Anbieter betrieben werden. Die technischen Basiskomponenten, die für das PaaS-Modell zur Anwendung kommen, unterscheiden sich nicht von jenen, die beim IaaS-Modell eingesetzt werden. Die Bereitstellung wird aber anders aufgesetzt:

- Beim IaaS-Modell "bucht" ein Kunde aus seinem Tenant heraus gewisse Ressourcen. In der Folge werden diese für den Kunden in dessen Berechtigungssystem registriert, und zwar dediziert (mittels logischen Definitionen in Identitätssystemen und Netzwerksystemen). Der Cloud-Anbieter stellt im Gesamtsystem wie bereits geschildert den Administratoren der obersten Ebene, der Kunde den Administratoren der zweitobersten Ebene (Rz. 72).

- Beim PaaS-Modell wird ein Service zuerst im Sinne eines Standardprodukts vom Cloud-Anbieter aufgesetzt. Damit stellt der Cloud-Anbieter hier gleichsam auch den Administratoren der zweitobersten Ebene (zusätzlich zum Administratoren der obersten Ebene). Wenn der Kunde aus seinem Tenant heraus solche Standardprodukte bucht, werden in seinem Berechtigungssystem Einträge generiert, die mit logischen Methoden sicherstellen, dass die Datenhaltung für das Standardprodukt in eindeutiger Weise und ausschliesslich für ihn (und nicht für einen anderen Kunden) mit dem Standardprodukt verknüpft wird. Der Administrator des Kunden wird im Gesamtsystem gleichsam der Administrator der drittobersten Ebene. Sollte der Kunde vom Cloud-Anbieter einen auf seinen Tenant bezogenen, dedizierten Support anfordern, würde der Administrator des Kunden den Supportmitarbeitenden auf die Tenant-Sicht des Kunden freischalten.

77 Die Nutzungsberechtigung des Kunden (d.h. der Bank) ergibt sich somit auch im PaaS-Modell über die Definition des Tenants. Das zentrale Stichwort dafür, wie der Kunde in einer PaaS-Umgebung Kontrolle über seine Daten behält, lautet "Tenant Isolation" (oder "tenant level isolation" oder dergleichen). Die Darstellung in Rz. 76 zeigt aber, dass verstärkt organisatorische Massnahmen zum Tragen kommen, um die Datenhaltung des Kunden gegen Zugriffe von Mitarbeitenden des Cloud-Anbieters zu schützen. In Bezug auf die strafrechtlich entscheidende Frage, ob eine relevante Offenbarung von geheimnisgeschützten Informationen entsteht, ändert sich im Resultat nichts – solange eben im Gesamtsystem genügende Methoden zur Sicherung gegen unbeabsichtigte Zugriffe auf die Datenhaltung der Bank nachweisbar sind. Das Fazit gemäss Rz. 75 kann somit auch auf das PaaS-Modell übertragen werden.

### c) Analyse bei der Nutzung von SaaS-Angeboten ohne Auslandsbezug (oder um SaaS-Komponenten ergänzte IaaS- oder PaaS-Angebote)

78 Bei einem SaaS-Modell verschiebt sich die Beherrschung des Gesamtsystems noch weiter hin zum Cloud-Anbieter. Während im IaaS-Modell noch vielfältige Schutzmechanismen greifen, die inhärent technischen Architekturfragen geschuldet sind, entfallen solche technischen Schutzmechanismen in signifikantem Umfang. Mit anderen Worten werden organisatorische Schutzmassnahmen im SaaS-Modell noch wichtiger. Um welche Schutzmechanismen es geht, kann hier nicht abstrakt geschildert werden, weil in SaaS-Modellen die konkreten Wirkmechanismen sehr individuell sein können. Entscheidend ist, dass die Bank nach Analyse dieser Wirkmechanismen (die wie gesehen v.a. organisatorischer Natur sein werden) bestätigen kann, dass im Normalbetrieb mit genügender Verlässlichkeit Mitarbeitende des Cloud-Anbieters nicht unbefugten Klartext-Zugriff auf geschützte Informationen der Bank bzw. ihrer Bankkunden nehmen werden.

## 3. Fazit

79 Die stark auf die anonymisierte Verwaltung der Basiskomponenten ausgerichteten Architekturen von reifen Cloud-Angeboten erlauben die Nutzung von fremden IT-Infrastrukturen, ohne dass es im Normalbetrieb zu Klartext-Zugriffen (Offenbarungen) kommt. Wenn die Bank sich vergewissert, dass entsprechende technische und organisatorische Massnahmen zum Schutz gegen Offenbarungen greifen, kann sie solche Cloud-Angebote nutzen, ohne Art. 47 BankG zu verletzen – und zwar auch wenn sie den Cloud-Anbieter nicht als Beauftragten bestellt. Solche Cloud-Angebote sind gleichsam Erweiterungen des physischen und logischen Perimeters der Bank (dazu Rz. 5), zu einer Erweiterung des personellen Perimeters kommt es nicht.

## II. Fallback: Absicherung von reinem "Incidental Access"

80 Im Folgenden geht es um die Frage, ob ein Supportmitarbeiter des Cloud-Anbieters in Supportsituationen einzelfallweise Klartext-Zugriff auf geschützte Information erhalten darf, wenn der Cloud-Anbieter nicht als Beauftragter bestellt wurde (sonst sind Supportzugriffe von vornherein privilegiert). Solche fallbezogenen Zugriffe auf geschützte Information können vorkommen in Fällen wie den folgenden:

a. Incident: Die Bank hat ein Problem *in* ihrem Tenant, zu dessen Behebung sie Unterstützung benötigt; sie will einen Mitarbeitenden des Cloud-Anbieters beiziehen.

b. Maintenance: Die Bank ist darauf angewiesen, dass der Hersteller gewisser Softwarekomponenten Arbeiten zur Softwarepflege in ihrem Tenant ausführt. Dieser möchte sich von einem Mitarbeitenden des Cloud-Anbieters helfen lassen.

c. Support: Die Bank wünscht Unterstützung bei der Vornahme von Arbeiten zur Softwarepflege, wozu sie einen Mitarbeitenden des Cloud-Anbieters beiziehen will.

81 Dass die Bank in diesen Situationen den Cloud-Anbieter bzw. dessen Mitarbeitende benötigt, ist so gut wie ausgeschlossen, auf jeden Fall sehr selten. Dennoch kann die Eventualität, dass eine Bank den Cloud-Anbieter trotzdem beiziehen will, nachstehend juristisch gewürdigt werden. Man muss sich aber bewusst sein, dass es sich dabei um überaus selten vorkommende Szenarien handeln wird.

82 So etwas wie "die Cloud" gibt es nicht (Rz. 67 ff.). Die vorstehenden Ausführungen haben dies bereits gezeigt. Auf eine erneute Differenzierung nach Service-Modellen wird an dieser Stelle verzichtet und es wird nur der Vergleich zwischen einer IaaS-Lösung und einer SaaS-Lösung vorgenommen.

### 1. Im IaaS-Modell

83 Wenn ein Mitarbeiter des Cloud-Anbieters über Remote-Access zum Beispiel Zugriff auf die Virtuelle Maschine der Bank erhält (weil die Bank ihm diesen gibt) und es in diesem Kontext zu Klartext-Zugriffen durch den Supportmitarbeitenden kommt, muss die Bank die Bewegungen des Support-Mitarbeiters in der Virtuellen Maschine mitverfolgen. Die Bank darf dem Support-Mitarbeitenden des Cloud-Anbieters nur in Ausnahmefällen (nur wo nötig: "need to know") die Steuerung des Bildschirms überlassen. Es ist in aller Regel auch gar nicht erforderlich, dass der Mitarbeitende des Cloud-Anbieters diese Steuerung selber führt. Der Mitarbeitende der Bank wird vielmehr über Sprachanweisungen des Supporters in der Lage sein, die Steuerung selber umzusetzen. Sollte ausnahmsweise doch erforderlich sein, dass der Mitarbeitende des Cloud-Anbieters kurzzeitig die Kontrolle über eine Virtuelle Maschine der Bank übernimmt, muss der Mitarbeitende der Bank jederzeit in der Lage sein, die Abläufe abzubrechen oder zu pausieren. Der Mitarbeitende der Bank darf dann den Bildschirm in keinem Zeitpunkt verlassen.

84 Im Supportfall besteht darüber hinaus eine limitierte Anzahl von denkbaren Fällen, in denen der Mitarbeitende des Cloud-Anbieters doch Kundendaten einsehen können muss. Erst in diesem Fall kommt es zu einer Offenbarung. Offenbarungen sind grundsätzlich unzulässig. Entsprechend hat die Bank solche Supportanfragen grundsätzlich zu unterlassen.

85 Wo solche, Bankkundendaten offenbarende Supportanfragen der Bank gleichwohl notwendig werden, wird es in aller Regel für die Bank möglich sein, entweder ein mitigierendes Dispositiv einzurichten oder einen Workaround vorzunehmen.

86 Möglichkeiten zu Workarounds sind etwa die folgenden:

a. Die Bank zieht einen lokalen Beauftragten bei, bestellt ihn formell als Beauftragten und lässt ihn diese ganz spezielle Aufgabenstellung umsetzen (eventuell mit offline-Support durch den Cloud-Anbieter).

b. Die Bank anonymisiert Bankkundendaten oder löscht sie kurzzeitig aus dem System.

c. Die Bank setzt vorübergehend eine identische digitale Kopie der Virtuellen Maschine ohne Kundendaten auf und visualisiert die Problemstellung gegenüber dem Support-Mitarbeitenden des Cloud-Anbieters auf dieser Basis.

87 Als mitigierendes Dispositiv kommen Kombinationen von Massnahmen in Betracht. Muss ein Supportmitarbeitender des Cloud-Anbieters tatsächlich Einsicht nehmen, könnte der Supportmitarbeiter mit besonders streng wirkenden Geheimhaltungsvorschriften (bspw. mit empfindlichen Konven-

tionalstrafen) in die Kontrollhoheit der Bank eingebunden werden. Mithin wird der Supportmitarbeitende für diese isolierte konkrete Handlung formell zum Beauftragten. Ansonsten muss im Einzelfall eine Lösung gefunden werden, die zu effektiver Kontrolle der Bank führt.

88 Schliesslich sind Szenarien denkbar, die im Einzelfall eine Rechtfertigungsmöglichkeit eröffnen könnten wie beispielsweise Notstand oder absolute Bagatellfälle. Solche Szenarien sollten aber nur sehr zurückhaltend im Rahmen einer vorab erfolgenden Risikoanalyse mitberücksichtigt und gewertet werden. Die Rechtfertigungsmöglichkeit ergibt sich für solche Szenarien dann, wenn sie den absoluten Ausnahmefall abbilden. Wären es regelmässig auftretende Ereignisse, müssten sie wohl dem Normalbetrieb zugerechnet werden. Dies würde anschliessend zu anderen Einschätzungen führen.

89 Zusammenfassend ergeben sich auch für die eingangs geschilderten (überaus seltenen) Szenarien in einem IaaS-Modell, in denen ein "Incidental Access" stattfinden könnte, derart zahlreiche Konstellationen ohne Offenbarung oder mit Rechtfertigungsmöglichkeit, dass im Resultat der Supportfall (und die anderen Szenarien von "Incidental Access") keinen Grund darstellen darf, der Bank a priori die Nutzung von Cloud-Angeboten generell und umfassend zu verbieten.

### 2. Im SaaS-Modell

90 Für SaaS-Komponenten kann man meist nicht mehr nach Virtuellen Maschinen differenzieren, da solche Virtuellen Maschinen meist nicht einem einzelnen Kunden zugewiesen sind. Die Analyse bezieht sich hier ausschliesslich auf *Tenants*, d.h. auf logisch getrennte Zugriffsbereiche, die über mehrere Virtuelle Maschinen hinweg dem Kunden bereitgestellt werden. Und auch hier lässt sich differenzieren danach, ob der Cloud-Anbieter zur Vornahme der in Rz. 80 genannten Arbeiten innerhalb des Tenants oder ausserhalb des Tenants arbeiten muss.

91 Der Cloud-Anbieter "nähert sich" im SaaS-Modell dem vom Kunden genutzten Tenant viel stärker als im IaaS- oder PaaS-Kontext. Auch die Softwarearchitekturen sind anders aufgesetzt und trennen die rein vom Kunden genutzten Ressourcen oft weniger genau von jenen, die vollständig vom Cloud-Anbieter verwaltet werden.

92 Auf jeden Fall sind die Möglichkeiten der Bank, Informationen über ihre Kunden so in die IT-Architekturen des Cloud-Anbieters zu speichern, dass der Cloud-Anbieter sie von vornherein nicht wahrnehmen kann, stark abhängig vom Lösungsdesign, das der Cloud-Anbieter aufgesetzt hat. Nur wenn der Cloud-Anbieter architektonisch dafür gesorgt hat, die im SaaS-Modell aufgesetzten Tenants von den zum Application Management und der Softwarepflege erforderlichen Basiskomponenten zu trennen, kann der Cloud-Anbieter darauf aufbauend auch klare organisatorische Regeln setzen, um seinen Mitarbeitern den Zugriff auf den Tenant des Kunden zu unterbinden. Die Auswahl von SaaS-Modellen erfordert darum vom Kunden ein noch sorgfältigeres Auswahlverhalten. Die Anforderungen an die intern bei der Bank für die Beschaffung zuständige Abteilung nehmen für solche Modelle zu. Hat der Cloud-Anbieter allerdings für solche IT-Architekturen gesorgt, kann er dem Kunden auch Abläufe anbieten, welche Berührungspunkte zum Tenant des Kunden proaktiv reduzieren oder weitgehend ausschliessen.

*Einzelne Cloud-Anbieter haben zum Beispiel für Arbeiten mit der Gefahr der Einsichtnahme in den Tenant des Kunden besondere Schutzmechanismen organisatorischer Art eingerichtet. Bekannt ist*

*bspw. ein "Customer Lockbox" genanntes Ablaufmodell (eine reine organisatorische Massnahme) von Microsoft. Ein Supportmitarbeitender kann unter diesem Regime kraft interner Weisungen erst dann auf den in Frage stehenden Tenant zugreifen, wenn er ein bestimmtes Verfahren durchlaufen hat. Microsoft äussert in Marketingunterlagen die Erwartungshaltung, dass es kaum je nötig sei, dass Microsoft auf den Tenant bzw. auf die im Tenant gespeicherten Daten zugreifen müsse (Ausnahmefälle, über die der Kunde proaktiv informiert werde und vorgängig seine Zustimmung erteilen kann, seien verschwindend klein).*

93 Fehlen die Grundlagen in der IT-Architektur für solche organisatorischen Massnahmen, bauen viele Cloud-Anbieter ein Dispositiv auf, das über Zugriffs-Logs prüft, inwiefern ein Mitarbeitender ohne ein ausgewiesenes Bedürfnis ("need to know") auf einen Tenant zugreift.[52] Dieser Schutz hat proaktive Wirkung dadurch, dass Mitarbeiter wissen, dass sie auf unzulässige Zugriffe geprüft werden und im Missbrauchsfall mit strengen Sanktionen zu rechnen haben. Logs ermöglichen im Übrigen aber erst eine retrospektive Kontrolle des Verhaltens des Cloud-Anbieters.

94 Fazit: Es sind technische Setups und organisatorische Dispositive möglich, die eine Offenbarung für Betriebshandlungen in genügendem Mass auch bei SaaS-Modellen ausschliessen.

### 3. Resultat

95 Die vorstehenden Überlegungen zeigen auf, dass die Bank für die womöglich angeforderte Unterstützung entweder nicht mit dem Cloud-Anbieter zusammenarbeiten wird (Maintenance-Arbeiten im IaaS- und PaaS-Modell für eigene Applikationen der Bank) oder vielfältige Sicherheitsdispositive eingerichtet werden können, welche die Integritätsinteressen der Bank und ihrer Bankkunden im Normalbetrieb schützen.

96 Es zeigt sich, dass im Kontext von Maintenance-Arbeiten, Incident-Handling und Supportanfragen nicht a priori ein Verbot besteht, dass die Bank nach dem Stand der Technik aufgesetzte Cloud-Angebote von vertrauenswürdigen und sorgfältig auditierten Cloud-Anbietern nutzt.

## ERGEBNIS: SCHWEIZERISCHE BANKEN KÖNNEN REIFE CLOUD-ANGEBOTE NUTZEN

Überlegungen zur vertraglichen Beziehung zwischen Bank und Bankkunde (Rz. 7 f., Rz. 11 und Rz. 13), die allgemeine Strafrechtsdogmatik (Art. 11 StGB, dazu Rz. 22 ff., und v.a. Rz. 26, und Art. 12 StGB, dazu Rz. 28), verfassungskonforme Überlegungen (Rz. 12), die neuste Rechtsprechung (Rz. 17) und der überwiegend einhellige Stand der Lehre führen insgesamt zu demselben Resultat: Der Einsatz von IT-Infrastrukturen muss einer Bank dann erlaubt sein, wenn diese IT-Infrastrukturen mit adäquaten Massnahmen (zum Stand der Technik siehe Rz. 26) geschützt sind. Wer diese IT-Infrastrukturen betreibt, steht nicht im Zentrum.

---

52 Lässt sich der Cloud-Anbieter auditieren, haben solche Zugriffslogs eine immense Bedeutung. Auditoren prüfen nach international anerkannten Standards (z.B. der International Standard on Assurance Engagements, ISAE, verwaltet von der International Federation of Accountants, IFAC), wobei Standards über die Verlässlichkeit finanzieller Informationen (ISAE 3402) von Standards betreffend die Integrität und den Schutz anderer Informationen (ISAE 3000) unterschieden werden (ähnlich die Unterscheidung SOC 1 v. SOC 2, wobei "SOC" für "Service Organisation's Controls" steht). Während solcher Prüfungen werden gewisse Zugriffs-Logs oft lückenlos überprüft, was mindestens eine nachträgliche Kontrolle über die Zuverlässigkeit der Massnahmen beim Cloud-Anbieter ermöglichen. Dabei wird unterschieden zwischen bloss einmaligen Bestandesaufnahmen (Type I, Type 1 oder in anderen Standards auch Typ A; "Snapshots") und solchen, die sich über einen längeren Zeitraum von meist einem halben Jahr erstrecken (Type II, Type 2 oder in anderen Standards auch Typ B).

Das Rechtsgutachten zeigt somit, dass schweizerische Banken Cloud-Angebote nutzen können, wenn sie im Rahmen eines sorgfältigen Beschaffungsprozess verlässliche Cloud-Anbieter auswählen, die eine reife IT-Infrastruktur bereitstellen. Mittels technischer, organisatorischer und teilweise vertraglicher Massnahmen können solche Cloud-Anbieter einen genügenden Schutz für geheimnisrelevante Informationen bereitstellen.

Solange der Cloud-Anbieter dafür sorgt, dass nirgends und in keinem Zeitpunkt in unbefugter Weise auf die Informationen bzw. auf die darunter liegenden Daten zugegriffen wird, welche die Bank in die IT-Infrastruktur des Cloud-Anbieters migriert hat, verletzt die Bank den objektiven Tatbestand von Art. 47 BankG nicht – sogar ohne den Cloud-Anbieter als Beauftragten zu bestellen.

Cloud-Anbieter können als Beauftragte der Bank bestellt werden. In der Praxis darf die Bedeutung der Einbindung des Cloud-Anbieters als Beauftragten im Sinne von Art. 47 BankG jedoch nicht überbewertet werden. Wenn die Bank im Einzelnen nachvollzieht, wie neuralgische Abläufe beim Cloud-Anbieter umgesetzt werden, wird sie in den meisten Fällen wohl bereits feststellen, dass es zu keinen massgeblichen Offenbarungen kommen wird – was eine Einbindung des Cloud-Anbieters als "Beauftragten" an und für sich entbehrlich machen wird. Diese Vergewisserung ist aber bereits aufgrund von Art. 11 Abs. 2 StGB und Art. 12 Abs. 3 StGB erforderlich, auch wenn die Bank den Cloud-Anbieter als Beauftragten bestellt.

* * *

## ANHANG: VERWENDETE BEGRIFFE

In diesem Rechtsgutachten werden die folgenden Begriffe einheitlich verwendet:

**Cloud-Anbieter** steht stellvertretend für Anbieter von IT-Dienstleistungen, welche auf der Basis des Cloud Computing aufbauen. Dies umfasst sämtliche Integrationstiefen der Cloud-Lösung, von IaaS über PaaS bis SaaS.

**Auslandsbezug** bezeichnet Bezüge entweder des Cloud-Anbieters (rechtlicher Sitz, etc.) oder des Cloud-Angebots (Rechenzentrumsstandort, Standort von Mitarbeitenden oder beigezogenen Dritten, etc.) ins Ausland. Ein Auslandsbezug liegt bspw. vor, wenn (i) der Cloud-Anbieter seinen rechtlichen Sitz im Ausland hat; (ii) der Cloud-Anbieter IT-Infrastrukturen im Ausland betreibt oder betreiben lässt oder (iii) der Cloud-Anbieter Personal im Ausland oder Subakkordanten im Ausland beschäftigt.[53]

**Bank** umfasst die dem Bankengesetz gemäss Art. 1*a*, Art. 1*b* sowie Art. 2 BankG unterstehenden Rechtsträger.

**Basiskomponenten** ist ein Begriff, der zum Ausdruck bringt, dass die IT-Infrastrukturen des Cloud-Anbieters über den Tenant hinaus auch Gegenstand von Betriebsleistungen des Cloud-Anbieters sind und vom Cloud-Anbieter im Hintergrund über Steuerungssysteme administriert werden.

**Cloud-Angebot oder Cloud-Lösung** ist die Gesamtheit der Leistungen, mit denen ein Cloud-Anbieter einer Bank die Nutzung gewisser IT-Infrastrukturen standardisiert, automatisiert, skalierbar und in nicht dedizierter Form über Datennetze gewährt. Cloud-Angebote können die Bank davon entbinden, eigene Rechenzentren, eigene Hardware und eigene Serversoftware zu betreiben (man spricht dann von Infrastructure as a Service, **IaaS**) oder weitergehend auch dazu dienen, dass die Bank gewisse Software (Betriebssoftware oder Anwenderapplikationen) nicht selber betreiben und warten muss (man spricht dann von Platform as a Service, **PaaS**, oder Software as a Service, **SaaS**). Cloud-Angebot steht hier stellvertretend für den umgangssprachlich geprägten Begriff **"Public Cloud"**, was zum Ausdruck bringen soll, dass die Basiskomponenten des Cloud-Anbieters für keinen Kunden individuell-exklusiv ("dediziert") nutzbar sind; demgegenüber ist die bereitgestellte Nutzungsmöglichkeit innerhalb eines Tenant kundenindividuell und abgegrenzt gegenüber anderen Kunden ("Isolation"), was mittels Netzwerktechnologie ermöglicht wird.

**IT-Infrastrukturen** verweist auf die Gesamtheit von Gebäuden, Hardware, Software, Netzwerktechnologie etc., die ein Cloud-Anbieter einsetzt, um ein Cloud-Angebot bereitzustellen.

**Klartext-Zugriff** meint den Vorgang, mit dem ein Mensch ohne weiteres Hilfsmittel den Bedeutungsgehalt von ihm präsentierten Zeichen erkennen, lesen und sich merken oder weitergeben kann. *Blosser Zutritt* zum Ort der Datenhaltung begründet demgegenüber keinen Klartext-Zugriff. Wer einen Serverraum besuchen darf und im Gang zwischen den Servern an den Datenträgern vorbeischlendert, hat offenbar Zutritt zu Daten (genauer: zum Ort der Datenhaltung). Selbst wenn er dies ohne Aufsicht tut, hat er von den Inhalten, die auf den Datenträgern gespeichert sind, noch keine Kenntnis erhalten. Wenn der Besucher

---

[53] Für diese Kategorie (Personal oder Subakkordanten) besteht der Auslandsbezug dann, wenn aus dem Ausland Zugriff auf das Cloud-Angebot genommen werden kann.

den Serverraum anschliessend wieder verlässt, ohne auf die Datenträger zuzugreifen, ist in Bezug auf das zu wahrende Geheimnis nichts passiert. Gleichermassen sprechen wir nicht von Klartext-Zugriff, wenn jemand erst ein technisches Hilfsmittel benötigt, bevor er den Bedeutungsgehalt erkennen kann etc. Ein solches Hilfsmittel könnte etwa ein Bildschirm sein, der an einem Datenverarbeitungsgerät angeschlossen ist; oder eine Applikation, die auf eine Datenbank zugreift und dank der die in der Datenbank gespeicherte Information erst für den Anwender transparent erkennbar wird. Der Begriff ist von Bedeutung für das Verständnis von Geheimnispflichten. Das schweizerische Recht hält aber keine geeigneten Begrifflichkeiten bereit, um für Menschen erkennbare Angaben von technisch geprägten Formatierungen zu unterscheiden, die nur von Maschinen interpretiert werden können, aber ohne Hilfsmittel nicht für Menschen erkennbar sind. Entsprechend verwenden wir hier diese umgangssprachliche Begrifflichkeit.

**Normalbetrieb**[54] meint, dass das Cloud-Angebot wie geplant vom Cloud-Anbieter betrieben wird (im Gegensatz zu ausserordentlichen Situationen, die dem Normalbetrieb nicht zuzurechnen sind, wie: Konkurs[55] des Cloud-Anbieters; Behördenzugriff[56] auf das Cloud-Angebot; Zugriffe von Kriminellen auf das Cloud-Angebot).

**Tenant** ist die der Bank bereitgestellte, kundenindividuelle Nutzungsumgebung und damit ein Zugriffsbereich, der mit Mitteln der Netzwerktechnologie ausschliesslich der Bank und ihren Mitarbeitenden zur Nutzung bereitsteht. Ein Tenant wird meist über mehrere Basiskomponenten hinweg ermöglicht; eine genaue Zuordnung eines Tenant zu einer bestimmten Basiskomponente ist in zeitlicher Hinsicht variabel; bei Betrachtung nur in einem konkreten Augenblick ("Snapshot") wäre eine Zuordnung zwar möglich, aber sehr aufwändig.

* * *

---

54 Die Berechtigung zu dieser Unterscheidung ergibt sich aus der Überlegung, dass eine Bank rechtliche Risiken der Offenbarung nur in dem Ausmass berücksichtigen muss, wie sie sie beherrschen kann. Soweit gewisse Risiken sich abstrakt vorhersehen lassen, können sie aber Informationspflichten gegenüber den Bankkunden auslösen.

55 Die Bank muss dieses Szenario sorgfältig planen und muss ausserdem den Cloud-Anbieter hinsichtlich des Insolvenzrisikos überwachen. Dies umfasst die Verpflichtung der Bank, eine enge Interaktion mit dem Key Account Manager des Cloud-Anbieters aufrechtzuerhalten und die Finanzabschlüsse des Cloud-Anbieters regelmässig zu überprüfen. Die Bank muss auch ihre Planung zur Aufrechterhaltung ihrer Geschäftstätigkeit (Business Continuity) an solchen Szenarien messen lassen können (um ein schnelles Back-Sourcing und das sofortige Löschen von Daten zu ermöglichen). Beispielsweise muss ein Notfallplan vorliegen, nach welchem die Bank geheimnisrelevante Daten sofort und direkt über das Verwaltungspanel des Kundenportals löscht, sobald die Bank Kenntnis vom Konkurs des Cloud-Anbieters erlangt – und zwar noch bevor der allenfalls bestellte Konkursverwalter der Bank die Zugänge auf die IT-Infrastrukturen des Cloud-Anbieters sperrt.

56 Eine Strafverfolgungsbehörde verlangt von der Bank oder vom Cloud-Anbieter, ihr Zugriff zu gewähren auf Daten eines Bankkunden (oder auf Daten der Bank). Sehr wenige Autoren diskutieren das Risiko eines ausländischen Strafverfolgungszugangs in angemessener Weise, d.h. ohne sich in die oft unscharfen Gespräche zu Themen wie dem CLOUD-Act, dem US-amerikanischen PATRIOT-Act und ähnlichen Regeln des Strafverfolgungsrechts ausländischer Regierungen zu äussern. Auch das Risiko eines Zugriffs durch inländische Behörden ist als Situation zu behandeln, die nicht dem Normalbetrieb zuzurechnen ist. Der Zugang einer Schweizer Behörde kann ähnliche oder sogar dramatischere Auswirkungen auf den Bankkunden haben als der Zugang einer ausländischen Strafverfolgungsbehörde. Natürlich kann es auch andersherum sein. Die Bank weiss in der Regel nicht, wie die Risikoexposition des Bankkunden diesbezüglich aussieht. Die Bank muss aber verstehen, mit welcher Wahrscheinlichkeit und unter welchen Umständen eine Behörde auf ihre Daten zugreifen kann (unabhängig vom Einsatz von Cloud-Angeboten).