walderwyss rechtsanwälte

Walder Wyss AG
Seefeldstrasse 123
Postfach
8034 Zürich
Schweiz

Telefon +41 58 658 58 58
Telefax +41 58 658 59 59
www.walderwyss.com

Gutachten

erstattet an	Schweizerische Bankiervereinigung (SBVg)
von	Walder Wyss AG (Dr. Michael Isler, Oliver M. Kunz, Dr. Thomas Müller, Dr. Jürg Schneider, Dr. David Vasella)
betrifft	**Zulässigkeit der Bekanntgabe von Bankkundendaten durch schweizerische Banken an Beauftragte im Ausland unter Art. 47 BankG**
Datum	15. Februar 2019 / 9101398v1

Inhalt

1. Ausgangslage 2

2. Ergebnisse 3

3. Grundlagen 5
3.1. Schutzrichtung des Bankkundengeheimnisses 6
3.2. Der Geheimnisbegriff von Art. 47 BankG 12
3.3. Der Begriff der Offenbarung 14
3.4. Subjektiver Tatbestand 16
3.5. Strafbarkeit der Tatbegehung im Ausland 18

4. Zur Zulässigkeit einer Auslagerung von CID an einen Dienstleister 19
4.1. Zulässigkeit einer Auslagerung an Hilfspersonen 19
4.2. Zulässigkeit einer Auslagerung ins Ausland 23
4.3. Ergebnis 24

5. Sorgfaltsmassstäbe bei der Auslagerung 25

1. Ausgangslage

1 Die Schweizerische Bankiervereinigung (**SBVg**) hat uns gebeten, das vorliegende Gutachten zur Beantwortung folgender Frage auszuarbeiten:

> *Verletzt eine schweizerische Bank das Bankkundengeheimnis i.S.v. Art. 47 Abs. 1 und 2 des Bundesgesetzes über Banken und Sparkassen (**BankG**), falls sie einem Empfänger im Ausland im Rahmen einer Auftragsbearbeitung Bankkundendaten übermittelt?*

2 Die Ausführungen im vorliegenden Gutachten beschränken sich auf die Beantwortung der genannten Frage. Nicht Gegenstand dieses Gutachtens sind namentlich folgende Themenbereiche:

(a) Der sachliche Anwendungsbereich von Art. 47 BankG;

(b) das Bundesgesetz über den Datenschutz (**DSG**);

(c) Geheimnisschutzvorschriften ausserhalb von Art. 47 Abs. 1 und 2 BankG wie etwa Art. 273 des schweizerischen Strafgesetzbuches (**StGB**) und Art. 35 DSG; und

(d) ausländisches Recht.

3 Die zu beantwortende Frage ist vor dem Hintergrund eines Vorentwurfs des „Cloud-Leitfadens – Wegweiser für sicheres Cloud Banking“ der SBVg (der **Leitfaden**) zu verstehen. Wir verweisen in diesem Gutachten zur Illustration auf den Leitfaden, äussern uns aber nicht zur Vollständigkeit und Angemessenheit der im Leitfaden genannten technischen und organisatorischen Massnahmen oder zur Frage, welche Kombination von Massnahmen im konkreten Einzelfall angemessen ist. Der Leitfaden erhebt denn auch keinen Anspruch auf Vollständigkeit und sieht vor, dass Banken bei der Anwendung des Leitfadens ihre Grösse und die Komplexität ihres Geschäftsmodells risikobasiert und verhältnismässig berücksichtigen.

4 Wir sprechen in diesem Gutachten jeweils von „Auslagerung“ bzw. „Beizug einer Hilfsperson“ und meinen damit, dass eine Bank Dienstleistungen eines IT-Providers – z.B. eines Cloud-Anbieters – in Anspruch nimmt und dieser dabei Zugriff auf dem Bankkundengeheimnis unterstehende Informationen hat oder haben kann. Auf technische Fragen wie unterschiedliche Servicemodelle gehen wir dabei nur sehr beschränkt ein.

2. Ergebnisse

5 Wir sind der Auffassung, dass der Beizug von Hilfspersonen durch eine Bank und die Bekanntgabe von **CID** (für „Customer Identifying Data“) an diese Hilfsperson zulässig ist,

(a) solange der Beizug einem vernünftigen Interesse der auslagernden Bank entspricht, die Hilfsperson die Geschäftstätigkeit der Bank unterstützt und ihrer Weisungsbefugnis untersteht und die Bank die mit dem Bankkunden vereinbarten Leistungen insgesamt im Schwergewicht weiterhin selbst erbringt; und

(b) nicht aus einer ausdrücklich oder stillschweigend getroffenen Abrede mit dem Bankkunden folgt, dass der fragliche Beizug unzulässig ist.

6 Dies ergibt sich primär aus Art. 68 des schweizerischen Obligationenrechts (**OR**). Für eine Beschränkung dieses Grundsatzes auf Inlandssachverhalte ist keine Grundlage ersichtlich. Der Grundsatz gilt daher auch dann, wenn eine Bank die Bearbeitung von CID an einen Dienstleister im Ausland auslagert bzw. der ausländische Dienstleister im Rahmen seiner Tätigkeit für die Bank Zugriff auf CID erhält. Entsprechend sind wir der Auffassung, dass eine Bank aus zivilrechtlicher Sicht CID auch an einen ausländischen Dienstleister, bspw. im Rahmen einer Cloud-Lösung, auslagern darf, und zwar selbst dann, wenn der Dienstleister dabei Kenntnis von den CID erlangt oder nehmen kann.

7 Das Bankkundengeheimnis (Art. 47 Abs. 1 und 2 des Bankengesetzes, **BankG**) ist als strafrechtliche Verstärkung der zivilrechtlich begründeten Geheimhaltungspflichten aufzufassen. Sofern deshalb eine vertragsrechtlich zulässige Auslagerung durch eine Bank vorliegt, ist diese auch in strafrechtlicher Hinsicht zulässig, weshalb die soeben genannten Grundsätze auch hier zur Anwendung kommen. Der Beizug eines Dienstleisters und die Bekanntgabe von CID an diesen ist folglich auch nach Art. 47 Abs. BankG grundsätzlich zulässig, auch wenn sich der Dienstleister im Ausland befindet. Sieht demgegenüber eine vertragliche Vereinbarung zwischen Bank und Bankkunde ein Verbot einer Auslagerung von dem Bankkundengeheimnis unterfallenden CID vor, ist die Einhaltung dieser Vereinbarung durch Art. 47 Abs. 1 und 2 BankG auch strafrechtlich abgesichert.

8 Die eingangs gestellte Frage ist daher wie folgt zu beantworten:

Eine schweizerische Bank verletzt das Bankkundengeheimnis i.S.v. Art. 47 Abs. 1 und 2 des Bundesgesetzes über Banken und Sparkassen (BankG), nicht, falls sie einem Empfänger im Ausland im Rahmen einer Auslagerung Bankkundendaten übermittelt, sofern

(a) der Beizug einem vernünftigen Interesse der auslagernden Bank entspricht, die Hilfsperson die Geschäftstätigkeit der Bank unterstützt und ihrer Weisungsbefugnis untersteht und die Bank die mit dem Bankkunden vereinbarten Leistungen insgesamt im Schwergewicht weiterhin selbst erbringt; und

(b) nicht aus einer ausdrücklich oder stillschweigend getroffenen Abrede mit dem Bankkunden folgt, dass der fragliche Beizug unzulässig ist.

9 Die Bekanntgabe von CID im Rahmen einer solchen Auslagerung stellt somit keine unzulässige Offenbarung i.S.v. Art. 47 Abs. 1 BankG dar, selbst wenn der Auftragsbearbeiter sich im Ausland befindet und im Rahmen seiner Tätigkeit Zugriff auf die Daten nehmen kann.

10 Nur wenn es zu einer Kenntnisnahme von CID durch einen *unbefugten* Dritten kommt, liegt eine Offenbarung vor, welche i.S.v. Art. 47 Abs. 1 BankG tatbestandlich sein könnte. Eine solche Offenbarung untersteht indes nur dann schweizerischem Recht, wenn sie in der Schweiz erfolgt. Hinzu kommt, dass Art. 47 BankG keine Kausalhaftung statuiert, sondern nur dann eingreift, wenn die Bank vorsätzlich oder fahrlässig handelt, d.h. wenn sie gebotene Sicherheitsmassnahmen unterlassen und die Offenbarung dadurch kausal (mit-)verursacht hat. Die Bank hat daher bei jeder Auslagerung auch in strafrechtlicher Hinsicht die nach den Umständen gebotene Sorgfalt einzuhalten, um sich nicht dem Vorwurf der Fahrlässigkeit auszusetzen.

11 Dabei muss die Bank freilich nicht jegliche Möglichkeit einer Kenntnisnahme ausschliessen. Nur die Schaffung eines *unerlaubten* Risikos ist fahrlässig, weshalb eine Fahrlässigkeit zu verneinen ist, wenn die Bank die nach den Umständen gebotene Sorgfalt eingehalten hat. Die gebotene Sorgfalt ist dabei in erster Linie durch das geltende Datenschutzrecht, durch die Anforderungen der FINMA im Rundschreiben 2008/21 Operationelle Risiken – Banken (Anhang 3) und durch den Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) zu den technischen und organisatorischen Massnahmen zum Datenschutz zu konkretisieren. Ebenfalls beizuziehen sind ggf. weitere technische Standards, soweit sie zum Stand der Technik zählen. Die Einhaltung der gebotenen Sorgfalt setzt sodann eine Einschätzung der für den Bankkunden durch die Auslagerung entstehenden Risiken voraus. Dabei hat die Bank neben den mit der Auslagerung verbundenen allgemeinen und anbieterspezifischen

Risiken ggf. auch die spezifischen Auslandsrisiken zu beurteilen. In diesem Zusammenhang spielt u.a. eine Rolle, an welchem Standort CID gespeichert sind oder sein können und von wo aus Zugriffe möglich sind; welche rechtlichen Risiken dem Anbieter im Fall eines Verstosses nach dem auf ihn anwendbaren lokalen Recht drohen; die rechtlichen und faktischen Zugriffsmöglichkeiten lokaler Behörden an den relevanten Standorten und die sich daraus ergebenden Risiken für den Bankkunden; und die durch die Auslagerung ggf. ausgelösten Zugriffsmöglichkeiten von Behörden ausserhalb der Belegenheit der Daten (etwa aufgrund des US CLOUD Act[1]).

12 Zusammenfassend ergibt sich, dass die auslagernde Bank bei einer Offenbarung an einen unbefugten Dritten nur dann zur Rechenschaft gezogen werden kann, wenn sie die gebotene Sorgfalt bei der Auslagerung nicht eingehalten hat und dies kausal dafür war, dass es zu einer unbefugten Offenbarung kam. Dass eine Auslagerung (insbesondere ins Ausland) oder die Gewährung von Zugriffsmöglichkeit zu Gunsten der Hilfsperson das Risiko eines unzulässigen Zugriffs abstrakt erhöht, genügt dabei für sich alleine nicht, eine Fahrlässigkeit der Bank zu begründen.

3. Grundlagen

13 Art. 47 BankG hat folgenden Wortlaut:

> *[1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird bestraft, wer vorsätzlich:*
>
> *a. ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Organ, Angestellter, Beauftragter oder Liquidator einer Bank, als Organ oder Angestellter einer Prüfgesellschaft anvertraut worden ist oder das er in dieser Eigenschaft wahrgenommen hat;*
>
> *b. zu einer solchen Verletzung des Berufsgeheimnisses zu verleiten sucht;*
>
> *c. ein ihm nach Buchstabe a offenbartes Geheimnis weiteren Personen offenbart oder für sich oder einen anderen ausnützt.*
>
> *[1bis] Mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe wird bestraft, wer sich oder einem anderen durch eine Handlung nach Absatz 1 Buchstabe a oder c einen Vermögensvorteil verschafft.*

1 Clarifying Lawful Overseas Use of Data Act, Pub.L. 115–141, www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm.

[2] Wer fahrlässig handelt, wird mit Busse bis zu 250 000 Franken bestraft.

[3] …

[4] Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses oder der Berufsausübung strafbar.

[5] Vorbehalten bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.

[6] Verfolgung und Beurteilung der Handlungen nach dieser Bestimmung obliegen den Kantonen. Die allgemeinen Bestimmungen des Strafgesetzbuches kommen zur Anwendung.

3.1. Schutzrichtung des Bankkundengeheimnisses

14 Im weiteren Verlauf dieses Gutachtens spielt die rechtliche Grundlage des Bankkundengeheimnisses eine Rolle. Dabei stehen sich zwei Konzepte gegenüber:

(a) Das Bankkundengeheimnis sichert die zivilrechtlich begründete Geheimhaltungspflicht der Bank gegenüber ihrem Kunden strafrechtlich ab (Individualschutz);

(b) das Bankkundengeheimnis dient in erster Linie dem öffentlichen Interesse an einem funktionierenden Finanzplatz, mit dem Schutz der Bankkundendaten als tragender Säule (System- oder Funktionsschutz).

15 Diese Unterscheidung hat Auswirkungen auf die Dispositionsfreiheit der Bankkunden in Bezug auf das Bankkundengeheimnis und die Bedeutung des Erwartungshorizonts der Bankkunden. Während eine Bank im ersten Fall die Aufnahme von Geschäftsbeziehungen grundsätzlich von einem Verzicht des Kunden auf das Bankkundengeheimnis abhängig machen kann, sind der Vertragsfreiheit im anderen Fall durch das öffentliche Interesse Grenzen gesetzt. Auch die Risikobetrachtung im Kontext einer Auslagerung ist unterschiedlich. Beim Individualschutz stehen die Erwartungen des Kunden an das Geschäftsgebaren der Bank und die negativen Auswirkungen einer Geheimnisverletzung auf den Kunden im Vordergrund, während beim Systemschutz in erster Linie die negativen Auswirkungen auf den schweizerischen Finanzplatz geprüft werden müssten.

16 Konzeptionell geht die herrschende Ansicht davon aus, dass das Bankkundengeheimnis die zivilrechtlich – d.h. vertraglich und persönlichkeitsrechtlich – begründete Pflicht zur Wahrung des Berufsgeheimnisses absichert.[2] Insofern hat Art. 47 Abs. 1 und 2 BankG in sachlicher Hinsicht keinen weiteren Anwendungsbereich als die Vertraulichkeitspflichten nach Art. 398 Abs. 1 in Verbindung mit Art. 321a Abs. 4 OR und nach Art. 28 des schweizerischen Zivilgesetzbuches (**ZGB**).

17 Diese Auffassung ist nach unserem Dafürhalten richtig. Sie wird durch die Ausführungen der Botschaft von 1970 über die Revision des Bankengesetzes gestützt:[3]

> *Das Bundesgericht hat schon vor der Inkraftsetzung dieses Erlasses die Geheimhaltungspflicht als selbstverständlichen Bestandteil jedes vertraglichen Verhältnisses zwischen der Bank und ihrem Kunden betrachtet. Dessen Preisgabe bedeute eine Verletzung übernommener Vertragspflichten, aber zugleich eine Verletzung des Anspruchs des Kunden auf die Geheimhaltung als eines Ausflusses des Persönlichkeitsrechts. Das Bankgeheimnis ergibt sich somit aus den allgemeinen Bestimmungen des Obligationenrechtes über den Vertrag sowie aus den Artikeln 27 und 28 des Zivilgesetzbuches […].*

18 In die gleiche Richtung – etwas weniger eindeutig – geht die Botschaft zur Banken-Initiative von 1982.[4] 2012 hat sich der Bundesrat ebenfalls dahingehend geäussert, dass das Bankkundengeheimnis zivilrechtlich begründet ist:[5]

> *Die Pflicht zur Wahrung des Bankgeheimnisses hat ihre Wurzel im Privatrecht. […] Schliesslich hat der Gesetzgeber mit Art. 47 des Bankengeset-*

---

2 BSK BankG-*Stratenwerth*, Art. 47 N 1; *Kleiner/Schwob/Winzeler*, Kommentar zum Bundesgesetz über die Banken und Sparkassen, Ausgabe Juli 2015, Art. 47 N 3 ff.; *Bühler*, Vom Bankgeheimnis zum automatischen Informationsaustausch, in: Breitenmoser/Ehrenzeller (Hrsg.), Aktuelle Fragen der internationalen Amts- und Rechtshilfe, 2017, 7; *Winzeler*, Das Schweizer Bankkundengeheimnis im Wandel – Totgesagte leben länger, SJZ 2011, 98; *Althaus Stämpfli*, Kundendaten von Banken und Finanzdienstleistern, 2009, 47; *Margiotta*, Das Bankgeheimnis – Rechtliche Schranke eines bankkonzerninternen Informationsflusses?, 2002, 60; *Rappo*, Le secret bancaire, 2002, Rz. 192, 697; *Brändli*, Outsourcing, 2001, Rz. 453 f.; *Honegger/Frick*, Das Bankgeheimnis im Konzern und bei Übernahmen, SZW 1996, 2; *Fellmann*, Berner Kommentar, Bd. VI/2/4, Der einfache Auftrag, Art. 394-406 OR, 1992, Art. 398 OR N 53.

3 Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes vom 13. Mai 1970, BBl 1970 I 1161.

4 Botschaft über die Volksinitiative „gegen den Missbrauch des Bankgeheimnisses und der Bankenmacht" (Banken-Initiative) vom 18. August 1982, BBl 1982 II 1224.

5 Bericht des Bundesrates „Die Behörden unter dem Druck der Finanzkrise und der Herausgabe von UBS-Kundendaten an die USA" in Erfüllung des Postulates 10.3390 GPK NR / 10.3629 GPK SR vom 30. Mai 2010, 10. Oktober 2012.

> *zes vom 8. November 1934 […] dem Bankkunden im Zusammenhang mit der Geheimhaltung seiner Bankbeziehung zusätzlich einen strafrechtlichen Schutz gewährt. Diese Strafbestimmung schützt das Bankgeheimnis jedoch nur in dem Umfange, wie es durch Vertrag und Persönlichkeitsrecht konkret begründet wurde.*

19 Allerdings lassen sich in den Materialien auch Aussagen finden, die als Hinweise auf einen Systemschutz gelesen werden können, so in der Botschaft von 1934 über den Erlass des Bankengesetzes:[6]

> *Die Tätigkeit der Banken ist so schwierig und vielgestaltig, dass man nicht an eine staatliche Kontrolle denken kann. Die amtliche Kontrolle ist übrigens weder für den Staat noch für die Banken wünschbar. […] Der Eingriff eidgenössischer Kontrolleure hätte auch noch andere Unzukömmlichkeiten zur Folge: Die Bankenkundschaft, die dem Bankgeheimnis grosse Bedeutung beimisst und darauf will zählen können, würde beunruhigt. Die Folge davon wäre wahrscheinlich eine Kapitalflucht der bei unsern Banken angelegten Gelder, ein Schaden, vor dem wir unser Land bewahren müssen.*

20 Im Zusammenhang mit einer von der FDP.Die Liberalen angeregten Verschärfung von Art. 47 BankG, die mit dem Bundesgesetz über die Ausweitung der Strafbarkeit der Verletzung des Berufsgeheimnisses vom 12. Dezember 2014 am 1. Juli 2015 in Kraft getreten ist, wurde sodann deutlich auf das öffentliche Interesse hingewiesen. In seiner Stellungnahme vom 13. August 2014 zum Bericht der zuständigen Kommission hat der Bundesrat festgehalten:[7]

> *Die Verletzung des Bankgeheimnisses durch den Geheimnisträger sowie die Verwendung und die Weitergabe unrechtmässig erworbener Bankkundendaten durch Dritte verletzt die Persönlichkeitsrechte der Bankkundinnen und -kunden. Die genannten Verhaltensweisen können ausserdem dazu führen, dass in- und ausländische Bankkundinnen und -kunden ihr Vertrauen in die betroffene Bank und den Finanzplatz Schweiz verlieren, was sich letztlich negativ auf die Wettbewerbsfähigkeit des Finanzplatzes und auch auf die schweizerische Volkswirtschaft auswirken kann.*

21 Das Bundesgericht hat sich zur Frage bisher nicht eindeutig geäussert. Es gibt aber Aussagen, die sich als Hinweise auf einen Systemschutz verstehen lassen.

---

6 Botschaft des Bundesrates an die Bundesversammlung betreffend den Entwurf eines Bundesgesetzes über die Banken und Sparkassen vom 2. Februar 1934, BBl 1934 I 180.

7 Parlamentarische Initiative „Den Verkauf von Bankkundendaten hart bestrafen", Bericht der Kommission für Wirtschaft und Abgaben des Nationalrates vom 19. Mai 2014 – Stellungnahme des Bundesrates vom 13. August 2014, BBl 2014 6243 f.

So hielt das Bundesgericht in BGE 141 IV 155 E. 4.2.5 fest (wenn auch unter Hinweis auf den Schutz von Geschäftsgeheimnissen der Bank und damit einer ausserhalb des Bankkundengeheimnisses liegenden Thematik):

> *Durch die Übergabe von Daten zahlreicher ausländischer Kunden einer schweizerischen Bank an ausländische Behörden werden nicht nur die Geschäftsgeheimnisse der Kunden, sondern auch die Geschäftsgeheimnisse der Bank betroffen. Das Bankkundengeheimnis, welches Art. 47 des Bankengesetzes […] strafrechtlich schützt, dient nicht nur dem einzelnen Bankkunden. Es hat vielmehr auch institutionelle Bedeutung und schützt die kollektiven Interessen des schweizerischen Finanzplatzes. Diese Interessen werden betroffen, wenn Daten zahlreicher Kunden verraten werden […].*

22 In mehreren Entscheidungen hielt das Bundesgericht sodann im Zusammenhang mit der internationalen Strafrechtshilfe fest,[8] dass wesentliche Interessen der Schweiz i.S. des früheren Art. 1 Abs. 2 und heutigen Art. 1a IRSG betroffen sein können:

> *[…] wenn es sich bei der vom ausländischen Staat verlangten Auskunft um eine solche handelt, deren Preisgabe das Bankgeheimnis geradezu aushöhlen oder der ganzen schweizerischen Wirtschaft Schaden zufügen würde.*

23 Im Zusammenhang mit Art. 273 StGB hat das Bundesgericht im Jahr 1985 die Systemrelevanz des Vertrauens zur Bank ebenfalls betont:[9]

> *Les relations entre les banques et leurs clients dépendent dans une large mesure de la confiance de ces derniers dans la discrétion dont la banque fera preuve à l'égard des faits touchant à la sphère privée du client. Si disparaît la garantie que de tels faits, révélés ou appris, resteront secrets, disparaît du même coup la confiance à cet égard du client envers la banque, et s'effondre ainsi l'une des conditions essentielles d'une activité bancaire viable.*

24 Das Bundesverwaltungsgericht hat das Bankkundengeheimnis in einem Entscheid aus dem Jahr 2010 dagegen eindeutig als dem Individualschutz verpflichtet aufgefasst:[10]

8 Urteil 1A.234/2005 vom 31. Januar 2015, E. 4; so auch BGE 123 II 153 E. 7.b; BGE 115 Ib 68 E. 4.b.

9 BGE 111 IV 74 E. 4.c.

10 Urteil B-1092/2009 vom 5. Januar 2010, E. 4.2.1.

> *Neben der privatrechtlichen Schadenersatzpflicht der Bank soll die Privatsphäre des Bankkunden im Verkehr mit der Bank auch dadurch sichergestellt werden, dass sich mit der Behandlung von Bankkundendaten Betraute strafrechtlich verantworten müssen, wenn sie gegen ihre Geheimhaltungspflichten verstossen. In Bezug auf Bankkundendaten ergibt sich die strafrechtliche Verantwortlichkeit nicht aus dem Berufsgeheimnis gemäss Art. 321 [StGB], sondern aus der Spezialbestimmung von Art. 47 BankG. Es handelt sich hierbei um das strafrechtliche Pendant zu Art. 398 OR […].*

25 In der Literatur findet sich im Anschluss an die Botschaft von 1934 und die genannte Rechtsprechung auch die Auffassung, Art. 47 BankG schütze u.a. den Finanzplatz.[11] Zuletzt haben *Kunz/Zollinger* diese Meinung vertreten.[12] Sie führen dabei das Argument an, dass Art. 47 BankG in einigen Punkten strenger sei als Art. 321 StGB. Die Verletzung von Art. 47 BankG stelle ein Offizialdelikt dar und sei auch bei fahrlässiger Begehung strafbar, und auch die Verbreitung und versuchte Verbreitung sei strafbedroht.

26 Nach unserer Auffassung sind die Argumente dafür, dem Bankkundengeheimnis auch Funktionsschutzzweck zuzubilligen, nicht so gewichtig, dass die herrschende Ansicht aufzugeben wäre. Insbesondere erlaubt der im Vergleich zu Art. 321 StGB stärkere Schutz nicht den Schluss, Art. 47 BankG bezwecke Funktionsschutz:

(a) Dass die Verletzung von Art. 47 BankG als Offizialdelikt ausgestaltet ist, kann damit erklärt werden, dass ausländische Bankkunden die kurze Antragsfrist möglicherweise nicht wahrnehmen könnten.[13] Die Verschärfung des Schutzes lässt sich sodann generell damit begründen, dass spe-

---

11 *Emmenegger/Zbinden,* Die Standards zur Aufhebung des Bankgeheimnisses, in: Emmenegger (Hrsg.), Cross-Border Banking, 2009, 207 f. *„[…] Zudem – und atypisch für das Strafrecht – dient Art. 47 BankG auch dem Funktionsschutz in Gestalt eines öffentlichen Interesses an einem attraktiven Finanzplatz Schweiz“*; *Heine*, Die Verletzung des Bankgeheimnisses: neue Strafbarkeitsrisiken der Bank bei grenzüberschreitenden Sachverhalten, in: Emmenegger (Hrsg.), Cross-Border Banking, 2009, 176 f. *(„Art. 47 BankG beschränkt sich aber nicht auf diesen Schutz individueller Interessen […] Es geht folglich um den Schutz der Institution Bankgeheimnis in ihrer Bedeutung für den Finanzplatz Schweiz“)*; *Berger*, Outsourcing vs. Geheimnisschutz im Bankgeschäft, recht 2000, 185 f. *(„Daraus erhellt, dass das geschützte Rechtsgut des Art. 47 BankG in Wahrheit primär der Funktionsschutz ist“); Graf*, Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext, SJZ 2016, 194, ohne Begründung oder Nachweise *(„Art. 47 BankG [schützt] die Interessen der Bankkunden bzw. des schweizerischen Finanzplatzes“)*; *Tissot-dit-Sanfin*, Beschränkung von grenzüberschreitenden Datenflüssen im Bankbereich, 1991, 56, ohne Begründung und Nachweise (*„in einem untergeordneten Rahmen wird auch der Schutz der Wirtschaft […] bezweckt“*).

12 *Kunz/Zollinger,* Der Schutzbereich von Art. 47 BankG, Jusletter v. 16. April 2018, Rz. 8 ff.

13 So *Kleiner/Schwob/Winzeler,* Art. 47 BankG N 2; *Kunz/Zollinger*, Rz. 11.

zifischen Gefahren für den – immer noch privatrechtlich begründeten – Geheimbereich der Bankkunden begegnet werden sollte, etwa dem Handel mit gestohlenen Daten.

(b) Auch in anderen Bereichen wird die Privatsphäre vermehrt strafrechtlich geschützt, etwa in der Europäischen Datenschutz-Grundverordnung und nach dem Willen des Bundesrats auch im zukünftigen Datenschutzgesetz, und hier wird ebenfalls nicht mit Funktionsschutz argumentiert, sondern mit der gestiegenen Bedrohung der Privatsphäre und dem Bedürfnis nach Abschreckung.

27 Auch aus der zitierten Rechtsprechung ergibt sich nicht hinreichend deutlich, dass das Bankkundengeheimnis Funktionsschutzzweck hat. Es trifft zwar zu, dass eine Aushöhlung des Bankkundengeheimnisses der Wirtschaft Schaden zufügen könnte (dazu vorne Rz. 21). Dies erlaubt aber nicht den Schluss, das Bankkundengeheimnis habe Funktionsschutz. Ein öffentliches Interesses daran, dass schweizerische Rechtsinstitute nicht unterlaufen werden, liegt zwar auf der Hand, sagt aber nichts über den Schutzzweck eines gefährdeten Rechtsinstituts. In diese Richtung sind auch die Urteile zur internationalen Strafrechtshilfe (vorne Rz. 22) zu verstehen. Auch hier dürfte es eher um das grundsätzliche Interesse am Institutionsschutz gehen und weniger um einen vom Bankkundengeheimnis seinerseits verfolgen Schutzzweck. Schliesslich lässt sich auch aus der Erhöhung des Strafrahmens von Art. 47 BankG durch die Schaffung des Bundesgesetzes über die Eidgenössische Finanzmarktaufsicht (**FINMAG**) nicht auf Funktionsschutz schliessen. Zwar ging es bei der Strafmasserhöhung durchaus um System-, Gläubiger- und Anlegerschutz.[14] Dass der Strafrahmen auch bei Art. 47 BankG erhöht wurde, war aber wohl nur der Vereinheitlichung geschuldet.[15] Es ist nicht zu verkennen, dass Individualschutz immer auch dem Systemschutz dient. In diesem Zusammenhang ist es aber bezeichnend, dass sämtliche Stellungnahmen, die dem Bankkundengeheimnis Systemschutzcharakter zuerkennen, die Gefahr einer *massenhaften* Verletzung des Bankkundengeheimnisses im Auge haben. Zu dieser Sichtweise passt das, dass die Sorgfalts- und Kontrollpflichten der Banken nach Grundsatz 9 des Anhangs 3 des FINMA-Rundschreibens 2008/21 – Operationelle Risiken Banken

14 Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz; FINMAG) vom 1. Februar 2006, BBl 2006, 2849.

15 Vgl. ebenfalls die Botschaft zum FINMAG, 2848: *„Der vorliegende Entwurf sieht eine neue, gestraffte und harmonisierte Sanktionenordnung vor, die einerseits aus überarbeiteten Strafbestimmungen und anderseits aus neuen Verwaltungssanktionen besteht. Die Strafbestimmungen werden verwesentlicht und harmonisiert und die Strafrahmen angehoben“.*

(**FINMA-RS 2008/21**) bei Outsourcing-Dienstleistungen und Grossaufträgen in Verbindung mit CID *zwingend* für alle Arten von Aktivitäten gelten, die den Zugriff auf *Massen-CID* beinhalten.[16] Das Bankkundengeheimnis will aber gerade nicht nur Geheimnisverletzungen von grosser Tragweite sanktionieren, sondern jeden einzelnen Fall. Im Ergebnis halten wir die herrschende Auffassung daher nach wie vor für richtig.

3.2. Der Geheimnisbegriff von Art. 47 BankG

28 Art. 47 BankG kennt keinen eigenständigen Geheimnisbegriff, sondern beruht im Grundsatz – aber mit Einschränkungen (s. sogl.) – auf dem einheitlichen strafrechtlichen Verständnis des Geheimnisses.[17] Danach setzt ein Geheimnis kumulativ folgendes voraus:[18]

(a) *Unbekanntheit:* Nur eine relativ unbekannte Information kann ein Geheimnis sein, d.h. eine Information, die weder offenkundig noch allgemein zugänglich ist;

(b) *Geheimniswille:* Der Geheimnisherr hat den Willen, die Kenntnisnahme der geheimen Tatsache auf einen bestimmten Kreis von Personen einzuschränken. Der Geheimniswille muss zudem erkennbar sein, wobei es genügt, wenn er sich aus den Umständen ergibt; und

(c) *Geheimnisinteresse:* Die Geheimhaltung der Tatsache liegt nach objektiven Kriterien in einem schutzwürdigen Interesse des Geheimnisherrn.

29 Das dritte Tatbestandselement gilt bei Art. 47 BankG allerdings nicht uneingeschränkt. Da das strafrechtliche Bankkundengeheimnis privatrechtlich begründet ist (vorne Rz. 14 ff.) und das Privatrecht nicht den Schutz objektiver Geheimnisse bezweckt, sondern allgemein der Verschwiegenheit,[19] kann nicht

---

16 FINMA RS 2008/21, Anhang 3, Rz. 47. Unter „Massen-CID" ist dabei eine Menge von CID zu verstehen, die im Vergleich zur Gesamtzahl der Konten/Gesamtgrösse des Privatkundenportfolios bedeutend ist.

17 BSK BankG-*Stratenwerth*, Art. 47 N 12; *Schwarz,* Geheimnisschutz- und Spionagestrafrecht, in: Jürg-Beat Ackermann/Günter Heine (Hrsg.), Wirtschaftsstrafrecht der Schweiz, § 19 Rz. 34 und 72.

18 *Schwarz*, § 19 Rz. 35.

19 Vgl. etwa *Fellmann*, Art. 398 N 53 *(„[…] Bei der vertraglichen Schweigepflicht geht es demgegenüber […] nicht primär um die Wahrung, von Geheimnissen, sondern generell um Verschwiegenheit […]. Entscheidend ist hier nicht, was objektiv geheimhaltungswürdig ist; massgebend ist vielmehr allein das Geheimhaltungsinteresse des Auftraggebers, wie es für den Beauftragten erkennbar war bzw. nach den Umständen erkennbar sein musste")*.

massgebend sein, was objektiv geheimhaltungswürdig ist. Entscheidend ist daher allein das Geheimhaltungsinteresse des Kunden, sofern die Berufung auf das Geheimnis nicht ausnahmsweise rechtsmissbräuchlich ist.[20]

30 Nicht von Art. 47 BankG geschützt sind anonyme Informationen, d.h. Informationen, die sich keiner natürlichen oder juristischen Person zuordnen lassen.[21] Dabei ist nach schweizerischem Recht auf die datenschutzrechtlichen Kriterien zum Personenbezug zurückzugreifen. Bankkundendaten sind somit alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG), wobei das Bundesgericht das Kriterium der Bestimmtheit wie folgt umschreibt:[22]

> *Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor […]. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat […].*

31 Anonym sind Informationen daher dann, wenn unter Berücksichtigung aller Umstände, insbesondere auch der technischen Möglichkeiten und des Interesses an einer Kenntnisnahme der dem Bankkundengeheimnis unterstehenden Informationen, nach allgemeiner Lebenserfahrung nicht mit der Möglichkeit einer Kenntnisnahme zu rechnen ist.[23] Keine Bekanntgabe von CID liegt danach

---

20 *Margiotta*, 38; *Michlig*, Bankgeheimnisverletzung (Art. 47 BankG) unter dem Aspekt der Lieferung von Personendaten ans U.S. Department of Justice, AJP 2014, 1059.

21 Vgl. das Urteil des Handelsgerichts Zürich HG150170 vom 30. Mai 2017, E. 5.3.5.1.

22 BGE 136 II 508 – Logistep, E. 3.2.

23 Vgl. dazu das Urteil des Handelsgerichts Zürich HG150170 vom 30. Mai 2017, E. 5.3.5.2 *(„Anonymisierung bedeutet, dass der Personenbezug irreversibel so aufgehoben wird, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind. Anders als bei der Pseudonymisierung darf kein Schlüssel (Zuordnungsregel) aufbewahrt werden, der die Re-Identifikation der betroffenen Person ermöglicht. Um eine Re-Identifikation auszuschliessen, reicht es vielfach nicht aus, klar identifizierende Merkmale wie Vorname, Name, Geburtsdatum und Adresse zu entfernen. Bei einer Pseudonymisierung soll der Personenbezug aufgehoben werden, aber bloss reversibel. Der Schlüssel zur Re-Personifizierung der Informationen bleibt erhalten. Deshalb bleiben pseudonymisierte Personendaten für alle, die Zugang zum Schlüssel haben, weiterhin Personendaten. Einzig für Aussenstehende, welche die pseudonymisierten Daten ohne Schlüssel ausgehändigt erhalten haben und die konkret auch keinen Zugang zum Schlüssel haben, sind pseudonymisierte Personendaten wie anonymisierte keine Personendaten mehr.“)*.

jedenfalls dann vor, wenn die Kenntnisnahme von CID unmöglich ist, etwa wenn die betreffenden Informationen anonymisiert oder so pseudonymisiert oder verschlüsselt werden, dass der Empfänger den Personenbezug nicht herstellen kann (vgl. Rz. 41 des Leitfadens; vgl. auch das FINMA-RS 2008/21, Anhang 3, Rz. 65).

3.3. Der Begriff der Offenbarung

32 Art. 47 Abs. 1 BankG verbietet die „Offenbarung" eines anvertrauten oder wahrgenommenen Geheimnisses. Der Begriff der Offenbarung wird dabei nicht definiert. Auszugehen ist von einem allgemeinen, strafrechtlichen Offenbarungsbegriff. Die Offenbarung bezieht sich dabei stets auf einen unbefugten Dritten, d.h. eine vom Geheimnisherrn und vom Geheimnisträger oder deren Angestellten und Hilfspersonen unterschiedene Person[24] (zum Beizug von Hilfspersonen hinten Rz. 47 ff.), was sich ohne weiteres aus dem Wortlaut von Art. 47 Abs. 1 lit. a BankG ergibt.

33 Als Offenbarung galt nach der bisherigen Rechtsprechung[25] bereits die Einräumung der Möglichkeit der Kenntnisnahme und nicht erst die tatsächliche Kenntnisnahme durch einen Dritten. Im Urteil 6B_1403/2017 ist das Bundesgericht von dieser Rechtsprechung allerdings ausdrücklich abgerückt; erforderlich sei die tatsächliche Kenntnisnahme durch den Dritten:[26]

> *Nach Art. 162 StGB macht sich unter anderem strafbar, wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät. Die Tathandlung ist dieselbe wie bei den Tatbeständen der Verletzung des Amtsgeheimnisses (Art. 320*

---

24 Vgl. *Schwarz*, § 19 Rz. 77 f. *(„Entscheidend ist also, dass vom Bankgeheimnis geschützte Informationen an Aussenstehende offenbart werden. Dies bietet keine Probleme, wenn der Geheimnisträger Informationen an weder mit der Bank noch mit dem Kunden in irgendeiner Art verbundene Dritte oder gar an die Öffentlichkeit gibt").*

25 So das Urteil des Bundesstrafgerichts vom 10. Dezember 2013, SK.2013.37, E. 3.2.1 betr. Art. 321 und 162 StGB *(„Umstritten ist, ob die Tat bereits mit der Einräumung der Möglichkeit der Kenntnisnahme des Geheimnisses an Dritte vollendet wird […] oder erst mit der Kenntnisnahme durch den Geheimnisempfänger […]. […] Aufschlussreich ist indessen die bundesgerichtliche Rechtsprechung zu Art. 321 StGB […]. […] Laut Bundesgericht umfasst der Begriff des Offenbarens im Sinne von Art. 321 StGB jede Art der Bekanntgabe des Geheimnisses, insbesondere auch die Aushändigung von Schriftstücken oder anderen Sachen, die das Geheimnis verraten […]. Eine Kenntnisnahme des Geheimnisses durch den Empfänger ist demnach für die Tatvollendung im Rahmen von Art. 321 StGB nicht erforderlich. Für Art. 162 al. 1 StGB kann nichts anderes gelten")*; bestätigt u.a. durch das Bundesstrafgericht im Urteil vom 4. April 2018, SK.2017.52; so auch BGE 142 IV 65 E. 5.1 *(„Ein Geheimnis offenbart, wer es einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme zumindest ermöglicht").*

26 Urteil 6B_1403/2017 vom 8. August 2017, E.1.2.2, SJZ 2018, 453.

> *StGB) oder des Berufsgeheimnisses (Art. 321 StGB). 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 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 […]. 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.*

34 Folgt man dieser Rechtsprechung auch für Art. 47 Abs. 1 und 2 BankG, genügt bspw. ein unsorgfältiges Aufbewahren von Daten nicht für eine Offenbarung, solange der Mangel an Sorgfalt nicht zu einer effektiven Kenntnisnahme der Daten durch einen Unbefugten führt. Zu diesem Ergebnis kommen auch *Schwarzenegger, Thouvenin*, *Stiller* und *George* auf Basis ihres Gutachtens zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte.[27] Sie halten im Anschluss an das genannte Urteil fest, es handle sich bei Art. 321 StGB um ein Erfolgs-, nicht um ein Tätigkeitsdelikt.

35 Die ältere Literatur ist überwiegend der Ansicht, es genüge bereits die Möglichkeit der Kenntnisnahme.[28] Auch die frühere Rechtsprechung hat sich in dieser Richtung geäussert, etwa das Obergericht Zürich in einem Urteil von 2017:[29]

> *[g]eheimzuhaltende Tatsachen zu offenbaren, bedeutet sodann, sie Unberufenen zugänglich zu machen.*

36 Ebenso hat sich das Bundesstrafgericht zuletzt 2013 geäussert.[30]

---

27 Vgl. *Schwarzenegger/Thouvenin/Stiller/George*, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, AnwaltsRevue 2019, 25 ff. Das Gutachten wurde im Auftrag des Schweizerischen Anwaltsverbands im November 2018 erstattet. Es ist bisher nicht veröffentlicht, liegt den Autoren aber vor und soll in der Reihe des Center for Information Technology, Society, and Law (ITSL) der Universität Zürich publiziert werden.

28 Etwa BSK-*Stratenwerth*, Art. 47 N 15; *Schwarz*, § 19 Rz. 76; *Jositsch/Conte*, Bankgeheimnisverletzung durch Whistleblowing, SJZ 2017, 360; *Stratenwerth/Bommer*, Schweizerisches Strafrecht BT II, 7. Aufl. 2013, § 61 Rz. 7 und 19 („nach allgemeiner Auffassung"); **anders** (Kenntnisnahme für die Tatvollendung erforderlich) *Dupuis, Moreillon et al.*, Petit Commentaire Code Pénal, 2. Aufl. 2017, Art. 320 StGB N 29 und Art. 321 StGB N 33.

29 Urteil SB160259 vom 16. August 2017, E. 6.1.1.

37 Diese Urteile und Lehrmeinungen sind allerdings älteren Datums als das erwähnte Urteil des Bundesgerichts. Es bestehen zudem keine Anhaltspunkte dafür, dass die strafbare Offenbarungshandlung je nach Geheimnis unterschiedlich zu verstehen ist. Es ist vielmehr von einem einheitlichen Begriff des Offenbarens auszugehen. Die Offenbarung i.S.v. Art. 47 Abs. 1 und 2 BankG ist demnach erst mit der tatsächlichen Kenntnisnahme des Geheimnisses durch einen Unbefugten vollendet. Bei einer (eventual-)vorsätzlichen Bekanntgabe ohne Kenntnisnahme käme demnach höchstens ein nach Art. 22 i.V.m. Art. 333 StGB strafbarer Versuch in Frage (vgl. dazu sogl., Rz. 39 f.). [31]

38 Als Zwischenergebnis ergibt sich folgendes:

(a) Eine erlaubte Bekanntgabe von CID (z.B. an eine befugterweise beigezogene Hilfsperson) stellt keine tatbestandsmässige Offenbarung dar, und zwar auch wenn sich diese Hilfsperson im Ausland befindet;

(b) eine Bekanntgabe von CID stellt auch dann keine tatbestandsmässige Offenbarung dar, wenn die betreffenden Daten für den Empfänger zuverlässig keinen Personenbezug darstellen, z.B. weil sie anonymisiert oder so pseudonymisiert sind, dass sie der Empfänger keiner Person zuordnen kann;

(c) eine Bekanntgabe von CID stellt schliesslich auch dann keine tatbestandsmässige Offenbarung dar, wenn sie nicht dazu führt, dass ein unbefugter Dritter von den betreffenden CID tatsächlich Kenntnis nimmt. Das kann selbst im Fall einer unsorgfältigen Aufbewahrung von CID zutreffen, wenn die Unsorgfalt folgenlos bleibt. In diesem Fall kann aber, bei entsprechendem (Eventual-)Vorsatz, ein strafbarer Versuch der Offenbarung vorliegen.

3.4. Subjektiver Tatbestand

39 In subjektiver Hinsicht setzen Art. 47 Abs. 1 und 2 BankG Vorsatz oder Fahrlässigkeit voraus:

---

30 Urteil SK.2013.37 vom 10. Dezember 2013, E. 3.3.2 c, forumpoenale 6/2014, 332 (Zustellung eines Datenträgers genügt).

31 Dazu BSK-*Niggli/Maeder*, Art. 22 StGB N 2.

(a) Im Fall des Vorsatzdelikts muss sich der Vorsatz auf alle objektiven Tatbestandselemente beziehen,[32] d.h. auch auf die unbefugte Kenntnisnahme der CID (vgl. vorne Rz. 32 ff.);

(b) bei fahrlässiger Bankgeheimnisverletzung muss eine Verletzung der Sorgfalt, zu der die Bank nach den Umständen verpflichtet ist (Art. 12 Abs. 3 StGB), kausal zur unbefugten Offenbarung geführt haben (zur Konkretisierung vgl. hinten Rz. 65 ff.).

40 Demnach stellt eine Bekanntgabe von CID keine tatbestandsmässige Offenbarung dar, wenn die Bank weder vorsätzlich noch fahrlässig handelt, selbst wenn es in der Folge (dennoch) zu einer Kenntnisnahme durch einen Unbefugten kommt. Dabei ist konkret zu prüfen, ob eine Sorgfaltspflichtverletzung überhaupt der Bank zuzurechnen ist, denn auch bei einer sorgfältigen Auslagerung lässt sich nicht ausschliessen, dass der Hilfsperson ein Fehler unterläuft. Insbesondere ist konkret zu prüfen, wem die konkret verletzte Sorgfaltspflicht (gemäss der zulässigerweise vorgenommen Rollenverteilung zwischen Bank und Hilfsperson) überhaupt oblag, denn nur diese Person kann die Pflicht überhaupt verletzt und damit fahrlässig gehandelt haben. Typischerweise beschränkt sich dabei das Pflichtenprogramm der Bank auf die Auswahl-, Instruktions- und Überwachungspflichten, welche sie gemäss den einschlägigen Bestimmungen bzw. Usanzen einzuhalten hat. Hat die Bank diese Pflichten erfüllt, darf ihr die Verletzung einer an die Hilfsperson delegierten Pflicht nicht als fahrlässiges Handeln vorgeworfen werden.

41 Hinzu kommt, dass nur die Schaffung eines *unerlaubten* Risikos eine Fahrlässigkeit zu begründen vermag.[33] Dass eine Tätigkeit (z.B. die Auslagerung von Datenverarbeitungen) generell mit vorhersehbaren Gefahren für Rechtsgüter verbunden ist, welche sich auch bei Einhaltung der gebotenen Sorgfalt nicht ausschliessen lassen, ist hinzunehmen (ausser der Gesetzgeber hätte die entsprechende Tätigkeit *per se* verboten, was vorliegend gerade nicht der Fall ist). Entsprechend darf aus der Verwirklichung von Restrisiken allein nicht auf eine Sorgfaltspflichtverletzung geschlossen werden.

42 Ein strafbarer Versuch einer Offenbarung ist sodann nur bei Vorsatz denkbar,[34] d.h. dann, wenn die Bank will oder zumindest im Sinne des Eventualvorsatzes in

32 *Donatsch/Tag*, Strafrecht I – Verbrechenslehre, 9. Aufl. 2013, 112.

33 BSK StGB-*Niggli/Maeder*, Art. 12 StGB N 98.

34 BSK StGB-*Niggli/Maeder*, Art. 22 StGB N 1 und 2.

Kauf nimmt, dass CID durch einen Unbefugten zur Kenntnis genommen werden, sich dieser Erfolg dann aber nicht verwirklicht.

3.5. Strafbarkeit der Tatbegehung im Ausland

43 Grundsätzlich ist das StGB in räumlicher Hinsicht anwendbar auf Taten, die in der Schweiz begangen werden (Art. 3 Abs. 1 StGB; Territorialitätsprinzip), wobei der Begehungsort nach Art. 8 Abs. 1 StGB den Erfolgs- und den Handlungsort umfasst (Ubiquitätsprinzip). Der Handlungsort liegt zunächst da, wo das objektiv tatbestandsmässige Verhalten ausgeführt wird, bei der unbefugten Offenbarung also da, wo diese Offenbarung stattfindet. Gibt eine schweizerische Bank CID unerlaubterweise bekannt, liegt der Handlungsort demnach in der Schweiz; und offenbart ein im Ausland ansässiger Dienstleister CID unbefugterweise, liegt er im betreffenden Ausland.

44 Der Erfolgsort liegt sodann da, wo der Taterfolg eintritt.[35] Folgt man der bundesgerichtlichen Rechtsprechung, wonach der Tatbestand der Geheimnisverletzung die Kenntnisnahme des Geheimnisses voraussetzt (vgl. vorne Rz. 32 ff.), kann der Erfolg nur dort liegen, wo sich diese Kenntnisnahme verwirklicht, d.h. dort, wo sich der unbefugte Empfänger der Information beim Informationsempfang befindet.

45 Übermittelt eine Bank also befugterweise CID an einen Dienstleister im Ausland und bringt dieser CID verbotenerweise einem Dritten im Ausland (z.B. einer ausländischen Behörde) zur Kenntnis, liegt der Erfolgsort im betreffenden Ausland. In dieser Konstellation fehlen mit Bezug auf den Dienstleister sowohl ein Handlungs- als auch ein Erfolgsort in der Schweiz. Hier hängt seine Strafbarkeit daher u.a. davon ab, ob die Voraussetzungen von Art. 7 StGB erfüllt sind, d.h. ob die Offenbarung auch am ausländischen Begehungsort strafbar ist.

46 Für die Bank liegt in dieser Konstellation demgegenüber ein Handlungsort in der Schweiz vor,[36] sofern sie eine ihr obliegende Sorgfaltspflicht (dazu vorne Rz. 40) verletzt und den Erfolg dadurch kausal mitverursacht hat, so dass für sie diesfalls ein Strafbarkeitsrisiko besteht.

35 Dazu *Gless*, Internationales Strafrecht, 2. Aufl. 2015, Rz. 149 ff.

36 Es genügt, dass der Tatbestand nur teilweise auf schweizerischem Boden erfüllt wird; vgl. dazu das Urteil 6B_86/2009 vom 29. Oktober 2009, E. 2.3.

4. Zur Zulässigkeit einer Auslagerung von CID an einen Dienstleister

47 Strafbar ist nur die Offenbarung gegenüber einem Unbefugten, was Art. 47 Abs. 1 BankG nicht ausdrücklich erwähnt, sich aber von selbst versteht. In diesem Zusammenhang stellt sich die Frage, ob und unter welchen Umständen ein Geheimnis einer Hilfsperson anvertraut werden darf.

4.1. Zulässigkeit einer Auslagerung an Hilfspersonen

48 Fraglos zulässig ist eine Auslagerung von CID,[37] die dem Bankkundengeheimnis unterfallen, wenn es dabei nicht zu einer Bekanntgabe kommt, d.h. wenn der Dienstleister von den CID keine Kenntnis erlangt. Das ist in praktischer Hinsicht allerdings nur bei Speicherlösungen denkbar, wenn die Hilfsperson verschlüsselte Daten erhält und diese Daten nicht entschlüsseln kann.

49 In Bezug auf die Bekanntgabe von unverschlüsselten CID (oder von verschlüsselten CID, bei welchen die Hilfsperson generell oder unter bestimmten Umständen zugreifen darf), wird teilweise, insbesondere von *Wohlers*, die Auffassung vertreten, die Auslagerung von CID setze eine Einwilligung des betreffenden Bankkunden voraus.[38] Dieser Auffassung ist zunächst entgegenzuhalten, dass der Beizug einer Hilfsperson in vielen Konstellationen unumgänglich ist und auch den Interessen des Bankkunden dient. *Wohlers* Auffassung ist damit zuerst einmal praxisfremd. Sie widerspricht aber auch der Haltung des Bundesrats, der eine Auslagerung bestimmter Leistungen an Beauftragte unter Bekanntgabe von CID schon vor Jahrzehnten als zulässig ansah. Die „Beauftragten" der Bank wurden bei der Revision des Bankengesetzes 1971 in den Kreis der Personen aufgenommen, die der Schweigepflicht nach Art. 47 Abs. 1 BankG unterliegen. Die Botschaft von 1970[39] hält dazu fest:

> *Mit der Unterstellung des Beauftragten sollen insbesondere auch Rechenzentren erfasst werden, die von Banken mit der elektronischen Datenverarbeitung betraut werden.*

50 Daraus geht hervor, dass die Auslagerung von CID an Beauftragte bspw. im IT-Bereich nach dem Willen des Bundesrats grundsätzlich zulässig ist. Auch das

37 „Auslagerung" wird hier mehr oder weniger synonym mit „Bekanntgabe" verwendet.

38 *Wohlers*, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), 2016, passim; *ders.*, Outsourcing durch Berufsgeheimnisträger, digma 2016 , passim.

39 Botschaft über die Revision des Bankengesetzes vom 13. Mai 1970, BBl 1970 I, 1182.

Bundesamt für Justiz ist in einer nicht öffentlichen Stellungnahme vom 21. Juni 1999 zur Auffassung gelangt, ein Outsourcing der Rechnungstellung und der IT-Leistungen durch Ärzte sei auch ohne Einwilligung der Patienten zulässig.[40]

51 Die Rechtsprechung geht ebenfalls davon aus, dass eine Auslagerung durch Banken im Grundsatz erlaubt ist. Das Bundesgericht hat in BGE 121 IV 45 (E. 2.a) etwa festgehalten:

> *Es entspricht einer Übung, dass auch juristische Personen mit eigenem Rechtsdienst, wie Versicherungen und Banken, Anwälte im Mandatsverhältnis beiziehen, wenn es um die Führung von Prozessen geht, nicht zuletzt deshalb, um von der forensischen Erfahrung der Anwälte zu profitieren. Dies erscheint zulässig, unter Umständen sogar geboten […].*

52 Das Zürcher Obergericht hat in einem Entscheid von 2015 festgehalten:[41]

> *[…] Im Urteil BGE 121 IV 45 E. 2b erachtete das Bundesgericht den Beizug von Anwälten durch eine Bank als Übung, wenn es um die Führung von Prozessen gehe. Die Bank profitiere von der forensischen Erfahrung der Anwälte, auch wenn sie über einen eigenen Rechtsdienst verfüge. Das scheine zulässig, unter Umständen sogar geboten. Daraus kann abgeleitet werden, dass der übungsgemässe Beizug von Anwälten offenbar nicht geradezu zwingend geboten sein muss, um zulässig zu sein. […]*

53 Das Kantonsgericht Luzern hat 2016 sogar Folgendes ausgeführt:[42]

> *Die Ausgestaltung der Beziehung zwischen der Bank und ihren Kunden (der Kundenbeziehung) stellt auf dem Finanzdienstleistungsmarkt ein erheblicher Wettbewerbsfaktor dar. Dementsprechend haben die Banken an einer Optimierung der Kundenbeziehungen ein starkes Interesse. Letzten Endes profitieren auch die Kunden davon. Die Erforschung der Kundenbedürfnisse entspricht damit fraglos einem ernstzunehmenden Interesse der Bank D AG, was zur Folge hat, dass die Beauftragung eines professionellen Marktforschungsinstituts – auch wenn der Kreis der Beauftragten im Sinne von Art. 47 Abs. 1 lit. a BankG eng auszulegen ist – in diesem Bereich möglich bleiben muss.*

54 Auch für andere Berufsgeheimnisse hat die Rechtsprechung eine Auslagerung als zulässig angesehen. So hat das Bezirksgericht Zürich festgehalten, der Beizug

40 *Casanova*, Datenverknüpfung in ausgewählten Bereichen: Gesundheitswesen, in: Epiney/Probst/Gammenthaler (Hrsg.), Datenverknüpfung – Problematik und rechtlicher Rahmen, Zürich 2011, 48.

41 Urteil vom 9. Juli 2015, Geschäfts-Nr. UE140317, E. 6.4.

42 Urteil vom 7. Dezember 2016, LGVE 2016 I Nr. 21, E. 6.4.

eines „Schreibbüros“ durch einen Arzt sei zulässig, weil das Schreibbüro als Hilfsperson zu qualifizieren sei.[43]

55 Die Literatur hat sich ebenfalls gegen *Wohlers* gewandt, soweit sie sich dazu geäussert hat.[44]

56 Aus all dem ist zu schliessen, dass die Auslagerung im Grundsatz zulässig sein muss, und zwar selbst dann, wenn die Hilfsperson dabei generell oder unter bestimmten Voraussetzungen Zugang zu den unverschlüsselten Daten erhalten kann. Eine eigentliche Notwendigkeit der Auslagerung ist dabei nicht zu verlangen. Die Rechtsprechung hat bei den beurteilten Fällen jeweils auch eine entsprechende Übung oder ein Interesse an der Optimierung der Kundenbeziehung genügen lassen. Auch die Literatur geht mehrheitlich davon aus, dass eine Auslagerung ohne Einwilligung des Bankkunden erlaubt ist, wenn sie angezeigt ist.[45] Einschränkend wird von diesen Stimmen in Übereinstimmung mit der genannten Rechtsprechung aber verlangt, dass die Auslagerung:

(a) *„einem ernsthaften Interesse an der Optimierung ihrer Leistungen oder an der Senkung ihrer Kosten entspricht“*;[46]

(b) *„aus Gründen der Arbeitsteilung und Kosteneffizienz“*,[47] z.B. beim *„Beizug von […] Softwareentwicklern“*.[48]

57 Diese Einschränkungen sind u.E. allerdings zu eng. Obligationenrechtlich ist nach Art. 68 OR von der grundsätzlichen – aber dispositiven – Zulässigkeit der Auslagerung an Hilfspersonen auszugehen:[49]

43 Urteil GG150233-L vom 18. November 2015, E. 2.5.

44 So *Chappuis/Alberini*, Secret professionnel de l’avocat et solutions cloud, AnwaltsRevue 2017, 337 ff.; *Thouvenin/Schwarzenegger/Stiller/George*, 26 ff.; *Trüeb/Zobl,* Steuerdaten in der Cloud, digma 2016, 105.

45 So BSK-*Stratenwerth*, Art. 47 BankG N 7; *Stocker*, Regulatorische Anforderungen an IT-Outsourcing: Finanzmarktbereich, in: Weber/Berger/Auf der Maur (Hrsg.), IT-Outsourcing, 2003, 250 f. (bei „Vorliegen einer gewissen Notwendigkeit“). **Anders** *Althaus Stämpfli*, 224, die ein Outsourcing ohne Einwilligung aus Kostenerwägungen der Bank ablehnt; *Berger*, 191, wonach ein rein finanzielles Interesse der Bank am Outsourcing nicht genügt und generell nicht auszumachen ist, welches Interesse der Bank am Outsourcing das Interesse des Kunden am Schutz seiner Geheimsphäre überwiegen könnte; *Aubert/Béguin/Bernasconi/Graziano-von Burg/Schwob/Treuillaud*, 103, wonach eine Auslagerung nur zulässig ist, soweit eine Bank nicht in der Lage ist, die betreffende Tätigkeit selbst auszuführen, was mit Zurückhaltung anzunehmen sei.

46 BSK-*Stratenwerth*, Art. 47 BankG N 7.

47 *Honegger/Frick*, 6; *Brändli*, Rz. 457.

48 *Honegger/Frick*, 6.

> *Dieser Grundsatz ist eine Voraussetzung einer arbeitsteiligen Gesellschaft; Art. 68 ist deshalb materielle Basis zahlreicher schuldrechtlicher Institute, z.B. des Wechsels und des Checks […] sowie des Arbeitsvertrages […], denn bestünde Art. 68 nicht in der vorliegenden Weise, müsste der Schuldner regelmässig persönlich leisten und dürfte die Arbeitslast nicht mittels Anstellung von Hilfskräften (Arbeitnehmer) verteilen. Art. 68 bringt insoweit einen wichtigen Beitrag zu einer – ökonomisch betrachtet – effizienteren Wirtschaft.*

58 Dies gilt auch für Banktätigkeiten. Aus Art. 398 Abs. 3 OR folgt zwar, dass eine „Übertragung" (d.h. Substitution) des Auftrags unzulässig ist, aber das bedeutet nicht, dass jeder Beizug eines Dritten ausgeschlossen ist. Der Beizug von Hilfspersonen im Sinne von Art. 101 OR bleibt – im Gegensatz zur Übertragung der Hauptleistungspflichten eines Auftrags (Substitution) – vielmehr weitgehend statthaft.[50] So bleibt bspw. sogar ein persönlich leistungspflichtiger Chirurg berechtigt, eine „Narkoseschwester" beizuziehen, *„solange das materielle Hauptgewicht auf seiner Leistung liegt"*, wobei *„je nach den konkreten Umständen […] auch die Aufsicht und Kontrolle durch den Schuldner [genügt]"*.[51] (Auch) für Banken ist demnach davon auszugehen, dass eine Auslagerung an Hilfspersonen zivilrechtlich zulässig ist, sofern:

(a) die Auslagerung einem vernünftigen Interesse der auslagernden Bank entspricht;

(b) die Auslagerung als Beizug einer Hilfsperson zu verstehen ist, d.h. die Tätigkeit der Hilfsperson die Geschäftstätigkeit der Bank unterstützt und ihrer Weisungsbefugnis untersteht; und

(c) die Bank die mit dem Bankkunden vereinbarten Leistungen insgesamt im Schwergewicht selbst erbringt.

59 Solange diese Bedingungen erfüllt sind, ist der Beizug als solcher nicht nur vertragsrechtlich zulässig (eine abweichende Vereinbarung vorbehalten), sondern verletzt auch nicht den persönlichkeitsrechtlichen Geheimnisschutz.[52] Es ist

---

49 *Weber*, in: Berner Kommentar Band/Nr. VI/1/4, Die Erfüllung der Obligation, Art. 68-96 OR, 2. Aufl. 2005, Art. 68 OR N 5.

50 *Bühler*, in: OFK OR, 3. Aufl. 2016, Art. 398 OR N 9; *Thionnet-Chevrier/Falletti/Bizzozero*, Le mandat de gestion de fortune, 2. Aufl. 2017, 131.

51 So BK-*Weber*, Art. 68 OR N 32.

52 Verletzt die Bank im Zusammenhang mit dem Beizug eine Auflage des Datenschutzrechts, bspw. eine etwaige Transparenzpflicht, wird dieser Verstoss nach Art. 12 Abs. 1 DSG zwar als Persönlichkeitsverletzung fingiert, aber

weiter davon auszugehen, dass das Bankkundengeheimnis lediglich die zivilrechtlich begründete Geheimhaltungspflicht strafrechtlich verstärkt (dazu vorne Rz. 14 ff.), weshalb in strafrechtlicher Hinsicht nichts anderes gelten kann als nach Art. 68 OR, zumal Art. 47 Abs. 1 BankG den Begriff des „Beauftragten" verwendet, den Kreis der Beauftragten aber nicht beschränkt.

60 Beim zulässigen Beizug besteht keine Obliegenheit, dass sich die Bank einzelfallweise durch einen „Waiver" oder generell vom Bankkundengeheimnis entbinden lässt.[53] Nicht die Geheimnisverletzung wird gerechtfertigt; vielmehr entfällt bereits der Tatbestand der unerlaubten Offenbarung.

61 Dies steht allerdings unter dem Vorbehalt, dass nicht aus einer – ausdrücklich oder stillschweigend getroffenen – Abrede folgt, dass der Beizug unzulässig ist. Sieht eine vertragliche Vereinbarung ein Verbot einer Bekanntgabe von CID ins Ausland vor, ist die Einhaltung dieser Vereinbarung durch Art. 47 Abs. 1 und 2 BankG auch strafrechtlich abgesichert. Eine Bekanntgabe ins Ausland setzt in diesem Fall eine vorgängige Einwilligung des Kunden für den konkreten Fall („Waiver") oder die vorgängige Änderung der entsprechenden Vertragsbestimmung voraus. Bei der Frage, ob ein Ausschluss der Auslandsbekanntgabe vereinbart wurde, sind nicht nur etwaige ausdrückliche Abreden der Bank mit dem Bankkunden zu beachten (z.B. entsprechende Bestimmungen in AGB), sondern auch alle weiteren Umstände, die insgesamt auf eine entsprechende Selbstverpflichtung der Bank (die nach Art. 6 OR stillschweigend angenommen werden kann) schliessen lassen sowie das Auftreten und die Marktpositionierung der Bank, ihre Datenschutzerklärungen und bis zu einem gewissen Grad die Branchenpraxis.

4.2. Zulässigkeit einer Auslagerung ins Ausland

62 Art. 47 Abs. 1 BankG verbietet auch eine Datenauslagerung ins Ausland nicht *expressis verbis*. Auch die Materialien enthalten keinen Hinweis auf eine entsprechende Strafbarkeit. In der Literatur findet sich aber die Auffassung, eine Auslagerung von CID ins Ausland führe dazu, dass der strafrechtliche Schutz des Bankkundengeheimnisses rechtlich (vgl. dazu vorne Rz. 43 ff.) oder faktisch entfalle und der Bankkunde davon ausgehen dürfe, dass eine Verletzung der Ge-

---

daraus lässt sich nicht ableiten, dass dieser den Beizug der Hilfsperson begleitende Verstoss die Offenbarung als solche unzulässig macht.

53 Fragen der datenschutzrechtlich ggf. geforderten Transparenz sind nicht Gegenstand dieses Gutachtens.

heimnispflicht strafrechtliche Sanktionen nach sich ziehe. Demnach verlange die Auslagerung ins Ausland eine Einwilligung.[54]

63 Für diese Auffassung spricht zwar die Tatsache, dass Art. 47 Abs. 1 und 2 BankG Geheimnisverletzungen mit Strafe bedrohen. Offenbar hielt es der Gesetzgeber zum Schutz des Bankkunden für erforderlich, die Geheimnisträger einer Strafdrohung zu unterstellen. Diese gesetzgeberische Wertung kann nicht gleichgültig sein, zumal die Strafdrohung in jüngerer Zeit noch verschärft wurde (vorne Rz. 20). Gleichwohl ist der Schluss, die Auslagerung an einen Beauftragten im Ausland sei unterschiedslos verboten, zu undifferenziert. Zum einen findet sich dafür keine klare Stütze in Art. 47 BankG, so dass die Bekanntgabe an einen Dienstleister im Ausland schon aufgrund des Legalitätsprinzips (Art. 1 StGB) nicht grundsätzlich ausgeschlossen sein kann. Zum anderen müssen auch bei der Auslandsbekanntgabe die Überlegungen den Ausschlag geben, die auch bei der Auslagerung an einen Dienstleister in der Schweiz massgeblich sind (dazu vorne Rz. 47 ff.). Auszugehen ist daher von der grundsätzlichen Zulässigkeit des Beizugs eines Dienstleisters auch im Ausland. Dabei hat die Bank wiederum die nach den Umständen gebotene Sorgfalt einzuhalten, was bei einer Bekanntgabe ins Ausland zusätzliche Fragen aufwirft (dazu sogl., Rz. 65 ff.).

4.3. Ergebnis

64 Die Bank darf CID einem Dienstleister übermitteln, sofern der Beizug einem vernünftigen Interesse der Bank entspricht und keiner Vereinbarung mit dem Bankkunden widerspricht. Das gilt grundsätzlich auch beim Beizug eines Dienstleisters im Ausland. Dabei ist nicht erforderlich, dass die CID so verschlüsselt werden, dass der Dienstleister von den CID keine Kenntnis nehmen kann. Strafbar i.S.v. Art. 47 Abs. 1 und 2 BankG macht sich die Bank nur dann, wenn sie:

(a) einer Person ohne Einwilligung des Bankkunden CID offenbart, die gar kein Beauftragter ist, sondern ein Dritter; oder

(b) erforderliche Risikominderungsmassnahmen unterlässt und dadurch kausal dazu beiträgt, dass CID von einem unbefugten Dritten zur Kenntnis genommen werden, falls die Bank dabei (eventual-)vorsätzlich oder fahrlässig handelt (vgl. vorne Rz. 39 f.). Darauf gehen wir im folgenden Abschnitt ein.

54 *Brändli*, Rz. 480.

5. Sorgfaltsmassstäbe bei der Auslagerung

65 Eine Bank ist verpflichtet, beim Beizug von Hilfspersonen die nach den Umständen gebotene Sorgfalt einzuhalten. Unterlässt sie diese Sorgfalt und kommt es in der Folge zu einer Offenbarung von CID durch die Hilfsperson gegenüber einem Unbefugten, die kausal durch den Sorgfaltsmangel verursacht ist, kann eine vorsätzliche oder fahrlässige Verletzung von Art. 47 Abs. 1 und 2 BankG vorliegen.[55]

66 Damit fragt sich, welche Sorgfalt „nach den Umständen geboten" (Art. 12 Abs. 3 StGB) ist. Diese Frage wäre im konkreten Fall durch den Strafrichter zu beurteilen. Der Strafrichter verfügt dabei über Ermessen, womit jeweils die Gefahr besteht, dass aus der unerlaubten Offenbarung direkt auf eine Sorgfaltspflichtverletzung geschlossen wird, was freilich unzulässig wäre.

67 Relevant ist sodann auch, dass in strafrechtlicher Sicht jeweils zu prüfen ist, wen die verletzte Pflicht überhaupt traf und ob überhaupt ein unerlaubtes Risiko geschaffen wurde (oben Rz. 40).

68 Für die Konkretisierung ist dabei zunächst von einschlägigen, gesetzlichen Sorgfaltsregeln auszugehen. Beachtlich sind darüber hinaus allgemein anerkannte Empfehlungen, Richtlinien, Merkblätter u. dgl. von privaten oder öffentlichen Stellen.[56] Im vorliegenden Zusammenhang dürften daher insbesondere (nicht abschliessend) die folgenden Regelwerke massgeblich sein:

(a) Die Anforderungen des schweizerischen Datenschutzrechts an die Datensicherheit (vgl. Art. 7 DSG, Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz, **VDSG**), was die Beachtung des „gegenwärtigen Stands der Technik" verlangt (Art. 8 Abs. 2 lit. d VDSG);

(b) ggf. die Anforderungen des schweizerischen Datenschutzrechts an die Übermittlung von Personendaten ins Ausland (Art. 6 DSG, Art. 5 ff. VDSG);

(c) die Anforderungen des FINMA-RS 2008/21, Anhang 3 (Umgang mit elektronischen Kundendaten);

---

55 Weitere Pflichten der Bank ergeben sich ggf. aus weiteren Bestimmungen zum Geheimnisschutz wie etwa Art. 162 oder Art. 273 StGB und aus dem anwendbaren Datenschutzrecht.

56 BSK-*Niggli/Maeder*, Art. 12 StGB N 111.

(d) der Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu den technischen und organisatorischen Massnahmen zum Datenschutz, soweit dieser Leitfaden Empfehlungen zum Einsatz bestimmter technischer und organisatorischer Massnahmen (**TOMs**) enthält.

(e) ggf. weitere einschlägige technische Standards, soweit sie zum gegenwärtigen Stand der Technik zählen.

69 Diese Vorgaben verlangen zunächst eine Erhebung und Einschätzung der mit der Auslagerung verbundenen Risiken. Unter diesem Titel hat die Bank allgemein etwa die folgenden Punkte zu beurteilen:

(a) die im konkreten Fall bestehenden Datensicherheitsrisiken, einschliesslich der Wirkung angemessener, mitigierender technischer und organisatorischer Massnahmen der Bank und des Anbieters, bspw. eine Verschlüsselung (unter Berücksichtigung des Schlüsselmanagements) und vertragliche Ge- und Verbote an den Dienstleister (vgl. insb. Rz. 24 ff. des Leitfadens);

(b) weitere anbieterspezifische Risiken, die im Rahmen des Auswahl- und Abschlussprozesses zu beurteilen, durch geeignete TOMs zu mitigieren und ggf. zu akzeptieren sind, einschliesslich des Einbezugs von Unterakkordanten und der Unterstützung bei einer Migration (vgl. Rz. 13 ff. des Leitfadens).

70 Sie hat mit dem Dienstleister ferner geeignete vertragliche Vereinbarungen zu treffen und deren Einhaltung angemessen zu überwachen und ggf. durchzusetzen (vgl. Rz. 12 des Leitfadens).

71 Im Fall einer Auslagerung ins Ausland – oder wenn Zugriffsmöglichkeiten auf CID aus dem Ausland eingeräumt werden, was weitgehend gleichbedeutend ist – sind überdies die spezifischen Auslandsrisiken zu berücksichtigen, insbesondere:

(a) an welchem Standort CID während der Vertrags- bzw. Bearbeitungsdauer gespeichert sind oder sein können und von wo aus Zugriffe möglich sind;

(b) welche rechtlichen Risiken im Fall einer Verletzung für den Dienstleister nach dem auf ihn anwendbaren lokalen Recht bestehen, z.B. allfällige

Strafdrohungen, und damit verbunden das Risiko, dass der ausländische Dienstleister aufgrund eines fehlenden oder niedrigeren Strafbarkeitsrisikos nicht mit der gleichen Sorgfalt vorgeht wie ein in der Schweiz ansässiger Dienstleister. Hier wäre es allerdings realitätsfremd anzunehmen, nur die Strafdrohung von Art. 47 Abs. 1 und 2 BankG könne einen Dienstleister daran hindern, CID an unberechtigte Dritte weiterzugeben. Das Reputationsrisiko dürfte stärker ins Gewicht fallen, jedenfalls bei global tätigen Anbietern, die bei Bekanntwerden einer unerlaubten Weitergabe von CID enorme Schäden zu befürchten hätten. Ebenfalls – aber vielleicht weniger stark – ins Gewicht fallen Schranken des lokalen Rechts wie bspw. § 203 des deutschen Strafgesetzbuchs oder die Bussendrohung nach der Europäischen Datenschutzgrundverordnung (Art. 83 DSGVO);

(c) die rechtlichen und faktischen Zugriffsmöglichkeiten lokaler Behörden an den relevanten Standorten und die sich aus einem Zugriff daraus ergebenden Risiken für den Bankkunden[57] sowie

(d) die Möglichkeiten der Bank und ihres Kunden, sich gegen einen Zugriff mit rechtlichen Mitteln zur Wehr zu setzen (weil das Risiko eines Zugriffs im Rahmen eines rechtsstaatlichen Verfahrens auch bei in der Schweiz liegenden Daten besteht und die Auslagerung ins Ausland nicht per se untersagt ist und bei einer entsprechenden Anfrage auch Rechtfertigungsgründe vorstellbar sind, genügt die Bank ihren diesbezüglichen Sorgfaltspflichten typischerweise dann, wenn sichergestellt wird, dass sie bzw. der betroffene Bankkunde eine entsprechende Anfrage in einem rechtsstaatlichen Verfahren überprüfen lassen können);

(e) die durch die konkrete Auslagerung ausgelösten rechtlichen und faktischen Zugriffsmöglichkeiten von Behörden ausserhalb der betreffenden Standorte, etwa im Anwendungsbereich einer Rechtsordnung, die die Bekanntgabe von ausserhalb des betreffenden Territoriums gespeicherter Daten verlangt. Dazu gehört bspw. der US CLOUD Act, der in den Stored Communications Act[58] die folgende Bestimmung eingefügt hat (Sec. 103(a)(1)):

[57] Das Risiko, dass überhaupt eine Behörde auf CID zugreift, besteht auch in der Schweiz und verletzt prinzipiell nicht das Bankkundengeheimnis. Zu berücksichtigen ist unter diesem Punkt nur das zusätzliche Risiko, das sich für den Bankkunden daraus ergibt, dass *eine ausländische* bzw. die *konkret zuständige ausländische* Behörde auf CID zugreift.

[58] Pub.L. 99–508,

> *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.*[59]

(f) Das Risiko, dass lokale Behörden unter Verletzung rechtsstaatlicher Grundsätze auf CID zugreifen könnten, wobei etwa die Gefahr eines Zugriffs aus rein fiskalischen oder politischen Motiven stärker ins Gewicht fiele als ein Zugriff aufgrund des begründeten Verdachts einer strafbaren Handlung;

(g) die verfügbaren Informationen, um diese Auslandsrisiken fundiert einschätzen zu können.

72 Diese Risikoeinschätzungen, Überlegungen, Schlussfolgerungen und Massnahmen sind zu dokumentieren und ggf. zu aktualisieren.

73 Bei einer Verletzung der gebotenen Sorgfalt gilt in strafrechtlicher Hinsicht das insb. vorne in Rz. 39 ff. und 65 Gesagte. Zusätzlich zu diesen Sorgfaltspflichten kann die Bank nach weiteren Bestimmungen, insbesondere nach weiteren Geheimnisschutzbestimmungen und dem anwendbaren Datenschutzrecht, zu weiteren Massnahmen verpflichtet sein, die nicht Gegenstand des vorliegenden Gutachtens sind.

[59] Sofern es sich um Daten von Personen handelt, die weder US-Staatsangehörige noch in den USA wohnhaft sind, kann allerdings eine Datenherausgabe gerichtlich unterbunden werden, sofern der Staat, in dem die Daten gehalten werden, mit den USA ein Exekutivabkommen abgeschlossen hat; vgl. *Determann/Nebel,* U.S. CLOUD Act – Wolken über der Datenschutz-Grundverordnung?, in: CR 6/2018, 408-412, 410.