www.jusletter.ch

David Rosenthal

Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act

Unternehmen wie Behörden drängt es in die Cloud. Doch Datenschützer warnen – vor allem vor dem US CLOUD Act: Gross ist die Angst vor dem Zugriff ausländischer Behörden. Viele haben Mühe, das Risiko einzuschätzen, tun es nur aus dem Bauch heraus. Dieser Beitrag stellt erstens eine neue, Management-taugliche Methode zur Einschätzung und Quantifizierung des Risikos eines ausländischen Behördenzugriffs à la CLOUD Act vor, und zeigt zweitens einen Weg, die gegensätzlichen Positionen im Expertenstreit um das Amts- und Berufsgeheimnisses in der Cloud zu vereinen. Beides soll helfen, Cloud-Projekte in sensitiven Bereichen nüchterner zu beurteilen.

Beitragsart: Wissenschaftliche Beiträge
Rechtsgebiete: Datenschutz; Informatik und Recht; Notariats- und Anwaltsrecht; Bankrecht; Strafrecht

Zitiervorschlag: David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

A. Ausgangslage und Einleitung

[1] Die Ausgangslage ist meist dieselbe und derzeit vielerorts in der Schweiz anzutreffen: Betriebe, ob in der Privatwirtschaft, Bund, Kantonen oder Gemeinden, überlegen sich, ihre IT-Anwendungen – ihre Büroautomation[1], CRM-Systeme[2] oder andere Anwendungen – in die Cloud zu migrieren. Diese Projekte sind nicht nur finanziell motiviert; die Verlagerung in die

1 Also Anwendungen wie E-Mail, Conferencing-Lösungen oder Office-Anwendungen wie Textverarbeitung.

2 Also Systeme zur Verwaltung von Kundenbeziehungen (*Customer Relationship Management*).

Cloud erlaubt es den Betrieben, ihren Benutzern mehr Funktionalität anzubieten,[3] da manche Anwendungen inzwischen nur noch in der Cloud angeboten werden oder die Cloud-Versionen von Anwendungen prioritär weiterentwickelt werden. In den Augen mancher Experten vermögen die grossen Cloud-Anbieter wie Microsoft, Google und Amazon auch ein höheres Niveau an Datensicherheit zu gewähren, auch wenn ein Kunde damit natürlich zugleich gewisse Klumpen- und Lock-in-Risiken eingeht.

[2] Diese Diskussion soll hier aber nicht geführt werden, denn sie lässt sich wissenschaftlich ohnehin nicht entscheiden, sondern ist über weite Strecken eine Glaubensfrage. Sie spielt in den Projekten nach der Erfahrung des Autors auch keine zentrale Rolle, denn jeder Betrieb, der sich mit einem Cloud-Vorhaben konfrontiert sieht, wird hierzu den Rat von internen oder externen Experten der Informationssicherheit einholen und sich diesbezüglich auf diesen verlassen müssen. Das war schon immer so und ist in einem Cloud-Vorhaben nicht anders. Letztlich ist der Gang in die Cloud nichts anderes als ein ganz normales Outsourcing von IT-Funktionen, und ein solches bringt immer Vor- und Nachteile mit sich, die beurteilt werden müssen. Die «Cloud» mag zwar für viele Personen weniger greifbar sein als wenn ein Unternehmen den Betrieb seiner Informatik an einen externen Rechenzentrumsbetreiber auslagert, aber im Grunde geht es um dasselbe. Was sich ändert sind gewisse kommerzielle und vertragliche Aspekte, die dem Provider und Kunden mehr Flexibilität bieten, und die Technik hat sich natürlich weiterentwickelt. Insbesondere die Virtualisierung von IT-Ressourcen hat viel ermöglicht. Daher ist auch die Diskussion um «private» oder «public» Cloud irreführend, denn auch Daten in einer «public» Cloud sind keineswegs öffentlich zugänglich, wie der Name suggeriert. Der Unterschied besteht in der Regel in gewissen technischen Betriebsmodellen und der Anzahl an virtuellen oder physischen «Schotten», die ein Provider zwischen den für verschiedene Kunden betriebenen Datenpools errichtet hat. Weil aber selbst Datenschutzbehörden teils fälschlicherweise zwischen «Cloud» und «Outsourcing» unterschieden haben,[4] sorgt der Begriff der Cloud in diesen Kreisen bis heute für ein schlechtes Gefühl. Der Einsatz von Cloud-Lösungen birgt durchaus Risiken, aber diese Risiken sollten mit Sachkunde nüchtern betrachtet und Gleiches mit Gleichem verglichen werden.

[3] Dabei sei aus Gründen der Transparenz offengelegt, dass dieser Beitrag zu wesentlichen Teilen aus der rechtlichen Beratungstätigkeit des Autors im Zusammenhang mit diversen Cloud-Projekten auf Seiten öffentlicher und privater Cloud-Nutzer (nicht auf Seiten der Anbieter Microsoft, Google oder Amazon) hervorgegangen ist. Namentlich das in der zweiten Hälfte dieses Beitrags vorgestellte Modell zur Beurteilung des Risikos eines *Lawful Access* durch ausländische Behörden wurde ursprünglich für eine grössere Schweizer Bank im Hinblick auf Bankkundendaten in der Cloud entwickelt. Weil solche Beurteilungsmodelle bisher nicht allgemein verfügbar waren, entschloss sich der Autor dieses Beitrags dazu, sein Modell zu veröffentlichen und der Allgemeinheit zur Verfügung zu stellen, damit es auch andere nutzen können. Der vorliegende Aufsatz soll einen Beitrag zur wissenschaftlichen Diskussion über Cloud-Risiken im Zusammenhang mit der Bearbeitung von Amts- und Berufsgeheimnissen und damit deren «Entmystifizierung» leisten. Eine solche Entmystifizierung tut Not.

---

3 Wie z.B. zusätzliche Anbindungen an das Internet oder andere Online-Dienste, was etwa bei CRM-Systemen von Nutzen sein kann.

4 So stellte der Datenschutzbeauftragte des Kantons Zürich in früheren Leitlinien für Cloud-Vorhaben strengere Anforderungen als für IT-Auslagerungen auf, obwohl es zwischen den beiden Szenarien keinen Unterschied gab, der die Ungleichbehandlung hätte rechtfertigen können.

[4] Von grösserer Bekanntheit ist in diesem Zusammenhang neben dem liberalen «Cloud-Leitfaden Wegweiser für sicheres Cloud Banking» der Schweizerischen Bankiervereinigung[5] und gewissen Auftragsgutachten (N 17 ff. und N 21 ff.) vor allem die kritische Position des Datenschutzbeauftragten des Kantons Zürich,[6] der in dieser Diskussion die Meinungsführerschaft unter den kantonalen Datenschützern übernommen hat. Ihren Niederschlag fand die kritische Haltung unter anderem im kürzlich überarbeiteten Merkblatt für Cloud-spezifische Risiken und Massnahmen von «privatim», der Konferenz der schweizerischen Datenschutzbeauftragten.[7] Vom Zürcher Datenschutzbeauftragten (heute eine Datenschutzbeauftragte) stammt auch folgende Zusammenfassung seiner Position:[8]

Besondere datenschutzrechtliche Aspekte der Cloud Nutzung –
unter Berücksichtigung des «CLOUD Act» (ausgenommen Schulen)

dsb
datenschutzbeauftragte kanton zürich

WICHTIG: Dieser Leitfaden ist Teil der datenschutzrechtlichen Ausführungen zur Auslagerung. Er gilt nur unter Berücksichtigung aller Anforderungen, konkretisiert in den Leitfäden Bearbeiten im Auftrag und Verschlüsselung der Daten im Rahmen der Auslagerung. In jedem Fall ist eine Risikobeurteilung vorzunehmen.

CLOUD Act ja/nein	Verschlüsselung	Datenschutzniveau	Besondere Voraussetzungen	Personendaten / Besondere Personendaten	
				Amtsgeheimnis	beispielsweise Steuergeheimnis Sozialhilfegeheimnis Berufsgeheimnis
CLOUD Act nicht anwendbar	Daten verschlüsselt/ Schlüsselmanagement beim öffentlichen Organ[1]	Angemessenes Datenschutzniveau[2]		✓	✓
		Nicht angemessenes Datenschutzniveau			
	Vertragliche Absicherung[3] (Schlüsselmanagement nicht beim öffentlichen Organ)	Angemessenes Datenschutzniveau[2]	CH Cloud, EU Cloud (DSGVO)	✓	✓
		Nicht angemessenes Datenschutzniveau	Standardvertragsklauseln[4]	✓	✗
				✗	
CLOUD Act anwendbar	Daten verschlüsselt/ Schlüsselmanagement beim öffentlichen Organ[1]	Angemessenes Datenschutzniveau[2]		✓	✓
		Nicht angemessenes Datenschutzniveau			
	Vertragliche Absicherung[3] (Schlüsselmanagement nicht beim öffentlichen Organ)	Angemessenes Datenschutzniveau[2]		✓	✗
		Nicht angemessenes Datenschutzniveau	Standardvertragsklauseln / Privacy Shield[4]		
				✗	
Spezialfall Wartung mit/ohne CLOUD Act	Wenn Verschlüsselung nicht möglich, vertragliche Absicherung[3]	Angemessenes Datenschutzniveau[2]		✓	✓
		Nicht angemessenes Datenschutzniveau	Standardvertragsklauseln / Privacy Shield[4]		

V 1.0 / Dezember 2019

[1] Mit dieser optimalen Lösung lassen sich alle Anforderungen abdecken. Konkret gilt der Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung.
[2] Liste der Staaten mit angemessenem Datenschutzniveau
[3] Der Auftragnehmer verpflichtet sich, den Schlüssel nur auf explizite Anfrage und nach expliziter Einwilligung des Auftraggebers einzusetzen.
[4] Oder andere Massnahmen, die einen angemessenen Schutz gewährleisten.

Datenschutz mit Qualität

[5] Der Zürcher Datenschutzbeauftragte war es auch, der ein umstrittenes Gutachten zur Frage der Vereinbarkeit von Auslagerungen mit dem Berufsgeheimnis in Auftrag gegeben hat, auf das auch in diesem Beitrag noch einzugehen sein wird (N 15 f.). Seine Publikationen und öffentli-

5 Schweizerische Bankiervereinigung, Cloud Leitfaden (https://www.swissbanking.org/library/richtlinien/cloud-leitfaden-wegweiser-fuer-sicheres-cloud-banking), kontrolliert am 3. Juli 2020.

6 Datenschutzbeauftragte des Kanton Zürichs (https://www.datenschutz.ch), kontrolliert am 3. Juli 2020.

7 Überarbeitetes privatim-Merkblatt Cloud-spezifische Risiken und Massnahmen (https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen/), kontrolliert am 3. Juli 2020.

8 Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act» (ausgenommen Schulen) (https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/leitfaeden/leitfaden_auslagerung_beruecksichtigung_des_cloud_act.pdf), kontrolliert am 3. Juli 2020.

che Verlautbarungen in der Tagespresse[9] erwecken sodann den Eindruck, dass den kantonalen Datenschutzbeauftragten im Zusammenhang mit Cloud-Projekten vor allem der US CLOUD Act Sorgen zu bereiten scheint.

[6] Der Autor des vorliegenden Beitrags vertritt hier eine andere Ansicht: Die mit dem US CLOUD Act verbundenen Risiken werden heute meist *überbewertet*, während die klassischen Risiken der Datensicherheit und der *Business Continuity* im Rahmen von Cloud-Projekten zu sehr in den Hintergrund rücken. Darauf wird in diesem Beitrag noch einzugehen sein.

[7] Der vorliegende Beitrag stellt jedoch keine umfassende Anleitung zur Verfügung, wie Cloud-Projekte rechtskonform und insbesondere im Einklang mit dem Datenschutz umzusetzen sind. Neben der hier diskutierten Frage, ob und unter welchen Voraussetzungen auch Amts- und Berufsgeheimnisgeschützte Daten in die Cloud im In- und Ausland dürfen, gibt es noch diverse andere Dinge, die in solchen Vorhaben zu beachten sind. Dazu gehören unter anderem die allgemeinen datenschutzrechtlichen Vorgaben an eine Auftragsbearbeitung (was u.a. einen entsprechenden Vertrag erfordert)[10] und ggf. die Bekanntgabe von Personendaten ins Ausland (die sich – sobald die Frage des Amts- und Berufsgeheimnisses gelöst ist – ohne Weiteres erfüllen lassen[11]), aufsichtsrechtliche Vorgaben (z.B. im Bereich der Finanzindustrie die FINMA Rundschreiben 2008/03 zum Outsourcing oder Anhang 3 zum FINMA Rundschreiben 2008/21 über operationelle Risiken sowie bei Versicherungen die Genehmigungspflicht) sowie die bei allen Auslagerungen erforderlichen Überlegungen zu den damit verbundenen operationellen Risiken (Vendor Assessment, Ausfallrisiken, geordnete Rückführung, Audits, Lock-in-Effekte, etc.).

B. Rechtliche Problemstellung und Überblick

[8] Der vorliegende Beitrag erörtert die Vereinbarkeit des Beizugs eines Cloud-Providers durch einen Berufsgeheimnisträger mit seinen Geheimhaltungspflichten aus dem Berufsgeheimnis. Es wird jeweils auf einen «Cloud-Provider» verwiesen. Gemeint ist damit ein gruppeninterner oder externer Anbieter von IT-bezogenen Dienstleistungen, welcher die ihm anvertrauten Informationen mit einer Cloud-basierten Infrastruktur speichert und bearbeitet.

[9] Regelungen zum Berufsgeheimnis finden sich in verschiedenen Bestimmungen des Schweizer Rechts. Es gibt Bestimmungen, die das Berufsgeheimnis *positiv* formulieren, d.h. direkt zu dessen Einhaltung verpflichten, auch wenn keine entsprechende vertragliche Regelung besteht (z.B. Art. 13 BGFA[12], Art. 43 FMG[13], Art. 33 ATSG[14], Art. 86 BVG[15]). Es gibt ferner diverse Be-

9 Vgl. etwa Fabian Fellmann, vom 25. Mai.2020, (https://www.tagesanzeiger.ch/datenschuetzer-warnen-vor-microsoft-produkt-841863907053), kontrolliert am 3. Juli 2020.

10 Dazu: David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage? in: Jusletter 17. Juni 2019 (http://www.rosenthal.ch/downloads/Rosenthal-ControllerProcessor.pdf), kontrolliert am 3. Juli 2020.

11 Art. 6 DSG.

12 Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte vom 23. Juni 2000 (Anwaltsgesetz, BGFA; SR 935.61).

13 Bundesgesetz über die fernmeldetechnische Übertragung von Informationen vom 30. April 1997 (Fernmeldegesetz, FMG; SR 784.10).

14 Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts vom 6. Oktober 2000 (Sozialversicherungsrecht, ASTG; SR 830.1).

15 Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge vom 25. Juni 1982 (Alters- und Invalidenvorsorge, BVG; SR 831.40).

stimmungen, welche die Verletzung des Berufsgeheimnisses unter Strafe stellen, sei es vertraglicher oder gesetzlicher Natur (z.B. Art. 321 ff. StGB[16], Art. 47 BankG[17], Art. 69 FINIG[18], Art. 35 DSG[19], Art. 76 BVG). Damit verwandt sind die Bestimmungen zum Amtsgeheimnis (z.B. die Strafnorm des Art. 320 StGB) und das Dienstgeheimnis im Militär (Art. 33 MG[20], Art. 77 und 106 MStG[21]). Ferner gibt es Normen, welche den Verrat von aus Gesetz oder Vertrag zu schützenden Geschäfts- und Fabrikationsgeheimnissen unter Strafe stellen – allgemein oder im Ausland (Art. 162 StGB, Art. 273 StGB). Ihnen gemein ist, dass sie *Offenbarung* von dem Geheimnisträger anvertrauten oder kraft seiner Stellung zugekommenen *Daten* gegenüber *Unberechtigten* unter Strafe stellen. Mehrheitlich ist hierfür Vorsatz erforderlich (wobei Eventualvorsatz genügt), ausnahmsweise genügt Fahrlässigkeit (namentlich bei Art. 47 BankG und Art. 69 FINIG).

[10] Wenn von «Offenbaren» die Rede ist, so ist damit der Tatbestand der Geheimnisverletzung im Rahmen der vorstehenden Bestimmungen gemeint. Die Preisgabe (einschliesslich Zugänglichmachen) von geheimnisgeschützten Daten an einen *Berechtigten* (oder «Berufenen») ist nicht tatbestandlich, auch wenn dies aus den Normen nicht ausdrücklich so hervorgeht. In der Praxis stellt sich nun die Frage, ob und in welchen Fällen der Beizug eines Cloud-Providers eine solche (strafbare) Offenbarung darstellt. Hierbei beschränken sich die folgenden Ausführungen auf Fälle, in denen der Beizug des Cloud-Providers bedeutet, dass dieser Zugang zu den geheimnisgeschützten Daten *im Klartext* erhält. Werden dem Cloud-Provider Daten in vollverschlüsselter Form zugestellt, die er nicht entschlüsseln kann, liegt von vornherein kein Offenbaren von Geheimnissen vor. In der Praxis wird dieser Ansatz aber kaum verfolgt, weil er in vielen Anwendungen nicht praktikabel ist bzw. der Beizug eines Cloud-Providers in dieser Konstellation wenig bringt.

[11] Die Lehre diskutierte vor diesem Hintergrund bisher kontrovers, ob der Begriff des Offenbarens bereits die Möglichkeit der Kenntnisnahme des Geheimnisses durch einen Unberechtigten umfasst oder ob diese Person tatsächlich vom Geheimnis Kenntnis genommen haben muss. Gemäss jüngster Rechtsprechung des Bundesgerichts zu Art. 162 StGB ist letzteres erforderlich.[22] Ob dieser Entscheid auch für die Normen des Berufsgeheimnisses gilt, kann an dieser Stelle offengelassen werden, weil die Frage für die hier relevante Problemstellung in der Regel irrelevant ist. Zwar gibt es Szenarien, in welchen ein Cloud-Provider so eingesetzt wird, dass dessen Mitarbeiter die Daten nie im Klartext zu Gesicht bekommen werden, weil sie in deren Computersystemen verborgen bleiben und daher gut vertreten werden kann, dass schon deswegen kein Offenbaren vorliegen kann. In der Praxis wird es jedoch immer Fälle geben, in denen ein Mitarbeiter Zugang zu Daten im Klartext braucht, weil er beispielsweise Support bieten muss. Zudem besteht dort, wo dies nicht nötig sein sollte, die Daten sich aber mindestens zeitweise im Klartext im System des Cloud-Providers befinden (was ungeachtet des Einsatzes von Verschlüsselungstechniken einschliesslich «Bring-your-own-key» fast immer der Fall ist), mindestens im Ausland das

16 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Strafgesetzbuch, StGB; SR 311.0).

17 Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (Bankengesetz, BankG; SR 952.0).

18 Bundesgesetz über die Finanzinstitute vom 15. Juni 2018 (Finanzinstitutsgesetz, FINIG; SR 954.1).

19 Bundesgesetz über den Datenschutz vom 1. März 2019 (Datenschutzgesetz, DSG; SR 235.1).

20 Bundesgesetz über die Armee und die Militärverwaltung vom 3. Februar 1995 (Militärgesetz, MG; SR 510.10).

21 Militärstrafgesetz vom 13. Juni 1927 (Militärstrafgesetz, MStG; SR 321.0).

22 BGer 6B_1403/2017 vom 8. August 2018, Erw. 1.2.2.; vgl. jedoch OGer ZH vom 27. Dezember 2019, UE190028-O, Erw. 5.1, wobei sich das Gericht mit der hier relevanten Frage nicht wirklich auseinandersetzt.

Risiko eines nach ausländischem Recht gestützten Zugriffs durch ausländische Behörden (*Lawful Access*). Ein solcher *Lawful Access* zu Daten im Klartext ist in jedem Fall ein Offenbaren. Dazu wird noch ausführlich einzugehen sein, weil beim Beizug von ausländischen Cloud-Providern eben dieser *Lawful Access* in den Augen vieler die Hauptherausforderung bei der Beurteilung der Risiken darstellt (N 75 ff.).

[12] Es herrschen in der Schweizer Lehre unterschiedliche Ansichten darüber, ob ein Berufsgeheimnisträger einem Cloud-Provider berufsgeheimnisgeschützte Daten *ohne Einwilligung seiner Kunden* anvertrauen darf, selbst wenn dieser sorgfältig ausgewählt wurde, eine angemessene Datensicherheit bietet, sein Vertrag den Vorgaben des DSG entspricht und der Provider (auch) vertraglich zur Geheimhaltung verpflichtet ist. Diese Frage stellt sich für Auslagerungen an Cloud-Provider in der Schweiz und erst recht an solche im Ausland. Die Praxis äusserte sich zur Frage bisher nicht, doch haben Aussagen in einem kürzlich ergangenen Bundesgerichtsentscheid zum Anwaltsgeheimnis zusätzliche Fragen mit Bezug auf die Subdelegation der Datenbearbeitung aufgeworfen.

[13] Einigkeit scheint in der Lehre immerhin dahingehend zu bestehen, dass die Preisgabe von berufsgeheimnisgeschützten Daten gegenüber einem beigezogenen Dritten in jedem Fall dann zulässig ist, wenn der Geheimnisherr darin auf informierter Basis eingewilligt hat. Umgekehrt ist klar, dass dort, wo mit einem Geheimnisherrn vereinbart wurde, dass *keine* Hilfspersonen beigezogen werden dürfen oder keine Auslagerung der Datenbearbeitung stattfinden darf oder nur mit vorheriger Einwilligung, eine solche Einwilligung zwingend erforderlich ist. Diese Fälle sollen hier nicht weiter erörtert werden, ebenso nicht die Frage, wie eine Einwilligung eingeholt werden kann.

[14] Nachfolgend soll zunächst die wichtigste bisherige Lehre und Praxis zum Thema dargestellt werden (N 15 ff.), um dann einen Weg aufzuzeigen, wie sich diese unterschiedlichen Ansichten für die Frage des Beizugs eines Cloud-Providers durch eine neue Perspektive in Einklang bringen lassen (N 30 ff.). Dabei wird bewusst nicht nach Berufsgeheimnis differenziert, da die Grundsätze nach der hier vertretenen Ansicht für alle Berufsgeheimnisträger (und darüber hinaus auch für zur Geheimhaltung verpflichtete Geschäftsgeheimnisträger) im Grundsatz dieselben sind (N 69 ff.). Auch das Thema der Subdelegation wird adressiert (N 58 ff.). Im Anschluss wird aufgezeigt, welches Restrisiko einer (strafbaren) Offenbarung akzeptabel bzw. erlaubt ist (N 75 ff.) und ein Modell vorgestellt, wie insbesondere das Risiko eines *Lawful Access* im Ausland beurteilt und quantifiziert werden kann, damit dazu ein Risikoentscheid möglich ist (N 106 ff.).

C. Bisherige Lehre und Praxis

1. Wohlers: Beizug Dritter nur mit Wissen und Willen des Geheimnisherrn

[15] Die strengste Position zum Thema vertritt Wohlers in einem Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich.[23] Er fokussiert auf Art. 321 StGB und stützt sich vor allem auf die deutsche Lehre zur deutschen Parallelnorm. Nach seiner Ansicht kommt

[23] Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Zürich/Basel/Genf 2016.

es nicht darauf an, ob der beigezogene Dritte (hier also der Cloud-Provider) als Hilfsperson im Sinne von Art. 321 StGB gilt und daher direkt dem Berufsgeheimnis unterliegt.[24] Damit es durch den Beizug des Dritten nicht zum tatbestandlichen Offenbaren eines Geheimnisses kommt, muss der Beizug seiner Ansicht nach erstens zur Erbringung der Dienstleistung *erforderlich* sein und zweitens für den Geheimnisherrn (hier: den Kunden des Berufsgeheimnisträgers) *voraussehbar* sein.[25] Beide Voraussetzungen beurteilt Wohlers streng: Erforderlich bedeutet für ihn «zwingend geboten», und voraussehbar als «sicher voraussehbar». Wenn das gegeben ist, zählt der Dritte zum «Kreise der zum Wissen Berufenen» und die Offenlegung der Geheimnisse an ihn stellen kein (strafbares) Offenbaren mehr dar.[26]

[16] Wer zu diesem Kreis gehören darf, darf seiner Ansicht nach hingegen nicht auf «ein finanziell und/oder organisatorisch motiviertes wirtschaftliches Interesse des Geheimnisträgers am Einbezug Dritter» gestützt werden, sondern muss auf ein mindestens konkludentes Einverständnis des Geheimnisherrn zurückzuführen sein. Ein solches Einverständnis wiederum setzt seiner Ansicht nach voraus, dass der Geheimnisherr sich über die Existenz der Dritten zumindest ein Bild machen können müsse, was nicht bei allen Varianten des modernen Outsourcing ohne weiteres angenommen werden könne.[27]

2. Schwarzenegger: Beizug Dritter unter Beachtung der Risikoadäquanz zulässig

[17] Die liberale Gegenposition vertreten am prominentesten Schwarzenegger/Thouvenin/Stiller in einem Rechtsgutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands.[28] Sie fokussieren sich im strafrechtlichen Teil ebenfalls auf Art. 321 StGB, allerdings ausschliesslich bezogen auf Anwälte und der Frage, ob diese die Cloud nutzen dürfen.

[18] Auch sie sehen ein (strafbares) Offenbaren erst dann als gegeben, wenn das Geheimnis einer «dazu nicht ermächtigten Drittperson» zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht.[29] Nach ihrer Ansicht sind jedoch alle Dritte, die als Hilfspersonen im Sinne von Art. 321 StGB gelten, ermächtigt.[30] Personen, die für die IT-Dienste des Anwalts zuständig sind oder Cloud-Lösungen für ihn betreiben *sind* ihrer Ansicht solche Hilfspersonen.[31]

[19] Schwarzenegger et al. sind der Ansicht, dass «Tätigkeiten, die objektiv bei einer sinnvollen Arbeitsteilung einer Arztpraxis, Anwaltskanzlei oder sonstigen Tätigkeit eines Berufsgeheimnisträgers notwendig und im beruflichen Kontext bei der Bewältigung der administrativen Prozesse üblich» seien, auch «ohne spezifische Einwilligung des Geheimnisherrn» übertragen werden

24 Wohlers, (Fn. 23), S. 25 f.

25 Wohlers, (Fn. 23), S. 26.

26 Wohlers, (Fn. 23), S. 19.

27 Wohlers, (Fn. 23), S. 19.

28 Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Zürich, Fassung vom 1. November 2018; vgl. die Zusammenfassung in https://bit.ly/34h0FT9, kontrolliert am 3. Juli 2020.

29 Schwarzenegger et. al, (Fn. 28), S. 29.

30 Schwarzenegger et. al, (Fn. 28), S. 30.

31 Schwarzenegger et. al, (Fn. 28), S. 30.

können.[32] Weil nach ihrer Ansicht auch der Gesetzgeber von einer solchen arbeitsteiligen Durchführung der Tätigkeit ausging, habe er den Kreis der Personen, die das Geheimnis zur Kenntnis nehmen und daher dem Berufsgeheimnis unterstellt werden müssen, breit gefasst.[33] Hilfsperson ist nach ihrer Ansicht damit, «wer bei der Berufstätigkeit eines (Haupt-)Geheimnisträgers in der Weise mitwirkt, dass er grundsätzlich von Geheimnissen Kenntnis erhalten kann».[34]

[20] Allerdings sind auch Schwarzenegger et al. nicht der Ansicht, dass der Anwalt jeden Dritten beiziehen darf. Vielmehr müsse «je nach Sensibilität der Information» entschieden werden, ob der Beizug der ins Auge gefasste Cloud-Provider «risikoadäquat» sei.[35] Ob die Hilfsperson sich in der Schweiz befindet oder im Ausland, spielt darüber hinaus nach ihrer Ansicht offenbar keine Rolle; Hilfstätigkeiten im Ausland seien «nicht ausgeschlossen».[36]

3. Weitere Lehrmeinungen

[21] Weitere Stimmen haben sich soweit ersichtlich ebenfalls gegen Wohlers ausgesprochen.

[22] In seiner Botschaft zur gegenwärtigen Revision DSG vertrat der Bundesrat die Ansicht, die Auslagerung der Bearbeitung von Personendaten (Auftragsbearbeitung) an eine Hilfsperson im Sinne von Art. 321 Abs. 1 StGB stelle keine unerlaubte Offenbarung dar.[37] Eine Auftragsbearbeitung setzt nach (dem revidierten) DSG im Ergebnis die Vereinbarung und DSG-konforme Ausübung eines Weisungsrechts, eine angemessene Datensicherheit und Kontrolle des Beizugs von Unterauftragsbearbeitern voraus, und sie muss verhältnismässig sein.

[23] In ihrem Gutachten im Auftrag der Schweizerischen Bankiervereinigung kommen Walder-Wyss zum Ergebnis,[38] dass eine Auslagerung an einen Cloud-Provider (und der damit verbundene Zugang zu geheimnisgeschützten Daten im Klartext) auch dann zulässig sein muss, wenn keine (absolute) Notwendigkeit dazu besteht.[39] Sie gehen davon aus, dass wenn vertragsrechtlich ein Beizug von Hilfspersonen erlaubt ist, ihnen auch unter dem Bankgeheimnis geheimnisgeschützte Daten offengelegt werden dürfen.[40] Sie verlangen, dass (a) die Auslagerung einem vernünftigen Interesse der auslagernden Bank entspricht, (b) die Auslagerung als Beizug einer Hilfsperson ausgestaltet ist (d.h. die Geschäftstätigkeit der Bank wird unterstützt und der Dritte untersteht ihrer Weisungsbefugnis) und (c) die Bank die Leistungen weiterhin schwergewichtig selbst erbringt.[41] Dass in Art. 47 BankG vom «Beauftragten» statt Hilfsperson die Rede ist, soll dabei keinen Unterschied machen.[42] Sie weisen darauf hin, dass der Beauftragte gerade zum Zweck in Art. 47 BankG

32 Schwarzenegger et. al, (Fn. 28), S. 27.

33 Schwarzenegger et. al, (Fn. 28), S. 19.

34 Schwarzenegger et. al, (Fn. 28), S. 20.

35 Schwarzenegger et. al, (Fn. 28), S. 28.

36 Schwarzenegger et. al, (Fn. 28), S. 28.

37 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 7031 f., m.w.H.

38 Michael Isler/Oliver M. Kunz/Thomas Müller/Jürg Schneider/David Vasella, WalderWyss, Zulässigkeit der Bekanntgabe von Bankkundendaten durch schweizerische Banken an Beauftragte im Ausland unter Art. 47 BankG, 15. Februar 2019, abrufbar auf der Website der schweizerischen Bankiervereinigung (SBVg).

39 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 21.

40 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 21 f.

41 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 22.

42 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 23.

eingeführt worden war, um Banken die Auslagerung der Datenbearbeitung an Rechenzentren zu ermöglichen.[43] Zur Frage der Zulässigkeit der Auslagerung ins Ausland argumentieren sie, diese sei nach dem Wortlaut von Art. 47 BankG nicht ausgeschlossen, weshalb sie im Rahmen einer Strafnorm aufgrund des Legalitätsprinzips (Art. 1 StGB) nicht grundsätzlich ausgeschlossen sein könne.[44] Nach ihrer Ansicht soll die Auslagerung ins Ausland zulässig sein, solange die Bank die «nach den Umständen gebotene Sorgfalt» einhalte.[45] Was dies konkret verlangt, sagen sie nicht wirklich, vertreten aber u.a. die Auffassung, die Bank genüge für den Fall des Zugriffs durch eine ausländische Behörde ihren Sorgfaltspflichten, wenn sichergestellt sei, dass der betroffene Kunde einen solchen Herausgabebefehl in einem rechtsstaatlichen Verfahren überprüfen lassen könne.[46]

[24] In einem ebenfalls im Auftrag der Schweizerischen Bankiervereinigung verfassten Gutachten kommen LauxLawyers auf etwas anderem Weg zu vergleichbaren Ergebnissen.[47] Sie gehen von einer «impliziten Einwilligung» des Kunden nach dem Vertrauensprinzip in Bezug auf die Art und Weise aus, wie die Bank sich intern organisiert (einschliesslich des Beizugs eines Cloud-Providers), solange sie «angemessene Schutzmassnahmen» trifft.[48] Solche sind ihrer Ansicht nach nur aber immerhin gegeben, wenn sie «dem aktuellen Stand der Technik» entsprechen,[49] deren Einsatz sie als Schutzpflicht der Bank aufgrund deren Garantenstellung gegenüber dem Bankkunden mit Bezug auf die von ihm der Bank anvertrauten Angaben verlangt.[50] Sie erachten den Cloud-Provider als «Beauftragten» im Sinne von Art. 47 BankG, weshalb diesem die Daten des Kunden anvertraut werden dürfen.[51] Diese «privilegierende Wirkung» dürfe auch bei Auslandsbezug nicht entfallen, wenn die Bank eine «genügende Kontrolle» über den Provider habe.[52] Dies begründen sie u.a. damit, dass jene Daten, an denen ausländische Behörden besonders interessiert sind, ihnen inzwischen ohnehin auf anderem Wege zukommen, und der Wortlaut von Art. 47 BankG keine Einschränkung mit Bezug auf das Ausland vorsieht.[53] Im Weiteren diskutieren sie Schutzmassnahmen.[54]

4. BGE 145 II 229 zur «Subdelegation» durch Hilfspersonen

[25] Auch das Bundesgericht scheint grundsätzlich von einer Zulässigkeit der Auslagerung der Bearbeitung von berufsgeheimnisgeschützten Daten an Hilfspersonen auszugehen, beschäftigte es sich in BGE 145 II 229 aus dem Jahre 2019 denn auch nicht mit der Frage, ob sie erlaubt ist,

43 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 19, mit Hinweis auf die Botschaft zur Revision des Bankengesetz (BBl 1970 I 1182).

44 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 24.

45 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 24 ff.

46 Isler/Kunz/Müller/Schneider/Vasella, (Fn. 38), S. 27.

47 Christian Laux/Alexander Hofmann/Mark Schieweck/Jürg Hess, Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG, Zürich, 14. Februar 2019.

48 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 4.

49 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 8.

50 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 6 f.

51 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 11.

52 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 12.

53 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 13 ff.

54 Laux/Hofmann/Schieweck/Hess, (Fn. 47), S. 16 ff.

sondern ob Hilfspersonen *ihrerseits* Dritte beiziehen können (was es als «Subdelegation» bezeichnete).

[26] Der Entscheid fokussiert stark auf den Berufsstand der Anwälte und lässt sich daher kaum auf andere Branchen übertragen. Das Bundesgericht beurteilte den Beizug von Hilfspersonen nicht nach Art. 321 StGB, sondern im Lichte von Art. 13 Abs. 2 BGFA (Pflicht des Anwalts, für die Wahrung des Berufsgeheimnisses auch durch Hilfspersonen zu sorgen). Es führte aus, ein Anwalt könne nicht nur Arbeitnehmer als Hilfspersonen beiziehen, sondern auch ausserbetriebliche Personen, wie z.B. eine Bank, einen Übersetzungsdienst oder auch einen externen Provider, der die Daten eines Anwalts in der Ferne aufbewahrt und schützt («le professionnel externe chargé de la conservation et de la protection à distance des données informatiques de l'avocat»).[55] Der Begriff der Hilfsperson sei weit zu fassen und schliesse nicht aus, dass es sich um eine juristische Person handle, die wiederum eigenes Personal beschäftige.[56] Aufgrund der Wichtigkeit des Anwaltsgeheimnisses sei jedoch der Kreis der Personen, die Zugang zu geheimen Informationen haben, «vernünftig zu beschränken» («une limitation raisonable») und es seien «hinreichende Massnahmen» zur Datensicherheit («mesures suffisantes pour sécuriser ces informations») zu treffen.[57]

[27] Das Bundesgericht erachtete es mit Bezug auf das Berufsgeheimnis als unsorgfältig und damit unzulässig, dass der Anwalt es der Hilfsperson erlaubte, ihre Haftung soweit gesetzlich zulässig auszuschliessen.[58] Der Anwalt habe alle Massnahmen zu treffen, die man «von ihm erwarten kann» («toutes les mesures que l'on peut attendre de lui»), um eine Verletzung des Berufsgeheimnisses zu vermeiden.[59] Er müsse insbesondere Hilfspersonen sorgfältig auswählen und sicherstellen, dass sie dem Anwaltsgeheimnis unterliegen, indem er sie über das Berufsgeheimnis belehrt, wenn nötig eine Vertraulichkeitsvereinbarung unterzeichnet und ihre Kontrolle im Hinblick auf die Wahrung des Berufsgeheimnisses sicherstellt.[60] Dieser Sorgfaltspflicht zwecks Einhaltung des Berufsgeheimnisses auch durch die Hilfsperson könne er sich nicht «befreien» («se libérer de l'obligation»).

[28] Von besonderem Interesse sind allerdings die Ausführungen des Bundesgerichts mit Bezug auf die Frage, inwieweit eine solche Hilfsperson ihrerseits Dritte beiziehen darf. Es erachtete es als nicht zulässig, dass ein Anwalt akzeptiere, dass seine Hilfsperson ihm übertragene Arbeiten von einem Dritten ausführen lässt, weil dies bedeute, dass eine Person «die nicht seine Hilfsperson ist und die auch nicht seiner Hilfsperson untersteht» Zugang zu den geheimnisgeschützten Daten hat («qu'une personne qui n'est pas son auxiliaire et qui n'est pas non plus subordonnée à son auxiliaire»).[61] Es genüge nicht, die Hilfsperson zu verpflichten dafür zu sorgen, dass der Dritte sich an das Anwaltsgeheimnis halte.[62] In diesem Zusammenhang ist allerdings zu berücksichtigen, dass die Hilfsperson im konkreten Fall sich gegenüber dem Anwalt vertraglich ausbedungen hatte, den von ihr beigezogenen Dritten selbst auszuwählen und die Gewährleistung für

55 BGE 145 II 229, Erw. 7.3.
56 BGE 145 II 229, Erw. 7.3.
57 BGE 145 II 229, Erw. 7.4.
58 BGE 145 II 229, Erw. 7.5.
59 BGE 145 II 229, Erw. 7.2.
60 BGE 145 II 229, Erw. 7.2.
61 BGE 145 II 229, Erw. 7.4.
62 BGE 145 II 229, Erw. 7.4.

diesen gegenüber dem Anwalt einschränkte (der genaue Wortlaut der betreffenden AGB ist nicht bekannt).[63]

[29] In der Lehre wurde dieser Entscheid mitunter als eigentliches Verbot der Subdelegation interpretiert[64] und entsprechend kritisiert.[65] Fellmann/Burger weisen darauf hin, dass die Hilfsperson nach Art. 13 Abs. 2 BGFA jener von Art. 101 OR entspreche und dort unterschieden werde zwischen Untergehilfen, die *mit* Ermächtigung des Geschäftsherrn beigezogen werden und solche, die ohne sein Wissen und seinen Willen eingesetzt werden; Hilfspersonen der ersten Kategorie müssen ihrer Ansicht nach als Hilfsperson im Sinne von Art. 13 Abs. 2 BGFA qualifiziert und als erlaubt betrachtet werden, auch wenn der Anwalt mit diesen Untergehilfen keinen direkten Vertrag hat.[66] Ihnen zufolge muss es genügen, dass die Hilfsperson vom Anwalt verpflichtet wird, die (ermächtigten) Untergehilfen zur Wahrung des Berufsgeheimnisses zu verpflichten; sie wären damit auch Hilfspersonen im Sinne von Art. 321 StGB und somit vom Berufsgeheimnis direkt erfasst.[67]

D. Analyse der Lehre und Praxis und Ansatz einer Weiterentwicklung

1. Stellungnahme zur bisherigen Lehre

[30] Die dargelegten unterschiedlichen Ansichten zum Beizug von Cloud-Providern und anderen Dritten durch Berufsgeheimnisträger scheinen sich auf den ersten Blick diametral entgegenzustehen. Sollte der BGE 145 II 229 (N 25 ff.) zudem tatsächlich als Verbot der Subdelegation verstanden werden, dürfte mindestens für Anwälte der Einsatz von Cloud-Providern ohne Einwilligung ihrer Klienten schwierig werden, sind doch viele dieser Provider auf den Einsatz von Untergehilfen angewiesen. Dies erscheint schon deshalb unbillig, weil es sich bei diesen Untergehilfen häufig um konzerneigene Unternehmen handelt und die Zulässigkeit somit von der – zufälligen – Frage abhängen würde, wie ein Provider seine Unternehmensgruppe zur Erbringung seiner Leistungen gesellschaftsrechtlich strukturiert hat; zu denken ist etwa an den Fall, in welchem ein Rechenzentrum von einer lokalen Tochtergesellschaft in der Schweiz betrieben wird, während die Kundenverträge über eine irische Gesellschaft abgeschlossen werden und bestimmte Supportleistungen von der US-Muttergesellschaft erbracht werden. Würde hingegen ausschliesslich mit Zweigniederlassungen einer einzigen Gesellschaft gearbeitet, käme der Provider technisch ohne Untergehilfen aus, obwohl das Risikoprofil aus Sicht des Berufsgeheimnisses praktisch identisch wäre. Dies macht deutlich, dass es nicht auf die juristische Organisationsform ankommen kann, sondern das Risikoprofil im Vordergrund stehen sollte.

[31] Um angesichts der diversen Lehrmeinungen die Frage zu beantworten, ob ein Berufsgeheimnisträger einen Cloud-Provider beiziehen darf, ist eine differenzierte Betrachtung der Argumente nötig.

---

63 BGE 145 II 229, Erw. 7.4., Sachverhalt A.b.

64 Martin Rauber, 2C_1083/2017: Geschäftsadresse eines Anwalts (institutionelle Unabhängigkeit, Berufsgeheimnis), in: swissblawg vom 25. Juni 2019.

65 Walter Fellmann/Yvonne Burger, Unabhängigkeit und Berufsgeheimnis bei Subdelegation durch Hilfsperson – BGer 2C_1083/2017 vom 4. Juni 2019, in: Anwaltsrevue, 8/2019, S. 341 ff.

66 Fellmann/Burger (Fn. 65), S. 346.

67 Fellmann/Burger (Fn. 65), S. 346.

[32] Wohlers ist darin zuzustimmen, dass ein Berufsgeheimnisträger nicht einfach beliebige Hilfspersonen beziehen kann mit dem Argument, dass sie als solche ebenfalls dem Berufsgeheimnis unterstehen; aus demselben Grund dürfen zwei Ärzte desselben Patienten sich nicht frei über diesen austauschen, obwohl sie beide unter dem Arztgeheimnis stehen. Wenn dann noch argumentiert wird, dass als Hilfsperson jeder gilt, der derart bei der betreffenden Tätigkeit mitwirkt, dass er von Berufsgeheimnissen Kenntnis erhalten kann, so ist dies schlicht ein Zirkelschluss. Darum kann es in der Tat nicht genügen, dass eine Person Hilfsperson im Sinne von Art. 321 StGB ist.

[33] Schwarzenegger et al. ist wiederum zuzustimmen, dass arbeitsteiliges Zusammenwirken in der heutigen Wirtschaft an der Tagesordnung ist und ohne ein solches ein vernünftiges Tätigwerden gar nicht mehr möglich ist. Das ist beim Einsatz von IT-Providern nicht nur eine Frage der Wirtschaftlichkeit, sondern immer häufiger auch eine der Sicherheit und Funktionalität: Cloud-Provider können heute mitunter eine wesentliche höhere Datensicherheit garantieren als wenn der Anwalt zum Beispiel seinen E-Mail-Server selbst betreibt. Der Beizug eines Cloud-Providers kann selbst dann im Interesse des Geheimnisherrn sein, wenn dieser – wie üblich – nicht direkt an der Leistungserbringung beteiligt ist. Er kann aus datenschutzrechtlicher Sicht mithin angezeigt (und somit angesichts der Sorgfaltspflicht des Berufsgeheimnisträgers sogar geboten) sein, wenn dadurch ein höherer Grad an Datensicherheit gewährleistet werden kann.

[34] Es ist denn auch allgemein anerkannt, dass Berufsgeheimnisträger ihrerseits alle möglichen externen Personen beiziehen dürfen, ohne dass sie dabei ihre Berufsgeheimnispflichten verletzen. Ein Beispiel ist die Bank, die selbstverständlich einen Anwalt zur Führung eines Prozesses gegen einen Kunden mandatieren darf, und umgekehrt der Anwalt eine Bank einsetzen darf, um für einen Klienten eine Zahlung an eine Gegenpartei durchzuführen. In beiden Fällen käme niemand auf die Idee, dass dem Geheimnisherr eine Mitsprache mit Bezug auf die Frage eingeräumt werden müsste, ob und welcher Anwalt oder welche Bank vom Berufsgeheimnisträger beigezogen werden darf. Dass diese nebst ihren eigenen Arbeitnehmern (auch diese sind notabene Hilfspersonen) noch weitere Hilfspersonen einsetzt (z.B. die Bank, die ihr Rechenzentrum durch Dritte betreiben lässt, was unbestritten zulässig ist), die wiederum auf Arbeitnehmer als Hilfspersonen zurückgreifen (was bereits als Subsubdelegation der Datenbearbeitung qualifiziert), wird ebenso selbstverständlich akzeptiert.

[35] Schon diese beiden Beispiele zeigen, dass es weder ein absolutes Verbot der Subdelegation geben kann noch in jedem Fall eine ausdrückliche Einwilligung des Geheimnisherrn braucht. Dass in den Beispielen die beigezogenen Personen ihrerseits Berufsgeheimnisträger sind (die vom Anwalt beigezogene Bank z.B. ihrerseits dem Bankgeheimnis untersteht), ändert nichts daran, denn als Hilfsperson eines Berufsgeheimnisträgers sind sie es – darin besteht Einigkeit – sowieso auch. Wenn argumentiert wird, dass der Beizug eines Dritten deshalb kein Problem darstellt, weil es sich um einen *originären* Berufsgeheimnisträger handelt, so verfängt dieses Argument höchstens soweit in dieser Situation tendenziell eine höhere Gewähr der Vertraulichkeit bestehen mag als bei einem Dritten, der selbst sonst nicht dem Berufsgeheimnis untersteht. Ob dem so ist, sei hier dahingestellt.

[36] Wie nachfolgend gezeigt wird, muss das primäre Kriterium für den Beizug eines Dritten daher nicht sein, ob er als Hilfsperson im Sinne von Art. 321 StGB gilt, sondern ob die Datensi-

cherheit und Verwendungskontrolle[68] in angemessener Weise gewährleistet ist. Kann der Berufsgeheimnisträger dies sicherstellen, kann es keine Rolle spielen, wie er dies erreicht – ob alleine oder unter Einbezug Dritter. Auch die Ausführungen in BGE 145 II 229 machen klar, dass sich die Diskussion über den Beizug von Hilfspersonen im Grunde darum dreht, wie dieses Ziel erreicht werden kann. Die kritischen Äusserungen zum Beizug von Hilfspersonen erscheinen in erster Linie als Ausdruck des Zweifels, dass bei einem allzu lockeren Umgang mit dem Beizug von Hilfspersonen eine angemessene Datensicherheit noch gegeben ist. Es ging dem Bundesgericht punkto Beizug Dritter offensichtlich um die Frage des «wie» und nicht des «ob» (dazu ausführlich noch N 58 ff.).

2. Grundprinzip: Pflicht zur angemessenen Datensicherheit und Verwendungskontrolle

[37] Wird der Meinungsstreit zwischen Wohlers und Schwarzenegger et al. vor diesem Hintergrund abstrahiert und aus der Distanz betrachtet, so wird klar, dass die beiden Positionen sich im Kern darin unterscheiden, *wer* das mit dem Beizug von Dritten verbundene Risiko der Datensicherheit einzuschätzen hat. Während ersterer der Ansicht ist, dies sei Sache des Geheimnisherrn und daher die Voraussetzungen für den Beizug Dritter ohne Einwilligung entsprechend eng formuliert, sind letztere der Ansicht, dass es Sache des Berufsgeheimnisträgers ist sicherzustellen, dass der Beizug kein unangemessenes Risiko für den Geheimnisherrn bzw. seine Daten mit sich bringt, also «risikoadäquat» erfolgt. Bei Lichte betrachtet ist das eine und das andere jedoch nur eine unterschiedliche Seite *derselben Medaille* und lässt sich durchaus in Einklang bringen.

[38] Um diesen Meinungsstreit aufzulösen, ist zunächst allerdings ein «Realitätscheck» zur Frage vonnöten, wem *nach dem Verständnis aller Beteiligter* die Einschätzung des Risikos eines Beizugs von Cloud-Providern in der Praxis wirklich zukommt, denn dieses Verständnis ist letztlich entscheidend für die Auslegung der Vereinbarung zwischen den Beteiligten, die wiederum die Tragweite des Berufsgeheimnisses bestimmt.

[39] Dazu drei Erfahrungswerte aus der Praxis, die weitgehend unbestritten sein dürften:

a. Die *erste Realität* ist, dass unabhängig von der Branche oder der Berufsgeheimnisnorm ein Kunde (d.h. der Geheimnisherr) normalerweise will, dass sein Anwalt, Arzt oder Bankier (d.h. der Berufsgeheimnisträger) die ihm anvertrauten Daten so schützt, dass keiner sie für andere Zwecke als seine Sache verwendet. Daraus ergibt sich wiederum die Notwendigkeit, die Preisgabe solcher Daten zu kontrollieren. Wenn keine besonderen Umstände vorliegen, muss davon ausgegangen werden, dass kein Kunde eine Preisgabe an Unberechtigte will (und überdies auch kein Berufsgeheimnisträger so etwas erleben möchte). Gleichzeitig ist klar und akzeptiert, dass fast jeder Berufsgeheimnisträger bestimmte Personen einweihen muss, um seine Leistungen vernünftig zu erbringen, und dass es eine absolute Datensicherheit nicht gibt. Es verbleibt *immer* ein Restrisiko eines Zugriffs unerwünschter Dritter

[68] Mit «Datensicherheit und Verwendungskontrolle» ist hier – wie nachfolgend dargelegt – gemeint, dass die Daten vor einer Preisgabe gegenüber Unberechtigten (einschliesslich etwaiger ausländischer Behörden über einen *Lawful Access*) und sonst vor einer Verwendung für andere Zwecke als jene des Kunden angemessen geschützt sind.

(oder eines Missbrauchs der Daten durch befugterweise eingeweihte Personen[69]). Das ist allgemein akzeptiert. Ob dieses Risiko sich dadurch verwirklicht, dass dem Berufsgeheimnisträger ein ungesicherter Memorystick mit heiklen Daten aus der eigenen Mappe gestohlen wird oder der Mitarbeiter eines Providers ihm anvertraute heikle Daten kopiert, um sie Dritten zu geben, macht für den Geheimnisherrn keinen Unterschied: Seine Daten sind ausser Kontrolle. Entscheidend ist daher, dass es *nicht* zu einer solchen Situation kommt.

b. Die *zweite Realität* ist, dass im Bereich der elektronischen Datenverarbeitung die Vorstellung, dass der Berufsgeheimnisträger alleine besser in der Lage ist, die Datensicherheit zu gewährleisten, antiquiert ist. Nicht selten ist das Gegenteil der Fall, haben professionelle Provider doch oft wesentlich mehr Mittel und Know-how, eine angemessene Datensicherheit zu gewährleisten. Diese Frage ist (auch im Hinblick auf BGE 145 II 229) von der Frage zu unterscheiden, wer letztendlich die Gesamtverantwortung für die Datensicherheit trägt. Das kann und wird der Berufsgeheimnisträger selbst sein, aber er wird die konkrete Umsetzung in aller Regel delegieren müssen. Auch in einem Unternehmen kann der Chef oder die Chefin nicht alles selbst machen.

c. Die *dritte Realität* ist, dass der Kunde normalerweise nicht in der Lage ist, die Datensicherheit bzw. das Restrisiko einer Verletzung der Datensicherheit beim Berufsgeheimnisträger objektiv und fachgerecht zu beurteilen. Das gilt selbst dann, wenn der Kunde des Anwalts, der Bank oder anderen Berufsgeheimnisträgers weiss, welchen Provider dieser beiziehen will. Tatsache ist, dass selbst viele Berufsgeheimnisträger ihre Mühe haben, dieses Risiko zu beurteilen – vor allem mit Bezug auf das Risiko eines Zugriffs durch ausländische Behörden im Falle eines ausländischen Providers. Selbst die Lehre lieferte gerade zu letzterem Punkt bisher keine vernünftige Handhabe. Das ist erfahrungsgemäss der Grund, warum viele Berufsgeheimnisträger den Beizug von ausländischen Cloud-Providern scheuen: Sie können das Risiko eines solchen *Lawful Access* im Ausland schlicht nicht einschätzen.

[40] Weil sich auch die Kunden eines Berufsgeheimnisträgers dieser Realitäten bewusst sind, ergibt sich die *vierte Realität*, dass es für sie in aller Regel einzig darauf ankommt, dass der Berufsgeheimnisträger die Bearbeitung seiner Daten mit entsprechenden technischen und organisatorischen Massnahmen *insgesamt* so ausgestaltet, dass die Wahrscheinlichkeit, dass es zu einer unerwünschten Preisgabe oder Verwendung seiner Daten kommt, hinreichend gering ist. Ist also dem *Risiko einer Verletzung der Datensicherheit* angemessen vorgebeugt, wird es für den Kunden normalerweise keine Rolle mehr spielen, ob und welche Dritte beigezogen wurden.

[41] Natürlich wird kein Kunde wollen, dass sein Anwalt, sein Arzt oder seine Bank beliebig viele weitere Personen beizieht und ihnen Zugang zu seinen Daten gibt. Er wird es jedoch regelmässig als Sache des Berufsgeheimnisträgers erachten, wie er sich punkto seiner Datenbearbeitung organisiert und welche technischen und organisatorischen Massnahmen der Datensicherheit er trifft. Wer zum Anwalt, Arzt oder zu einer Bank geht, wird davon ausgehen, dass dieser bzw. diese *selbst* dafür zu sorgen hat, dass die ihm bzw. ihr anvertrauten Daten sicher sind und nicht zu vielen Personen zugänglich gemacht werden. Kein Bankkunde interessiert sich dafür, wie der Provider heisst, in dessen Rechenzentrum die Kernbankenlösung der Bank läuft, solange die Da-

69 Dies zählt genau genommen nicht zu einer Verletzung der Datensicherheit und stellt auch keine Verletzung des Berufsgeheimnisses dar. Zu einer solchen kommt es erst, wenn die betreffende, dem Berufsgeheimnis selbst ebenfalls unterstellte Person die Daten im Rahmen ihrer Nutzung einem Dritten zugänglich macht.

ten dort «sicher» sind – auch vor Zugriffen durch ausländische Behörden. Ist dies gewährleistet, wird es auch für den Mandanten des Anwalts oder den Patienten des Arztes keine Rolle spielen, ob seine Textverarbeitung oder Adressverwaltung auf dem Server im Keller oder in der Cloud läuft. Es ist jedem klar, dass der Anwalt und Arzt eine Textverarbeitung und Adressverwaltung braucht und irgendwie betreiben muss, und ein Kunde wird auch davon ausgehen, dass er dies möglicherweise nicht selbst tun kann oder will, weil dies nicht seine Kernkompetenz oder zu teuer ist. Indem der Kunde in diese Details nicht involviert wird, wird im Übrigen sichergestellt, dass der Anwalt, der Arzt und die Bank für ihre Wahl der beigezogenen Dritten vertraglich selbst verantwortlich bleiben.

[42] Ausnahmen sind höchstens dort gegeben, wo die Person des Dritten selbst das Problem ist, etwa weil es sich um einen Konkurrenten des Kunden handelt oder sonst befürchtet, dass er die Daten für eigene oder fremde Zwecke nutzen wird[70] (diese Frage stellt sich freilich immer – auch bei eigenen Arbeitnehmern des Berufsgeheimnisträgers), oder wo der Kunde aus anderen Gründen wie z.B. besondere interne oder gesetzliche Vorgaben und eigenes Know-how über den Beizug mitentscheiden oder diesen überwachen will (in welchem Falle er sich dies in seinem Vertrag mit dem Berufsgeheimnisträger ohnehin vorbehalten wird, ungeachtet der gesetzlichen Regelung des Berufsgeheimnisses seines Dienstleisters).

[43] Diese Ausnahmen können dazu führen, dass trotz allem eine Einwilligung des Kunden für den Beizug eines Dritten erforderlich ist (N 49 ff.). Nach der hier vertretenen Ansicht wird ein Kunde jedoch so oder so erwarten, dass sein Anwalt, Arzt oder sonst ein von ihm beauftragter Berufsgeheimnisträger dafür sorgt, dass seine Daten seitens des Berufsgeheimnisträgers nicht nur vertraulich bleiben (= Aspekt der Datensicherheit), sondern auch nicht für Zwecke verwendet werden, die nicht die seinen sind – jedenfalls solange die Daten einen Bezug zu ihm aufweisen (= Aspekt der Verwendungskontrolle). Das ist auch der Grund, warum viele *Non-Disclosure Agreements* (Vertraulichkeitserklärungen) diesen Punkt nebst der reinen Pflicht zur Geheimhaltung ebenfalls abdecken. Das DSG verlangt dies im Rahmen einer Auftragsbearbeitung ebenfalls.

[44] Diese Erwartungshaltung des Kunden, von welcher in guten Treuen auch der Berufsgeheimnisträger ausgehen muss und darf, führt rechtlich gesehen auch ohne ausdrückliche Abrede zu einer *vertraglichen Pflicht zur Datensicherheit und Verwendungskontrolle*, was hier verstanden wird als Pflicht, die Daten des Kunden angemessen vor einer Preisgabe gegenüber Unberechtigte (einschliesslich ausländische Behörden) und sonst vor einer Verwendung für andere Zwecke als jene des Kunden zu schützen.[71] Gleichzeitig muss und darf ein Berufsgeheimnisträger aus denselben Gründen mangels anderer Abrede oder Ausnahmesituation (N 49 ff.) nach dem Vertrauensprinzip davon ausgehen, dass sein Kunde die Details der Datenbearbeitung und sonstige interne Arbeitsorganisation *ihm* überlässt, d.h. er selbst bestimmen kann und muss, ob und welche Dritte er beizieht – solange eine angemessene Datensicherheit und Verwendungskontrolle gewährleistet ist. Das ist nicht nur ein «Recht», sondern auch eine Pflicht, für deren Erfüllung er nötigenfalls fachliche Expertise beziehen muss. Sie sind das Ergebnis mindestens eines normativen Konsen-

70 Vgl. etwa den Fall, in welchem Microsoft gewisse im Rahmen ihrer Cloud-Dienste anfallenden Daten auch für eigene Zwecke bzw. als Verantwortlicher nutzte; es handelte sich allerdings dem Vernehmen nach nicht um Kundendaten im engeren Sinne (vgl. z.B. https://www.privacycompany.de/datenschutz-folgenabschatzung-zeigt-risiken-bei-microsoft-office-proplus-enterprise/), kontrolliert am 3. Juli 2020.

71 Der Begriff der «Datensicherheit» wird normalerweise so verstanden, dass er nicht nur die Gewährleistung der Vertraulichkeit, sondern auch der Integrität und Verfügbarkeit der Daten umfasst, nicht jedoch eine zweckwidrige Verwendung durch den Geheimnisträger selbst.

ses, weil Berufsgeheimnisträger angesichts der genannten Realitäten mangels anderer Umstände heute davon ausgehen müssen und dürfen, dass ihre Kunden dies auch so sehen. Eine positive gesetzliche Regelung wie in Art. 13 BGFA, welcher ausdrücklich die «Wahrung des Berufsgeheimnisses» auch im Falle eines Beizugs Dritter verlangt, ist daher nicht nötig und vom Gesetzgeber auch nicht für alle Berufsgeheimnisse statuiert worden;[72] sie widerspricht dem aber auch nicht.

[45] Vor zehn Jahren hätte kaum jemand diese Schlussfolgerungen angezweifelt. Dass die Diskussion um den Beizug Dritter heute trotzdem mit viel Verunsicherung geführt wird, hat im Wesentlichen damit zu tun, dass mit Bezug auf gewisse Formen der Auslagerung der Datenbearbeitung an Dritte nicht mehr wie früher an die Sicherheit der Daten «geglaubt» wird. Das hat zwei Gründe:

a. Erstens ist aus wirtschaftlicher und funktionaler Sicht der Bedarf entstanden, Dritte nicht nur aus und in der Schweiz beizuziehen, sondern auch aus dem und im Ausland. Im Ausland oder in den Händen ausländischer Provider sind Daten in den Augen vieler mindestens gefühlt viel schlechter geschützt als in der Schweiz (was keineswegs zutreffen muss, wie der «Cryptoleaks»-Skandal zeigt). Die Schlagzeilen um den US CLOUD Act haben die Angst vor dem Ausland in besonderem Masse geschürt, auch wenn erfahrungsgemäss viele nicht wissen, was der US CLOUD Act tatsächlich bedeutet. Das gilt selbst für Datenschutzbehörden (N 4 f.). Wie erwähnt hat auch die Lehre hier bisher kaum konkrete Hilfestellung geboten. Da nützt es auch nichts darauf hinzuweisen, dass beispielsweise das Datenschutzrecht der EU, dem grosse Cloud-Provider wie Microsoft unterliegen, bisher strenger ist als jenes der Schweiz und Verstösse dagegen auch härter sanktioniert werden und Daten insofern im Ausland mitunter besser geschützt sind.
b. Zweitens verursachte der Begriff der «Cloud» in den vergangenen Jahren vielen Personen deshalb Unbehagen, weil sie sich darunter nichts Genaues vorstellen können. Sie haben den Eindruck, ihre Daten seien im Falle einer Cloud irgendwo auf der Welt und könnten von irgendwem eingesehen werden, was verständlicherweise nicht vertrauensfördernd ist.

[46] Dieser zweite Aspekt dürfte nur vorübergehender Natur sein, denn das Publikum wird sich an den Begriff und entsprechende Anwendungen gewöhnen, sie selbst immer mehr einsetzen und erkennen, dass «Cloud» lediglich ein Schlagwort ist, das unterschiedlichste Formen der Datenbearbeitung zusammenfasst und es auf die Einzelheiten ankommt. In vielen Fällen ist das, was ein Cloud-Provider tut nichts anderes als der Betrieb eines Rechenzentrums, und Rechenzentren werden seit Jahrzehnten betrieben. Der erste Aspekt hingegen ist von entscheidender Bedeutung, denn mit ihm sind zwei Probleme verbunden: Die mangelnde Durchsetzbarkeit bzw. Schutzwirkung des (Schweizer) Berufsgeheimnisses im Ausland, und das Risiko des Zugriffs durch ausländische Behörden, wenn sich Daten in ihrem Territorium befinden. Auf beides wird darum noch einzugehen sein.

[47] Wird die Pflicht zur angemessenen Datensicherheit und Verwendungskontrolle als Bestandteil der Vereinbarung zwischen Geheimnisherrn und Berufsgeheimnisträger verstanden, unter deren Wahrung der Beizug eines Cloud-Providers erlaubt ist, lassen sich auch die Positionen von Wohlers und Schwarzenegger et al. weitgehend in Einklang bringen:

72 Wie etwa dort, wo lediglich die Strafbarkeit seiner Verletzung statuiert wird.

a. Der Beizug Dritter ist zwar nicht direkt, über die Pflicht zur angemessenen Datensicherheit und Verwendungskontrolle aber indirekt vom Wissen und Willen des Geheimnisherrn gedeckt. Das ist die zentrale Forderung von Wohlers. Dass der Geheimnisherr normalerweise nicht weiss, wer und wo die Dritten sind, die der Anwalt, Arzt oder die Bank für die Durchführung ihrer Datenbearbeitung beizieht, ist richtig. Die Differenz zu Wohlers besteht darin, dass nach der hier vertretenen Ansicht der Geheimnisherr dies normalerweise gar nicht wissen will, *sofern* sichergestellt ist, dass seine Daten sicher sind und nicht zweckentfremdet werden. Gilt dies wie oben gezeigt als vereinbart, ist der Beizug eines Cloud-Providers auch vom Willen des Geheimnisherrn gedeckt. Das schliesst selbstverständlich nicht aus, dass der Berufsgeheimnisträger seine Pflicht durch einen Beizug im Einzelfall *verletzt*. Ist dies der Fall und kommt es zu einer Offenbarung z.B. gegenüber einer ausländischen Behörde, muss er entsprechend mit Vorwürfen einer Berufsgeheimnisverletzung rechnen. Die Lösung von Wohlers, eine vorgängige Einwilligung, schützt den Kunden nicht wirklich besser, es sei denn, er würde einwilligen, dass seine Daten einem Cloud-Provider im Ausland anvertraut werden dürfen, ohne dass sie sicher sein müssten. Das aber wird kein vernünftiger Kunde tun. Eine Einwilligung macht somit nur dann wirklich Sinn, wo der Kunde der Einschätzung des Providers nicht traut und daher selbst beurteilen will (und kann), ob ihm das Risiko wert ist, oder wo er von Gesetzes wegen dazu verpflichtet ist (dazu sogleich).

b. Auch Schwarzenegger et al. haben recht, wenn sie verlangen, dass der Beizug des Cloud-Providers «risikoadäquat» erfolgen muss. Denn dies bedeutet nichts anderes, als dass der Beizug nur zulässig ist, wenn trotzdem eine angemessene Datensicherheit und Verwendungskontrolle gewährleistet werden kann. Das wiederum ist anhand des durch einen Beizug geschaffenen Risikos einer unerwünschten Preisgabe und Verwendung zu beurteilen und ob eine solche hinreichend beschränkt werden kann.

[48] Zu erwähnen ist noch, dass die Normen zum Berufsgeheimnis zwar primär dem Schutz des Geheimnisherrn dienen, weshalb dessen Einwilligung zur Straflosigkeit führt. Sekundär kommt dem Berufsgeheimnis jedoch auch eine öffentliche Schutzfunktion zu.[73] Dieser Schutzfunktion wird die aufgezeigte Lösung jedoch ebenfalls gerecht, indem sie dem Geheimnisherrn ungeachtet einer Erlaubnis zum Beizug Dritter und selbst beim Fehlen einer Regelung zur Geheimhaltung einen «Basisschutz» verschafft: Der Berufsgeheimnisträger ist so oder so dafür verantwortlich, dass eine angemessene Datensicherheit und Verwendungskontrolle besteht. Das entspricht im Übrigen dem, was der Gesetzgeber für den Schutz von Personendaten in Art. 7 Abs. 1 und 10a DSG bereits vorsieht – und künftig teilweise ebenfalls strafrechtlich absichern wird.

3. Ausnahme: Spezifische oder allgemeine Einwilligung in den Beizug Dritter

[49] Die Pflicht zur angemessen Datensicherheit und Verwendungskontrolle als Basis für den Beizug eines Cloud-Providers schliesst wie erwähnt nicht aus, dass dieser ausnahmsweise einer

73 Vgl. dazu etwa das *obiter dictum* in BGE 145 IV 114, Erw. 4.2, zum Bankkundengeheimnis, das auch den kollektiven Interessen des schweizerischen Finanzplatzes diene; BGE 145 II 229, Erw. 7.1, für das Anwaltsgeheimnis.

spezifischen oder allgemeinen Einwilligung des Kunden bedarf. Ein solches Erfordernis kann sich entweder aus Gesetz oder aus Vertrag ergeben:

[50] Namentlich sieht das künftige DSG vor, dass im Falle einer *Auftragsbearbeitung* der Beizug eines Unterauftragsbearbeiters eine spezifische oder allgemeine Einwilligung des für die Datenbearbeitung Verantwortlichen erfordert (Art. 8 Abs. 3 E-DSG). Diese Regelung entspricht der Regelung der DSGVO. Gemäss DSG und DSGVO genügt jedoch eine Veto-Lösung, d.h. es reicht aus, dass der Verantwortliche vorgängig über den Beizug informiert wird und nicht widerspricht. Ein ähnliches Vorgehen verlangt seit 1. Januar 2020 auch die FINMA von Banken und Versicherungen, welche wesentliche Funktionen an Dritte auslagern und diese Dritten ihrerseits Dritte beiziehen wollen.[74] In beiden Fällen behält damit *der Kunde* die Oberverantwortung. Die Oberverantwortung behalten muss gemäss Bundesgericht wie gezeigt auch der Anwalt, der eine Hilfsperson beizieht (N 27). Für das DSG ist allerdings darauf hinzuweisen, dass ein seinerseits beigezogener Berufsgeheimnisträger im Normalfall kein Auftragsbearbeiter, sondern selbst ein für die Datenbearbeitung «Verantwortlicher» im Sinne des DSG sein wird und daher sowohl unter dem heutigen als auch dem künftigem DSG grundsätzlich nicht verpflichtet ist, für den Beizug eines Cloud-Providers die Zustimmung seines Kunden (oder den betroffenen Personen) einzuholen. So hielt es auch der Bundesrat in seiner Botschaft zum Entwurf eines revidierten DSG fest.[75] Das DSG stützt somit das vorstehend dargelegte Grundprinzip, wonach der Beizug eines Cloud-Providers grundsätzlich keiner Einwilligung bedarf. Nach DSG muss der Berufsgeheimnisträger selbst im Rahmen einer Auftragsbearbeitung lediglich sicherstellen, dass der Cloud-Provider die Daten nur so bearbeitet, wie er dies selbst auch tun darf, eine angemessene Datensicherheit gewährleistet und er Unterauftragsbearbeitern mindestens widersprechen kann.

[51] Bestehen keine gesetzlichen Einschränkungen, können sich solche allenfalls aus Vertrag ergeben. Ist dem Berufsgeheimnisträger der Beizug von Hilfspersonen vertraglich erlaubt, so wird in aller Regel auch erlaubt sein, diesen Hilfspersonen berufsgeheimnisgeschützte Daten zugänglich zu machen, soweit sie diese zur Erbringung ihrer Leistung (an den Berufsgeheimnisträger) benötigen. Ist der Beizug von Hilfspersonen unter dem Vertrag des Berufsgeheimnisträgers von einer Einwilligung des Kunden abhängig, wie dies in Datenschutzklauseln oft vorgesehen ist, so muss dies auch unter dem Berufsgeheimnis so gelten, soweit es um Personendaten geht. Ist der Beizug von Hilfspersonen zwar nicht ausdrücklich geregelt, ergibt sich jedoch aus anderen Umständen wie z.B. der zur erbringenden Leistung, dass dieser zulässig ist oder eben nicht, so wird dies unter dem Berufsgeheimnis normalerweise analog zu beachten sein.[76]

[52] Ist im Gesetz und Vertrag nichts dergleichen vorgesehen, so ist höchstens in Ausnahmefällen davon auszugehen, dass der Beizug gewisser Dritter (z.B. eines Cloud-Providers im Ausland) für einen Berufsgeheimnisträger nach dem Vertrauensprinzip trotz angemessener Datensicherheit und Verwendungskontrolle vertraglich ausgeschlossen ist. Eine solche Vertragsauslegung fällt insbesondere dann in Betracht, wenn aus der Sicht des Kunden des Berufsgeheimnisträgers

74 FINMA, Rundschreiben 2018/3 «Outsourcing», Rz. 33.

75 BBl 2017 7031 f., m.w.H.

76 Preist beispielsweise ein Unternehmen die Speicherung von Daten in einem Militärbunker in den Schweizer Alpen an, so sichert der Provider im Ergebnis zu, dass die Daten genau dort gespeichert werden und nicht in einer Cloud im Ausland.

a. der Berufsgeheimnisträger durch sein Verhalten die Erwartungshaltung des Kunden geweckt hat, keinen solchen Dritten beizuziehen;
b. der Beizug eines Dritten in der geplanten Form in der betreffenden Branche ungewöhnlich ist, d.h. seitens des Kunden nicht damit gerechnet werden muss;
c. die Daten bzw. Tätigkeiten so sensitiv sind, dass seitens des Kunden vernünftigerweise nicht davon ausgegangen werden kann, dass eine angemessene Datensicherheit und Verwendungskontrolle gewährleistet ist (z.B. wenn die Hilfsperson in einem Interessenkonflikt bezüglich der Eigenverwendung der Daten steht); oder
d. die oben zitierten «Realitäten» im konkreten Fall in anderer Hinsicht nicht zutreffen und daher der (normative oder tatsächliche) Konsens der Parteien bezüglich dem, was gilt, ein anderer ist.

4. Gilt das Grundprinzip auch für den Beizug von Cloud-Providern aus dem Ausland?

[53] Wird das obige Grundprinzip angewandt, so kann es konzeptionell ebenfalls nicht mehr darauf ankommen, ob sich ein beigezogener Cloud-Provider im Ausland befindet oder nicht, da diesem Aspekt bereits bei der Beurteilung der Datensicherheit Rechnung getragen wird. Es wird nur aber immerhin beurteilt werden müssen, ob und inwiefern eine unerwünschte Preisgabe und Verwendung der Daten (insbesondere im Rahmen eines *Lawful Access* durch eine ausländische Behörde) dadurch wahrscheinlicher wird, dass der Cloud-Provider sich im Ausland befindet oder dort Daten bearbeitet, und ob das Restrisiko nach wie vor akzeptabel ist.

[54] Das ist auch bei sensitiven Daten keineswegs ausgeschlossen. So geht das Bundesamt für Gesundheit in seinem Kreisschreiben 7.1 davon aus, dass auf die Auslagerung der Bearbeitung von besonders schützenswerten Personendaten durch einen Krankenversicherer ins Ausland «wenn immer möglich» zu verzichten ist, schliesst im Umkehrschluss eine solche Auslagerung trotz gesetzlicher Schweigepflicht aber nicht aus.[77] Solche Auslagerungen werden heute in verschiedenster Hinsicht praktiziert, im Übrigen auch in anderen Bereichen des Gesundheitswesens, wo Art. 321 StGB greift. Auch Schwarzenegger et al., WalderWyss und LauxLawyers sehen wie oben dargelegt keinen Grund, dem Berufsgeheimnisträger den Beizug von Cloud-Providern im Ausland zu untersagen, soweit die Datensicherheit sichergestellt ist.

[55] Der Umstand, dass Strafnormen wie Art. 321 StGB und Art. 47 BankG sich gegen einen ausländischen Provider und dessen Arbeitnehmer *de facto* nicht durchsetzen lassen, schliesst dessen Beizug daher nicht aus, sofern auch dieser Umstand bei der Risikobeurteilung beachtet wurde: Steigt die Wahrscheinlichkeit, dass ein Mitarbeiter geheime Daten einer unbefugten Person zugänglich macht, wenn er dafür von den Schweizer Strafverfolgungsbehörden faktisch nicht verfolgt werden kann, weil er sich nicht in der Schweiz befindet? Wird dies verneint, weil der Mitarbeiter trotzdem eine Strafverfolgung nach Schweizer Recht befürchtet (was häufig der Fall ist[78]), dem Mitarbeiter stattdessen eine Verfolgung nach ausländischem Recht droht oder er der-

77 Bundesamt für Gesundheit, Kreisschreiben Nr. 7.1, 1. Januar 2016, S. 5.

78 Dies belegen zahlreiche Erfahrungen im Bereich des Bankgeheimnisses und Art. 273 StGB (wirtschaftlicher Nachrichtendienst). Ein typischer Fall sind US-Anwälte, die von einem Schweizer Unternehmen im Zusammenhang mit

art rechtschaffen ist, dass er die Geheimhaltung auch ohne Strafdrohung respektiert, dann spielt die fehlende Durchsetzbarkeit des Berufsgeheimnisses keine Rolle mehr. Es verbleibt in diesem Fall lediglich das Risiko eines *Lawful Access* im Ausland, was separat zu beurteilen ist. Wird die Frage bejaht, dann werden andere Massnahmen getroffen werden müssen, um dieses Manko zu kompensieren.

[56] Die Erfahrung zeigt, dass strafrechtliche Drohungen zwar eine gewisse abschreckende Wirkung haben, sich eine Abschreckung aber auch anders erzielen lässt und sie keineswegs zuverlässig vor einer unerwünschten Preisgabe geheimer Daten schützt. Kommt hinzu, dass zur angemessenen Datensicherheit nicht nur der Schutz vor unerwünschten Preisgaben gehört, sondern auch die Verwendungskontrolle. Diese decken die Strafnormen des Berufsgeheimnisses ebenso wenig ab wie weitere technische und organisatorische Massnahmen zum Geheimnisschutz. Pauschal zu verlangen, dass eine Hilfsperson als solche direkt dem Berufsgeheimnis unterstehen muss, wäre daher falsch. Zivilrechtliche Geheimhaltungsverbote mit entsprechenden Sanktionen können im Gegenteil sogar wesentlich wirksamer sein, da sich unter ihnen Verstösse einfacher und rascher sanktionieren lassen als auf dem Weg über das Strafrecht. Die Erfahrung zeigt auch, dass ein hohes Risiko der Aufdeckung eines Datenmissbrauchs abschreckender wirkt als die hohe Sanktion einer solchen Tat.

[57] Von der fehlenden Durchsetzbarkeit von Art. 321 StGB und vergleichbaren Bestimmungen zu trennen ist die Frage, ob der beigezogene Dritte deshalb nicht unter diese Bestimmungen fällt, weil er nicht mehr als Hilfsperson des Berufsgeheimnisträgers gilt. Geschieht dies in der Schweiz, wäre dies rechtlich problematischer, weil dann unter Umständen auch die Zeugnisverweigerungsrechte und Beschlagnahmungsverbote der diversen Schweizer Prozessgesetze nicht mehr greifen und ein *Lawful Access* in der *Schweiz* droht; diese Frage soll hier allerdings aufgrund ihrer eher theoretischen Natur nicht vertieft werden. Fällt ein ausländischer Dritter nicht darunter, ergibt sich dieses Problem hingegen nicht, da er dannzumal ohnehin nicht im Hoheitsbereich der Schweizer Behörden wäre.

5. Ist die Subdelegation nach BGE 145 II 229 noch zulässig?

[58] Den vorstehenden Ausführungen steht auch der bereits zitierte BGE 145 II 229 nicht entgegen, obwohl der Entscheid auf den ersten Blick den Eindruck erweckt, dass er den Einsatz von Untergehilfen jedenfalls bei Anwälten untersagt und damit den Einsatz von Cloud-Providern faktisch verunmöglicht.

[59] Auf den zweiten Blick tut der Entscheid dies jedoch nicht, sondern differenziert: Das Bundesgericht begründete die Unzulässigkeit der Subdelegation an einen Dritten damit, dass in diesem Fall der Dritte nicht nur nicht dem Anwalt untersteht, sondern «auch nicht» seiner Hilfsperson.[79] Daraus lässt sich im Umkehrschluss folgern, dass es sich *nicht* zur Konstellation äusserte, in welcher der Untergehilfe zwar nicht direkt dem Anwalt, wohl aber seiner Hilfsperson «untersteht». In Tat und Wahrheit deutet der Sachverhalt des beurteilten Einzelfalls darauf hin, dass es im kon-

Informationsersuchen von US-Behörden beigezogen werden. Werden diese darüber informiert, dass die Herausgabe der Unterlagen unter Schweizer Recht strafbar sein könnte, weigern sich viele von diesen, an einer solchen Herausgabe mitzuwirken, auch wenn ihnen klar ist, dass das Risiko einer persönlichen Strafverfolgung für sie selbst gering ist. Sie sind jedoch schlicht nicht bereit, dieses Risiko nur für ihren Kunden oder Arbeitgeber einzugehen.

79 BGE 145 II 229, Erw. 7.3.

kreten Fall um einen Dritten ging, der zwar zur Geheimhaltung verpflichtet war, aber offenbar *unabhängig* operierte und von der Hilfsperson des Anwalts in eigener Regie beigezogen wurde (*i.c.* um dem Anwalt einen Telefondienst zu erbringen).

[60] Vor diesem Hintergrund ist die Differenzierung des Bundesgerichts nachvollziehbar, denn der Begriff der Hilfsperson nach Art. 101 OR erfordert nicht zwangsläufig ein Subordinationsverhältnis zum Geschäftsherrn: Eine Hilfsperson kann auch weisungs*ungebunden* sein. Eine solche Situation wollte das Bundesgericht jedenfalls bei Untergehilfen eines Anwalts offenbar verhindern. So gesehen schliesst BGE 145 II 229 den Beizug von Untergehilfen nur dann aus, als der Anwalt gegenüber diesen weder direkt noch indirekt (d.h. über seine Hilfspersonen) ein Weisungsrecht hat.

[61] Hat also der Anwalt ein Weisungsrecht auch mit Bezug auf Untergehilfen seiner Hilfspersonen (einschliesslich deren Beizug), so sind auch Untergehilfen erlaubt, also Hilfspersonen, mit denen er keinen direkten Vertrag und keine direkte Beziehung hat. Selbstverständlich muss das Weisungsrecht über die gesamte Kette wirksam sein, der Anwalt muss es tatsächlich auch ausüben und seine Einhaltung kontrollieren. Aus den Ausführungen des Bundesgerichts wird deutlich, dass deren Einsatz so ausgestaltet sein muss, dass die «primäre» Verantwortung («responsabilité première») für die Einhaltung des Berufsgeheimnisses durch Hilfspersonen weiterhin beim Anwalt liegt.[80] Das bedeutet im Umkehrschluss aber nichts anderes, als dass eine gewisse Verantwortung auch an die Hilfsperson (oder Dritte[81]) delegiert werden kann; von einer primären Verantwortung zu sprechen macht nur Sinn, wenn es auch eine sekundäre gibt.

[62] Beim Einsatz von Cloud-Providern durch einen Berufsgeheimnisträger wird eine solche Subordination an der Tagesordnung sein, da sie regelmässig als Auftragsbearbeiter gelten. Für diese verlangt das DSG im Ergebnis bereits heute, dass sie unter ein Weisungsrecht ihres Kunden gestellt werden, dass diese über die ganze Kette an Unterauftragsbearbeitern wirksam ist und dass auch hier die primäre Verantwortung beim Kunden als «Verantwortlichen» bleibt.

[63] Das Bundesgericht zählt im Entscheid überdies selbst diverse Beispiele des Beizugs Dritter auf, die genau so ausgestaltet sind und die es offenkundig als zulässig erachtet, so namentlich Banken, Übersetzungsdienste und sogar Provider zur «Aufbewahrung von Daten in der Ferne». Sie alle kommen ihrerseits nicht ohne eigene Arbeitnehmer und weitere Hilfspersonen aus, und auch bei diesen haben nicht alle ein direktes Vertragsverhältnis mit dem Anwalt.[82] Es muss also nicht davon ausgegangen werden, dass das Bundesgericht den Einsatz von Cloud-Providern untersagen wollte, selbst wenn diese ihrerseits Hilfspersonen einsetzen. Im Gegenteil hat es mit den erwähnten «Fern»-Providern wohl genau Cloud-Provider gemeint, zumal es mehrfach aus mehreren Aufsätzen zu genau diesem Thema zitiert. All die genannten Beispiele können auch einer strengeren Lesart des Entscheids entgegengehalten werden, wonach die Subdelegation zwar erlaubt ist, aber nur an Arbeitnehmer des beigezogenen Dritten; sie wären bei einer solchen Interpretation nicht mehr möglich.

80 BGE 145 II 229, Erw. 7.4.

81 Zum Beispiel Stellen, die die Einhaltung der Datensicherheit bei Hilfspersonen und Untergehilfen überprüfen und bestätigen, wie Cloud-Provider sie regelmässig einsetzen.

82 BGE 145 II 229, Erw. 7.3.

6. Weitere Voraussetzungen für den Beizug von Cloud-Providern?

[64] In seinem Entscheid BGE 145 II 229 erwähnt das Bundesgericht eine Reihe von weiteren Anforderungen an den Beizug von Hilfspersonen, wie namentlich deren sorgfältige Auswahl, deren Unterstellung unter das Anwaltsgeheimnis und deren Überwachung sowie eine über das gesetzliche Minimum hinausgehende Haftung der Hilfsperson (N 26 f.). Weitere Voraussetzungen für den Beizug eines Cloud-Providers sind dies allerdings nicht, denn sie alle zählen zu dem, was als angemessene Datensicherheit bezeichnet werden kann. Das Bundesgericht spricht selbst von hinreichenden Massnahmen zur Datensicherheit bzw. Massnahmen, die zu treffen sind, um eine Verletzung des Berufsgeheimnisses zu vermeiden.[83]

[65] Nebst der angemessenen Datensicherheit erwähnt das Bundesgericht als weitere Voraussetzung schliesslich eine «vernünftige» Beschränkung des Kreises der Personen mit Zugang zu geheimen Informationen.[84] Ein Erfordernis der Beschränkung des Informationszugangs nach dem Grundsatz «need to know» ergibt sich für Personendaten bereits aus dem Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG), kann als organisatorische Massnahme der Datensicherheit qualifiziert werden und ist auch in der Lehre anerkannt. Unterschiedlich sind die Lehrmeinungen dahingehend, *woran* die Notwendigkeit gemessen werden soll, damit der Berufsgeheimnisträger für den Beizug nicht um eine Einwilligung ersuchen muss: Muss der Beizug *für die Erbringung der Leistung* zwingend geboten sein, wie Wohlers vertritt (vgl. oben N 15), oder muss es lediglich *für eine sinnvolle Arbeitsteilung im Betrieb* erforderlich sein, einen Dritten beizuziehen, wie Schwarzenegger et al. der Meinung sind (vgl. oben N 19). WalderWyss wiederum verlangen für den Fall der Bank ähnliches in anderen Worten, nämlich ein *vernünftiges Interesse* des auslagernden Geheimnisträgers am Beizug eines Cloud-Providers und dass dieser die Leistung weiterhin *schwergewichtig selbst* erbringt (vgl. oben N 23).

[66] Den beiden letztgenannten Ansichten ist im Wesentlichen zuzustimmen: Der Beizug Dritter darf die Leistungserbringung an den Kunden auch nur indirekt unterstützen. So erbringt ein Anwalt seinen Klienten normalerweise Anwalts- und nicht IT-Dienstleistungen. Für seine Leistungserbringung ist der Beizug eines Dritten zum Betrieb seiner IT-Systeme daher nicht «zwingend geboten», wie Wohlers es verlangt: Der Anwalt könnte die Server auch selbst betreiben, genauso wie er Texte für seine Arbeit zum Beispiel auch selbst übersetzen könnte. Trotzdem wird völlig unbestritten sein, dass er für den Betrieb seiner Server auch ohne Einwilligung seines Kunden einen IT-Dienstleister und für seine fremdsprachigen Texte einen externen Übersetzer beiziehen darf. Entscheidend ist, dass der Beizug nötig ist, um die *vernünftigen eigenen Ansprüche des Berufsgeheimnisträgers an die Durchführung seiner Tätigkeit* zu erfüllen, also beispielsweise dem effizienten, zuverlässigen, sicheren oder wirtschaftlichen Betrieb seiner IT-Systeme und die kostengünstige und für ihn zeitsparende Übersetzung. Das steht der Position von Wohlers genau genommen nicht einmal entgegen, handelt es sich bei diesen Tätigkeiten doch um Aktivitäten, bei welchen der Kunde die Wahl der Mittel unter Vorbehalt der Datensicherheit und Verwendungskontrolle wie gezeigt *dem Berufsgeheimnisträger* auferlegt und überlassen hat und dieser im vernünftigem Rahmen somit mit Willen seines Kunden selbst bestimmen können muss, was für seine Arbeit «nötig» ist und wie er sie erledigt. Dafür muss der Berufsgeheimnisträger am Ende

83 BGE 145 II 229, Erw. 7.2 und 7.4.

84 BGE 145 II 229, Erw. 7.4.

der Tage auch einstehen. Solange dabei eine angemessene Datensicherheit gewährleistet bleibt, ist auch das Berufsgeheimnis nicht in Gefahr.

[67] Dass diese Dritten alle als «Hilfspersonen» im Sinne von Art. 321 StGB gelten und damit direkt dem Berufsgeheimnis unterstehen, dürfte weitgehend anerkannt sein, jedenfalls soweit ihre Tätigkeit eine Kenntnisnahme von geheimnisgeschützten Daten mit sich bringen kann.[85] Ist die Datensicherheit anderweitig gewährleistet, ist dies jedoch nach der hier vertretenen Ansicht keine zwingende Voraussetzung für deren Beizug (vgl. auch N 53 ff.). Auch eine Aussage des Bundesgerichts im bereits zitierten Entscheid kann dahingehend interpretiert werden: Im Rahmen der Sorgfaltspflichten verlangt es vom Anwalt, dass er seine Hilfspersonen über das Berufsgeheimnis belehren und «wenn nötig» eine Vertraulichkeitsvereinbarung unterzeichnen lässt («de les instruier sur le secret professionnel, le cas échéant par la signature d'un accord de confidentialité, . . . »):[86] Eine Vertraulichkeits*vereinbarung* ist gemeinhin nur dann «nötig», wenn die Hilfsperson nicht schon von Gesetzes wegen dem Berufsgeheimnis untersteht. Offenbar ging das Bundesgericht davon aus, dass dies nicht zwingend der Fall sein muss. Mit einer Vertraulichkeitsvereinbarung kann notabene im Falle von Geschäftsgeheimnissen über Art. 162 StGB oder Art. 273 StGB trotz allem ein strafrechtlicher Schutz herbeigeführt werden, wobei im Falle einer Verletzung von Art. 273 StGB das Weltrechtsprinzip gilt (Art. 4 Abs. 1 StGB), d.h. das Schweizer Strafrecht auch dann anwendbar ist, wenn die Tat vollumfänglich im Ausland verübt wurde.

[68] Im Zusammenhang mit dem Beizug von Cloud-Providern stellt sich schliesslich noch die Frage, ob die Kunden als Geheimnisherrn darüber zu informieren sind. Streng genommen verlangt das Berufsgeheimnis *keine* solche Information. Eine solche wäre nur erforderlich, wenn der Geheimnisherr um eine Einwilligung in den Beizug gebeten wird, doch dies ist – wie gezeigt – nur ausnahmsweise nötig. Es ist jedoch davon auszugehen, dass das Publikum eine Information zunehmend erwarten wird. Andere Gesetze erfordern sie in Kürze ohnehin: Im künftigen DSG wird eine generelle Informationspflicht eingeführt, die auch Angaben zu den Kategorien von Datenempfängern und die Länder erfordert, in welche Personendaten bekanntgegeben werden (Art. 17 E-DSG). Der Name des Cloud-Anbieters muss nicht erwähnt werden. In aller Regel genügt der Hinweis auf den Beizug von Auftragsbearbeitern und weiteren Dienstleister. Aus dem Auftragsrecht lässt sich eine Informationspflicht ebenfalls ableiten, soweit der Beizug eines Cloud-Providers für einen Auftraggeber ein relevanter Aspekt für die Weiterführung oder Kündigung des Mandats sein kann.

7. Übertragbarkeit auf andere Berufsgeheimnisse?

[69] Der vorstehend zitierte Entscheid des Bundesgerichts erging ausschliesslich zu Art. 13 Abs. 2 BGFA, der das Berufsgeheimnis von Anwälten statuiert. Da das Anwaltsgeheimnis aufgrund seiner Wichtigkeit gemäss Bundesgericht hinsichtlich dessen Kontrolle durch den Anwalt besonders streng zu handhaben ist,[87] ist nicht zu erwarten, dass für andere Berufsgeheimnisse und den Schutz von Geschäftsgeheimnissen nach Art. 162 StGB noch strengere Regeln gelten.

85 Schwarzenegger et al. (Fn. 7), S. 17 f., m.w.H.

86 BGE 145 II 229, Erw. 7.2.

87 BGE 145 II 229, Erw. 7.4.

[70] Auch die Frage, ob die Figur der Hilfsperson nach Art. 13 Abs. 2 BGFA jener von Art. 321 StGB entspricht, kann an dieser Stelle offenbleiben. Zwar mag die Hilfsperson nach Art. 321 StGB je nach Ansicht enger verstanden werden. Für die vorliegende Diskussion ist dies jedoch irrelevant, da der zitierte Entscheid zu Art. 13 Abs. 2 BGFA für den Fall des Cloud-Providers keine nennenswerte Einschränkung mit sich bringt, und sich die Zulässigkeit des Beizugs eines Cloud-Providers nicht danach bestimmt, ob er als Hilfsperson nach Art. 321 StGB gilt. Nach der hier vertretenen Ansicht dient Art. 321 StGB (und das Zeugnisverweigerungsrecht in den Prozessgesetzen) nicht der Legitimation des beigezogenen Dritten, sondern dem Schutz des Geheimnisherrn, indem es jene, die tatsächlich beigezogen wurden und Zugang zu seinen Daten hatten, durch eine Strafdrohung zusätzlich zur Geheimhaltung motiviert.

[71] Es sind auch keine Gründe ersichtlich, warum das für Art. 321 StGB und Art. 47 BankG oben entwickelte und dargelegte Grundprinzip für den Beizug von Cloud-Providern nicht auch für andere Berufsgeheimnisse und gesetzlichen Pflichten zum Schutz von Geschäftsgeheimnissen (und das Amtsgeheimnis) gelten sollte. Ob diese Geheimnispflichten nur jeweils dem Geheimhaltungsinteresse des Geheimnisherrn oder auch öffentlichen Interessen dienen, spielt – wie gezeigt (N 48) – keine Rolle, da ein Beizug ohnehin nur dann erlaubt ist, wenn die Datensicherheit und Verwendungskontrolle angemessen bleibt. Dieses Kriterium erlaubt es, der Sensitivität der Daten bzw. der Risikolage für jede Art von Berufsgeheimnis gerecht zu werden: Während somit der Beizug eines ausländischen Cloud-Providers bei dem Arztgeheimnis unterliegenden Daten ohne Weiteres zulässig sein kann, weil das Risiko eines *Lawful Access* im Ausland schon aufgrund der Natur der Daten gering ist, mag die Beurteilung im Falle militärischer Daten, an denen ausländische Behörden womöglich sehr viel höheres Interesse haben, eine andere sein und dem Beizug des Dritten mithin entgegenstehen, wenn sich das Offenbarungsrisiko im Ausland aller Massnahmen zum Trotz nicht hinreichend tief halten lässt.

[72] Die obigen Ausführungen gelten nach der hier vertretenen Ansicht im Übrigen auch für jene Geheimhaltungspflichten, die nicht wie Art. 321 StGB oder Art. 47 BankG eine Regelung für «Hilfspersonen» oder «Beauftragte» vorsehen, wie etwa Art. 162 StGB, Art. 320 StGB, Art. 33 ATSG oder auch Art. 35 DSG: Eine solche separate Erwähnung ist nicht erforderlich, wenn Hilfspersonen aufgrund der neutralen Formulierung direkt erfasst sind (Beispiel: «Personen, die an der Durchführung … beteiligt sind, haben …»[88]), und selbst wo dem nicht so wäre ist nach der hier vertretenen Auffassung die Strafbarkeit einer Hilfsperson für den Fall der Offenbarung grundsätzlich keine Voraussetzung für deren Beizug, sondern höchstens die Folge davon (dazu N 53 ff. und N 67).

8. Zusammenfassung

[73] Zusammenfassend darf ein Berufsgeheimnisträger einen Cloud-Provider für seine Datenbearbeitung mangels anderer Abrede beiziehen, wenn:

a. Die Datensicherheit und Verwendungskontrolle weiterhin angemessen ist, d.h. die Daten auch beim Cloud-Provider vor einer Preisgabe gegenüber Unberechtigten (einschliesslich

88 Art. 33 ATSG.

etwaiger ausländischer Behörden über einen *Lawful Access*) und sonst vor einer Verwendung für andere Zwecke als jene des Kunden angemessen geschützt sind;

b. Der Beizug nötig ist, um die vernünftigen Ansprüche des Berufsgeheimnisträgers an die Durchführung seiner Tätigkeit (z.B. hinsichtlich Leistungsfähigkeit, Zuverlässigkeit, Sicherheit, Funktionalität oder Wirtschaftlichkeit seiner Systeme) zu erfüllen;

c. Keine Umstände dem Kunden nahelegen, dass der Berufsgeheimnisträger einen Cloud-Provider nicht oder nur unter weiteren Voraussetzungen beizieht, namentlich wenn ein Beizug ungewöhnlich wäre, es der geweckten Erwartung oder der vereinbarten Leistung widerspricht oder der Kunde davon ausgehen muss, dass eine angemessene Datensicherheit nicht möglich ist;

d. Keine gesetzliche Pflicht eine spezifische oder allgemeine Einwilligung erfordert, so etwa im Falle einer Auftragsbearbeitung unter dem künftigen DSG;

e. Zwischen dem Berufsgeheimnisträger und dem Cloud-Provider (und von diesem beigezogenen Dritten) ein effektives Subordinationsverhältnis besteht, auch wenn das Weisungsrecht gegenüber gewissen Dritten nur indirekt besteht.

[74] Ferner sollte der Kunde spätestens unter dem künftigen DSG in allgemeiner Form über den Beizug von Providern informiert werden, einschliesslich darüber, wo im Ausland sich diese gegebenenfalls befinden.

E. Angemessenheit der Datensicherheit und Verwendungskontrolle

1. Welche Risiken sind relevant?

[75] Traditionell zielte die von einem Berufsgeheimnisträger zu gewährleistende Datensicherheit und Verwendungskontrolle primär auf die Abwehr von widerrechtlich handelnden Angreifern (z.B. Hacker, Autoren von Malware, interne Datendiebe) und die Vermeidung von fahrlässigen Datenpannen (z.B. verlorene Datenträger). Solange sich die Daten ausschliesslich in der Schweiz befanden und bearbeitet wurden, genügte dies selbst im Falle eines Outsourcing-Providers. Diese Form der Datensicherheit (und Verwendungskontrolle) warf und wirft denn auch keine besonderen Fragen auf. Es bestehen gute Erfahrungswerte, welche technischen und organisatorischen Massnahmen nötig sind, um ein angemessenes Niveau an Datensicherheit zur Verhinderung solcher Angriffe zu schaffen. Darum wird dieser Aspekt der Datensicherheit hier nicht weiter vertieft.

[76] Immerhin ist zu erwähnen, dass diese «traditionelle» Datensicherheit nicht unterschätzt werden sollte. Das betrifft nicht nur die Gewährleistung des Schutzguts der Vertraulichkeit, sondern auch jener der Integrität und Verfügbarkeit: Wie wird sichergestellt, dass nach erfolgter Auslagerung die Daten und Funktionen, für die nun ein Dritter verantwortlich zeichnet, gewährleistet werden kann und wie gut? Wie ist insgesamt die Business Continuity sichergestellt? Und wie sieht es mit der Rückführbarkeit aus, sollte der Vertrag mit dem Dritten beendet werden müssen, was früher oder später immer der Fall sein wird? Diese Fragen sind auch beim Beizug von weit verbreiteten Standard-Angeboten zu stellen und die Antwort des Managements darauf mitsamt den Erwägungen und getroffenen Massnahmen zu dokumentieren, weil hierbei immer Risiken eingegangen werden. Das ist nichts schlechtes; auch beim «inhouse»-Betrieb der Informatik gibt

es solche, aber solch gewichtige Entscheide sollten in Kenntnis der Fakten und Risiken erfolgen und dies sollte im Sinne einer sauberen Governance auch dokumentiert sein.

[77] Seitdem Berufsgeheimnisträger jedoch nicht nur ein Interesse am Beizug von Dritten in der Schweiz haben, sondern solche auch im Ausland einsetzen möchten, besteht nebst den traditionellen Bedrohungen der Datensicherheit eine zusätzliche Bedrohung: Abzuwehren sind nicht nur widerrechtlich handelnde Angreifer, Fehlmanipulationen und technische Störungen, sondern auch auf ihrem Territorium rechtmässig handelnde ausländische Behörden. Möchten sie an Daten gelangen, die ein Berufsgeheimnisträger in der Schweiz hat, nutzen sie nicht mehr Amts- oder Rechtshilfe, um über die Schweizer Behörden an die Daten zu gelangen. Befindet sich der Provider des Berufsgeheimnisträgers in ihrem Land, werden sie sich die Daten unter Umständen direkt von ihm «holen». Hierzu können sie sich normalerweise auf ihr eigenes Recht stützen und ihm einen Herausgabebefehl vorlegen. Ist dieser nach lokalem Recht korrekt ergangen, wird ihm der Provider normalerweise Folge leisten, soweit er dazu technisch in der Lage ist. Sein Kunde, der Berufsgeheimnisträger, wird einen solchen *Lawful Access* normalerweise nicht verhindern können.

[78] Kommt es zu einer solchen Herausgabe, so liegt aus Schweizer Sicht eine strafbare Offenbarung vor, weil die Daten in die Hände von (aus Schweizer Sicht) unbefugten Personen (der ausländischen Behörde) gelangt sind. Dieses Risiko eines *Lawful Access* im Ausland ist in der öffentlichen Diskussion das Hauptproblem des Beizugs von Cloud-Providern im Ausland, weil für viele unklar ist, wie gross dieses Risiko ist und wie sie damit umgehen sollen. Es ist dies das vielzitierte «CLOUD Act»-Risiko.

[79] Wenn somit davon ausgegangen werden darf, dass die «traditionelle» Datensicherheit (Schutz gegen Hacker, versehentliche Offenbarungen, Ransomware, etc.) gewährleistet ist, stellt sich bei einem Cloud-Provider im Ausland vor allem die Frage, (a) welches Restrisiko eines *Lawful Access* ausländischer Behörden angesichts der konkreten Cloud-Lösung und der dabei getroffenen Schutzmassnahmen besteht und (b) ob dieses Restrisiko noch akzeptabel ist und daher einer angemessenen Datensicherheit und Verwendungskontrolle entspricht.

2. Welches Restrisiko eines ausländischen Lawful Access ist noch akzeptabel?

a. Grundsätzliches

[80] Welches Restrisiko eines *Lawful Access* durch eine ausländische Behörde noch akzeptabel ist, hängt vom gewählten Massstab ab: Es kann dies die Vermeidung der *Strafbarkeit* der für den Einsatz des Cloud-Providers verantwortlicher Organe sein. Die meisten Berufsgeheimnisse verlangen mindestens Eventualvorsatz; in wenigen Fällen (Bankgeheimnis) genügt allerdings bereits Fahrlässigkeit. Sollen *zivilrechtliche Ansprüche* vermieden werden, muss in jedem Fall Fahrlässigkeit als Massstab gewählt werden. Zur Anwendung kommen kann aber auch ein selbstgesetzter, noch strengerer Massstab, der auch die *reputative Wirkung* eines *Lawful Access* berücksichtigt.

[81] Auf letzteren, selbstgewählten Massstab soll an dieser Stelle nicht weiter eingegangen werden, da dies ein rein unternehmerischer Entscheid ist. Stattdessen wird nachfolgend für das Strafrecht dargelegt, wie weit mit technischen und organisatorischen Gegenmassnahmen das Restrisiko eines *Lawful Access* oder sonst unerwünschten Zugriffs reduziert werden muss, um weder

eventualvorsätzlich noch fahrlässig zu handeln. Die Besonderheiten des zivilrechtlichen Fahrlässigkeitsbegriffs werden hier nicht weiter erörtert.

b. Massstab zur Vermeidung des Vorwurfs des Eventualvorsatzes

[82] Wird ein strafrechtlicher Massstab angewandt, ist normalerweise zu prüfen, ob der Berufsgeheimnisträger die Berufsgeheimnisverletzung wissentlich und willentlich verübte, d.h. vorsätzlich oder mindestens eventualvorsätzlich gehandelt hat (Art. 12 Abs. 2 StGB).

[83] Bei Delikten, die den Eintritt eines Erfolges erfordern, gehört zur Wissensseite eine Vorstellung über den Zusammenhang zwischen dem eigenen Handeln und dem Erfolg. Die Tatbestände der Verletzung des Berufsgeheimnisses gelten nach herrschender Lehre und Praxis als Erfolgsdelikte.[89] Der Täter muss das Vorhandensein oder Eintreten der Tatumstände nicht zwingend für sicher halten; es genügt, dass er sie für real möglich hält.[90] Im Fall eines Cloud-Providers muss der Täter es somit für real möglich gehalten haben, dass es aufgrund seines Beizugs des Providers trotz aller Gegenmassnahmen zur (strafbaren) Offenbarung des Berufsgeheimnisses kommt.

[84] Auf der Willensseite muss geprüft werden, ob sich der Täter gegen das rechtlich geschützte Gut entschieden hat, indem er den Taterfolg wünschte oder als notwendige Nebenfolge sah (direkter Vorsatz) oder aber diesen Taterfolg zwar nicht anstrebte, aber trotz seinem Wissen um die reale Möglichkeit seiner Verwirklichung handelte, weil er den Taterfolg in Kauf nahm, sich mit ihm abfand, mag er ihm auch unerwünscht gewesen sein (Eventualvorsatz).[91] Der Eventualvorsatz grenzt sich zur Figur der bewussten Fahrlässigkeit ab: Bei letzterer hält der Täter den Taterfolg zwar ebenfalls für möglich, vertraut aber darauf, dass er ausbleibt. Bewusst fahrlässig handelt selbst der Täter, der sich leichtfertig bzw. frivol über die Möglichkeit der Tatbestandserfüllung hinwegsetzt und mit der Einstellung handelt, es werde schon nichts passieren.[92]

[85] In der Praxis ist insbesondere der Nachweis der Willensseite ein Problem. Nach der Rechtsprechung darf darum ein Richter vom Wissen des Täters auf seinen Willen schliessen, wenn sich dem Täter die Verwirklichung der Gefahr als so wahrscheinlich aufdrängte, dass die Bereitschaft, sie als Folge hinzunehmen, vernünftigerweise nur als Inkaufnahme des Erfolges ausgelegt werden kann.[93] Zu den äusseren Umständen, aus denen der Schluss gezogen werden kann, der Täter habe die Tatbestandsverwirklichung in Kauf genommen, zählt gemäss Bundesgericht unter anderem auch die Grösse des dem Täter bekannten Risikos der Tatbestandsverwirklichung, die Schwere der Sorgfaltspflichtverletzung, die Beweggründe des Täters und die Art der Tathandlung; je grösser die Wahrscheinlichkeit der Tatbestandsverwirklichung ist und je schwerer die Sorgfaltspflichtverletzung wiegt, desto näher liegt gemäss Bundesgericht die tatsächliche Schlussfolgerung, der Täter habe die Tatbestandsverwirklichung in Kauf genommen.[94] Der Schluss, der Täter habe die Tatbestandsverwirklichung in Kauf genommen, darf aber gemäss Bundesgericht nicht

89 Schwarzenegger et al. (Fn. 7), S. 15.

90 BGE 130 IV 58, Erw. 8.1 und 8.2.

91 BGE 130 IV 58, Erw. 8.2, m.w.H.

92 BGE 130 IV 58, Erw. 8.3.

93 BGE 130 IV 58, Erw. 8.4.

94 BGE 133 IV 9, Erw. 4.1; BGE 130 IV 58, Erw. 8.4, m.w.H.; vgl. jedoch BGE 131 IV 1, Erw. 2.2, wonach selbst bei sehr geringer Wahrscheinlichkeit bei entsprechenden Umständen Eventualvorsatz vorliegen kann (i.c. ging es um eine HIV-Ansteckung).

allein aus der Tatsache gezogen werden, dass sich dieser des Risikos der Tatbestandsverwirklichung bewusst war und dennoch handelte, da dieses Wissen um das Risiko der Tatbestandsverwirklichung auch bei der bewussten Fahrlässigkeit vorausgesetzt wird.[95]

[86] Beim Beizug eines Cloud-Providers durch einen Berufsgeheimnisträger stellt sich somit die Frage, für wie wahrscheinlich er eine Offenbarung trotz Gegenmassnahmen hielt und wie er damit umging. Prüfte er das Risiko einer Offenbarung sorgfältig, versucht er alle möglichen Massnahmen zu treffen, um eine solche zu verhindern, und kam er zum Schluss, dass zwar rechnerisch eine nicht nur theoretische Wahrscheinlichkeit einer Offenbarung besteht, diese aber nicht allzu hoch war und er somit darauf vertrauen konnte, dass nichts passiert, so handelte er nicht mehr eventualvorsätzlich.

[87] Wie tief die Wahrscheinlichkeit hierzu sein muss, lässt sich nicht pauschal festlegen, weil schon die Berechnung der Wahrscheinlichkeit keine exakte Wissenschaft darstellt und sich die Frage stellt, wie umfassend sie abgeschätzt worden ist. Zudem besteht beim Risiko eines *Lawful Access* aufgrund mangelnder Erfahrungswerte und der Unwissenheit zum Thema eine Tendenz, Wahrscheinlichkeiten subjektiv höher einzustufen, als sie es sind. Wenn ein Berufsgeheimnisträger sich für den Beizug eines Cloud-Providers entscheidet, muss er daher zur Vermeidung des Eventualvorsatzes einerseits zeigen, warum er die Wahrscheinlichkeit einer Offenbarung angesichts der von ihm getroffenen Massnahmen für tief hält, und andererseits mit vernünftigen oder unvernünftigen Argumenten zeigen, warum er davon ausgeht, dass sich auch dieses Restrisiko nicht verwirklichen wird (vgl. zum Thema auch N 128 ff.).

c. Massstab zur Vermeidung des Vorwurfs der Fahrlässigkeit

(1) Grundsätzliches

[88] Ist die tatbestandliche Offenbarung eines Berufsgeheimnisses ausnahmsweise auch bei fahrlässiger Begehung strafbar (namentlich im Falle des Bankgeheimnisses nach Art. 47 BankG und dem Berufsgeheimnis anderer Finanzinstitute nach Art. 69 FINIG), so kommt es auf das Wissen und den Willen des Täters nicht mehr an. Vielmehr stellt sich die Frage, ob der Taterfolg die Folge einer pflichtwidrigen Unvorsichtigkeit ist, d.h. das Resultat der Verletzung einer Sorgfaltspflicht (Art. 12 Abs. 3 StGB). Eine solche Verletzung liegt gemeinhin vor, wenn der Täter eine Sorgfaltsnorm verletzt, der Taterfolg *vorhersehbar* und *vermeidbar* ist und zwischen Tathandlung und Taterfolg ein *Risikozusammenhang* besteht. Im vorliegenden Fall besteht die Tathandlung im Beizug eines Cloud-Providers und der Taterfolg in der Offenbarung von Bankgeheimnisdaten.

(2) Sorgfaltsnorm

[89] Um zu beurteilen, ob die Tat pflichtwidrig begangen wurde, muss vorerst nach den konkreten Umständen beurteilt werden, welches Mass an Sorgfalt zu beachten ist. Wo besondere Normen ein bestimmtes Verhalten gebieten, richtet sich das Mass der im Einzelfall zu beachtenden Sorgfalt, in erster Linie nach diesen Vorschriften.[96] Wo solche Normen fehlen, kann der Vorwurf der Sorgfaltsverletzung auch auf allgemeine Rechtsgrundsätze, wie den allgemeinen Gefahrensatz,

95 BGE 130 IV 58, Erw. 8.4.

96 BGE 135 IV 56, Erw. 2.1.

gestützt werden.[97] Der allgemeine Gefahrensatz besagt, dass derjenige der eine Gefahr schafft, alles Zumutbare zur Vermeidung der Verletzung fremder Rechtsgüter vorzukehren hat.[98] Es ist aber denkbar, dass ein Verhalten als sorgfaltswidrig erwachtet wird, obwohl es gegen keine bestimmte Verhaltensnorm verstösst, die konkreten Umstände und persönlichen Verhältnisse des Täters von ihm aber dennoch eine bestimmte Vorsicht verlangen.[99]

[90] Im Falle des Bankgeheimnisses kommt als Sorgfaltsnorm Art. 47 BankG in Frage. Die Bestimmung verlangt, dass Bankkundendaten durch eine angemessene Datensicherheit geschützt werden; wie gezeigt untersagt sie den Einsatz von Cloud-Providern als solches weder im In- noch im Ausland. Auch aus dem Gefahrensatz lässt sich ein generelles Verbot des Einsatzes von Cloud-Providern weder im In- noch im Ausland ableiten. Dasselbe gilt für Art. 7 und 10a DSG, welche die Datensicherheit und Auftragsbearbeitung regeln. Sie alle verlangen eine angemessene Datensicherheit. Ist sie auch mit Bezug auf Zugriffe durch ausländische Behörden gewährleistet, ist der Beizug des Cloud-Providers wie oben gezeigt grundsätzlich zulässig.

[91] Nebst Art. 47 BankG kommt betreffend die Sorgfaltspflicht von Banken im Umgang mit Cloud-Providern ferner der Cloud-Leitfaden der Schweizerischen Bankiervereinigung vom März 2019 in Betracht.[100] Gemäss der bundesgerichtlichen Rechtsprechung kommt Standesregeln zur Sorgfaltspflicht der Banken für die strafrechtliche Beurteilung aber lediglich die Bedeutung einer Auslegungshilfe zu.[101] Allerdings äussert sich der Cloud-Leitfaden zum Hauptproblem des Beizugs eines Cloud-Providers, dem *Lawful Access* durch ausländische Behörden, nicht wirklich. Standesregeln zum Beizug von Dienstleistungsanbietern im Hinblick auf die Frage eines *Lawful Access* gibt es keine; eine Usanz ebenfalls nicht. Im Gegenteil: Bisher galt – wie der Cloud-Leitfaden selbst festhält – der Grundsatz «over-the-border out-of-control», was jede Auslagerung, bei welcher ein ausländischer Zugriff auf Bankkundendaten im Klartext vorkommen kann, als sorgfaltswidrig erscheinen lassen würde. Der Cloud-Leitfaden äussert sich im Weiteren lediglich zur Frage, ob die Offenbarung von Bankkundendaten im Klartext an einen Dienstleister im Ausland bereits eine Verletzung des Bankkundengeheimnisses darstellt, was abgelehnt wird.[102] Die Frage des *Lawful Access* durch eine ausländische Behörde wird nur aufgeworfen, aber nicht beantwortet.[103] Der Cloud-Leitfaden hilft somit im entscheidenden Punkt (ebenfalls) nicht weiter.

[92] Mangels konkreter Vorgaben muss somit auf den allgemeinen Grundsatz zurückgegriffen werden, dass die Datensicherheit dann angemessen ist, wenn sie *risikoadäquat* ist, d.h. die getroffenen Massnahmen zur Verhinderung einer Verletzung der Datensicherheit in einem vernünftigen Verhältnis zur Eintrittswahrscheinlichkeit und Schadenshöhe stehen. Wird die Schadenshöhe ausgeblendet, weil sie im Rahmen von Art. 47 BankG und Art. 69 FINIG keine Rolle spielt (jede Offenbarung erfüllt den objektiven Tatbestand), verbleibt als entscheidender Faktor die Wahrscheinlichkeit, dass es zum Taterfolg kommt. Dies führt zugleich zu den weiteren Voraus-

97 BGE 106 IV 80, Erw. 4b.

98 Marcel Alexander Niggli/Stefan Maeder, in: Basler Kommentar, Strafrecht I, Basel 2018, Art. 12 N 112; Praxis des Bundesgerichts siehe nur: BGE 78 IV 73; 127 IV 62.

99 BGE 135 IV 56, Erw. 2.1.

100 Schweizerische Bankiervereinigung, Cloud-Leitfaden, Wegweiser für sicheres Cloud Banking, März 2019.

101 BGE 125 IV 139, Erw. 3d.

102 Cloud-Leitfaden (Fn. 53), S. 37, Rz. 50.

103 Cloud-Leitfaden (Fn. 53), S. 37, Rz. 50.

setzungen einer Sorgfaltspflichtverletzung: Der Vorhersehbarkeit, der Vermeidbarkeit und dem Risikozusammenhang.

(3) Vorhersehbarkeit

[93] Die Sorgfaltspflichtverletzung ist gemäss Art. 12 Abs. 3 Satz 2 StGB, neben den konkreten Umständen, auch anhand der «persönlichen Verhältnisse» zu beurteilen. Die Vorhersehbarkeit des Erfolgs ist nach Lehre und Praxis eine Grundvoraussetzung für das Bestehen einer Sorgfaltspflichtverletzung und mithin für die Fahrlässigkeitshaftung.[104] Die zum Erfolg führenden Geschehensabläufe müssen für den konkreten Täter mindestens in ihren wesentlichen Zügen voraussehbar sein.[105] Sind sie dies nicht, kann von ihm auch nicht erwartet werden, sichernd einzugreifen.

[94] Für die Beantwortung dieser Frage gilt nach der bundesgerichtlichen Rechtsprechung der Massstab der Adäquanz: «Danach muss das Verhalten geeignet sein, nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens einen Erfolg wie den eingetretenen herbeizuführen oder mindestens zu begünstigen. Die Adäquanz ist nur zu verneinen, wenn ganz aussergewöhnliche Umstände, wie das Mitverschulden des Opfers beziehungsweise eines Dritten oder Material- oder Konstruktionsfehlers, als Mitursache hinzutreten, mit denen schlechthin nicht gerechnet werden musste und die derart schwer wiegen, dass sie als wahrscheinlichste und unmittelbarste Ursache des Erfolgs erscheinen und so alle anderen mitverursachenden Faktoren – namentlich das Verhalten des Angeschuldigten – in den Hintergrund drängen.»[106]

[95] Aus dieser Regel ergäbe sich umgekehrt, dass grundsätzlich mit jedem Fehlverhalten eines Dritten gerechnet werden müsste, das einigermassen voraussehbar bzw. nicht geradezu unsinnig oder aussergewöhnlich ist. Insbesondere im Strassenverkehr erscheint dieses Resultat kaum haltbar.[107] Die Praxis entwickelte deshalb das sog. Vertrauensprinzip.[108] Nach dem Vertrauensprinzip «darf jeder Strassenbenützer, sofern nicht besondere Umstände dagegen sprechen, darauf vertrauen, dass sich die anderen Verkehrsteilnehmer ebenfalls ordnungsgemäss verhalten.»[109] Obwohl das Fehlverhalten anderer im Strassenverkehr in gewissem Umfang vorhersehbar ist, kann folglich darauf vertraut werden, dass sich die anderen Verkehrsteilnehmer regelkonform verhalten.

[96] Das Vertrauensprinzip gründet darin, dass zahlreiche erwünschte Verhaltensweisen nur unter unverhältnismässigen Schwierigkeiten durchführbar wären, wenn ständig jedes erdenkliche Fehlverhalten einkalkuliert werden müsste.[110]

[97] Es ist allgemein anerkannt, dass das Vertrauensprinzip auch ausserhalb des Strassenverkehrs Anwendung findet, und zwar überall dort, wo sich das Verhalten mehrerer Personen überschnei-

104 BGE 135 IV 56. Erw. 2.1; BGer 6B_1050/2018 vom 8. März 2019, Erw. 2.2.

105 BGE 135 IV 56. Erw. 2.1.

106 BGE 135 IV 56. Erw. 2.1.

107 Günter Stratenwerth, Schweizerisches Strafrecht, AT I, Bern 2011, S. 511.

108 Abgeleitet aus Art. 26 SVG.

109 BGE 120 IV 252. Erw. 2.d.

110 Günter Stratenwerth, Schweizerisches Strafrecht, AT I, Bern 2011, S. 511.

det und man darauf angewiesen ist, sich auf das Handeln anderer einstellen zu können.[111] Von grosser Bedeutung ist das Vertrauensprinzip unter anderem bei arbeitsteiliger Zusammenwirkung.[112] Folglich kann im Rahmen von arbeitsteiligen Unternehmungen grundsätzlich darauf vertraut werden, dass die mitwirkenden Personen sich pflichtgemäss Verhalten.[113]

[98] Die Berufung auf das Vertrauensprinzip findet aber seine Grenzen, wenn konkrete Anzeichen für ein regelwidriges Verhalten bestehen oder wenn jemand gerade verpflichtet ist, eine andere Person zu beaufsichtigen.[114] Konkrete Anzeichen auf ein Fehlverhalten können sich entweder aus Verhalten eines andern oder aus der Unklarheit oder Ungewissheit einer bestimmten Lage ergeben, die nach allgemeiner Erfahrung die Möglichkeit fremden Fehlverhaltens unmittelbar in die Nähe rückt.[115] Keine Verpflichtung zur Beaufsichtigung besteht, wenn «die Beteiligten auch tatsächlich an einem arbeitsteiligen Produktions- oder Arbeitsablauf zusammenwirken, wo es – entsprechend der Funktion des Vertrauensprinzips – darum geht, die einzelnen Verantwortungsbereiche gegeneinander abzugrenzen.»[116] Die Rechtsprechung ist mit der Anwendung des Vertrauensgrundsatzes – ausserhalb des Strassenverkehrs – zurückhaltend.[117]

[99] Der Täter handelt folglich nicht fahrlässig, wenn der Eintritt des Taterfolgs dermassen unwahrscheinlich erscheint und deshalb nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens nicht vorhersehbar ist. Ist der Erfolgseintritt vorhersehbar, bleibt der Täter dennoch straffrei, wenn der Taterfolg durch das pflichtwidrige Verhalten einer Drittperson herbeigeführt wurde, sich der Täter aber gemäss dem Vertrauensprinzip darauf verlassen durfte, dass die mitwirkende Person sich pflichtgemäss Verhalten würde.

(4) Vermeidbarkeit und Risikozusammenhang

[100] Weitere Voraussetzung der Sorgfaltspflichtverletzung ist, dass der Taterfolg vermeidbar war. «Dabei wird ein hypothetischer Kausalverlauf untersucht und geprüft, ob der Erfolg bei pflichtgemässem Verhalten des Täters ausgeblieben wäre.»[118] Nach dem allgemeinen Gefahrensatz hat sich der Täter pflichtgemäss Verhalten, wenn alle zumutbaren Massnahmen getroffen wurden, um die Verletzung fremder Rechtsgüter zu vermeiden. Es stellt sich diesbezüglich die Frage, mit welchem Grad an Wahrscheinlichkeit der Erfolg hätte vermieden werden müssen, damit zwischen Taterfolg und Tathandlung ein sog. Risikozusammenhang besteht.

---

111 BGE 120 IV 300. Erw. 3.d.; Andreas Donatsch, Sorgfaltsbemessung und Erfolg beim Fahrlässigkeitsdelikt, Zürich 1987, S. 192; Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, Zürich 2013, S. 355; Günter Stratenwerth, Schweizerisches Strafrecht, AT I, Bern 2011, S. 511.

112 Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, Zürich 2013, S. 355.

113 Günter Stratenwerth/Wolfgang Wohlers, Schweizerisches Strafgesetzbuch, Handkommentar, Zürich 2013, Art. 12 N 12; Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, Zürich 2013, S. 355.

114 Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, Zürich 2013, S. 356; BGE 120 IV 300, Erw. 3.d.

115 BGE 98 IV 273, Erw. 2., mit Bezugnahme auf den Strassenverkehr.

116 BGE 120 IV 300, Erw. 3.d., in diesem Entscheid verneinte das Bundesgericht die Berufung auf das Vertrauensprinzip. Im Rahmen eines Mehrfachsicherungssystems könne der Verantwortliche des primären Sicherungssystems gerade nicht auf das ordnungsgemässe Funktionieren des sekundären Systems vertrauen.

117 Andreas Donatsch, Sorgfaltsbemessung und Erfolg beim Fahrlässigkeitsdelikt, Zürich 1987, S. 194; keine Entlastung aufgrund des Vertrauensgrundsatzes bspw. in BGE 120 IV 300, Erw. 3.d, BStGer SK.2018.1 vom 30. Mai 2018, Erw. 2.6.5 und BGer 6B_195/2018 vom 24. August 2018, Erw. 2.4.

118 BGE 135 IV 56, Erw. 2.1; BGer 6B_351/2017 vom 1. März 2018, Erw. 1.3.1.

[101] In der Lehre wird diesbezüglich teilweise die sog. Risikoerhöhungstheorie vertreten, wonach ein Risikozusammenhang besteht bzw. der Taterfolg vermeidbar gewesen wäre, wenn das pflichtgemässe Verhalten das Erfolgsrisiko deutlich gesenkt hätte.[119] Das Bundesgericht hingegen lehnt die Risikoerhöhungstheorie explizit ab und wendet, in konstanter Praxis, die sog. Wahrscheinlichkeitstheorie an. Nach der Wahrscheinlichkeitstheorie wäre der Taterfolg vermeidbar gewesen, wenn das pflichtgemässe Verhalten den Erfolg höchstwahrscheinlich vermieden hätte. Nach der Rechtsprechung genügt für die Zurechnung des Erfolgs folglich, wenn das Verhalten des Täters mindestens mit einem hohen Grad an Wahrscheinlichkeit die Ursache des Erfolgs bildete.[120]

[102] Der Täter bleibt folglich straffrei, wenn er zwar – durch Beizug des Cloud-Providers – eine Gefahr geschaffen hat, aber alle zumutbaren Massnahmen getroffen hat, um das Risiko des Erfolgseintritts auszuschliessen, bzw. keine weiteren zumutbaren Massnahmen ersichtlich sind, die den Taterfolg mit höchster Wahrscheinlichkeit vermieden hätten.

(5) Ergebnis

[103] Wenn ein Berufsgeheimnisträger sich für den Beizug eines Cloud-Providers entscheidet und sich vor dem Vorwurf der Fahrlässigkeit mit Bezug auf eine unbefugte Offenbarung schützen will, sollte er zeigen können, dass er alle zumutbaren Massnahmen getroffen hat, die in ihrer Gesamtheit jene Offenbarung höchstwahrscheinlich vermeidet, mit welcher er nach dem gewöhnlichen Lauf der Dinge und Erfahrungen des Lebens rechnen musste.

[104] Dabei darf er grundsätzlich davon ausgehen, dass jene Dritte, die mit ihm arbeitsteilig zusammenwirken – wie etwa seine Hilfspersonen – sich mindestens in der Schweiz auch an das Schweizer Recht halten werden, soweit dem keine Aufsichtspflichten und Hinweise auf ein pflichtwidriges Verhalten entgegenstehen.

[105] Somit muss auch im Hinblick auf die Fahrlässigkeit im Ergebnis beurteilt werden, wie wahrscheinlich der Beizug eines Cloud-Providers zu einer Offenbarung z.B. gegenüber einer ausländischen Behörde führt. Im Gegensatz zum Eventualvorsatz muss die Wahrscheinlichkeit hier jedoch geringer sein, nämlich so gering, dass der Richter zum Schluss kommt, dass der Taterfolg sich *höchstwahrscheinlich nicht verwirklicht*, mit ihm also nicht (mehr) gerechnet werden musste.

F. Berechnung der Wahrscheinlichkeit eines Lawful Access im Ausland

1. Grundsätzliches

[106] Um bestimmen zu können, wie wahrscheinlich ein *Lawful Access* durch eine ausländische Behörde im Falle des Beizugs eines Cloud-Providers ist, hat der Autor dieses Beitrags ein spezielles Modell zur Beurteilung des Risikos und dessen Dokumentation entwickelt.

[107] Das Modell geht von der Annahme aus, dass das Risiko eines *Lawful Access* einerseits von technischen und organisatorischen Massnahmen abhängt, die der Berufsgeheimnisträger mit Bezug auf den Einsatz des Cloud-Providers unternimmt, und andererseits von den rechtlichen

119 Pozo Hurtado, Droit pénal, Partie générale, N 544.

120 BGE 135 IV 56. Erw. 2.1; BGE 130 IV 7. Erw. 3.2; BGE 127 IV 34. Erw. 2.a.

Möglichkeiten, mit welchen ausländischen Behörden vom Provider die Herausgabe der Daten verlangen können. Ersteres ist fallspezifisch, d.h. hängt von der konkreten Ausgestaltung der Auslagerung an den Cloud-Provider ab, einschliesslich der mit ihm getroffenen Vereinbarung (dazu sogleich).

[108] Mit Bezug auf die rechtlichen Möglichkeiten der ausländischen Behörden ist das Beurteilungsmodell nicht eingeschränkt. In der Praxis dürften jedoch Zugriffsmöglichkeiten nach dem Vorbild des US CLOUD Act im Vordergrund stehen, welcher wiederum Art. 18 Abs. 1 des Übereinkommens über die Cyberkriminalität[121] umsetzt, sowie nachrichtendienstliche Zugriffsbefugnisse wie etwa gemäss Section 702 des US Foreign Intelligence Surveillance Act (FISA). Die nachfolgenden Detailausführungen gehen nur auf diese Sorte von Zugriffen im bzw. aus dem Ausland ein, da sie im Fokus der Diskussionen zum Thema stehen. Nicht diskutiert werden Zugriffe ausländischer Behörden, die gestützt auf weitergehende Befugnisse nach dem jeweils lokalen Recht erfolgen, wie sie z.B. bei im eigenen Land der Behörde gespeicherten Daten bestehen können (Beispiel: Beschlagnahmung von Daten, die ein Cloud-Provider wie z.B. Amazon in seinem Rechenzentrum in Frankfurt speichert, durch die deutschen Behörden). Auch diese lokalen Befugnisse im Land sind in die Risikoüberlegungen einzubeziehen, insbesondere wo Daten nicht in einem Rechenzentrum in der Schweiz, sondern im Ausland gespeichert werden. Allerdings zeigt die Erfahrung, dass seit der Verfügbarkeit von Cloud-Rechenzentren in der Schweiz viele Betriebe diese favorisieren. Das hat auch eine sehr konkrete Auswirkung auf das Gesamtrisiko, wie noch gezeigt wird.

2. Das Beurteilungsmodell

[109] Das Beurteilungsmodell geht dabei zusammengefasst davon aus, dass *sieben* Voraussetzungen kumulativ erfüllt sein müssen, damit es zu einem «erfolgreichen» *Lawful Access* durch eine ausländische Behörde kommen kann. Es sind dies folgende:

a. Die Behörde weiss um den vom Unternehmen beigezogenen Provider und dessen Subunternehmer;
b. Der Provider oder einer seiner Subunternehmer kann sich technisch Zugriff auf Kundendaten im Klartext verschaffen;
c. Der Provider oder einer seiner Subunternehmer kann nach Kundendaten suchen;
d. Der Provider, einer seiner Subunternehmer oder seine Muttergesellschaft befindet sich im Zuständigkeitsbereich einer Behörde, die konkretes Interesse an der Erzwingung eines *Lawful Access* hat;
e. Die Behörde ist nach ihrem Recht befugt, diesem Provider, Subunternehmer oder der Muttergesellschaft zu befehlen, sich technischen Zugang zu den Kundendaten zu verschaffen und diese herauszugeben (hier wird der CLOUD Act für sich beurteilt);
f. Die Mitarbeiter des Providers oder eines seiner Subunternehmer können in der Schweiz de facto nicht strafrechtlich belangt werden, wenn sie die Kundendaten der ausländischen Behörde herausgeben (hier werden Abwehrmassnahmen gegen den CLOUD Act auf Basis des

[121] Übereinkommen über die Cyberkriminalität (SR 0.311.43).

Schweizer Rechts beurteilt und das strafrechtliche Vertrauensprinzip im Schweizer Recht berücksichtigt);

g. Dem Unternehmen gelingt es nicht, die relevanten Kundendaten rechtzeitig in Sicherheit zu bringen bzw. dem Zugriff des Providers zu entziehen.

[110] Jeder dieser Voraussetzungen bzw. deren Verwirklichung kann mit verschiedenen technischen und organisatorischen Gegenmassnahmen entgegengewirkt werden, was im Zuge einer Beurteilung ihrer Wirksamkeit zu einer Wahrscheinlichkeit führt, dass die jeweilige Voraussetzung trotz allem erfüllt ist. Es wurde darauf geachtet, dass diese Voraussetzungen nicht überlappen, d.h. eine Wahrscheinlichkeit nicht doppelt gezählt wurde, auch wenn ein und dieselbe Gegenmassnahme sich auf verschiedene Voraussetzungen auswirken kann: Die Begrenzung der tatsächlichen Zugriffsmöglichkeit des Cloud-Providers auf Daten in Klartext hat beispielsweise auch einen Einfluss, ob die fraglichen Daten für die Zwecke des US CLOUD Act rechtlich als unter seiner Kontrolle gelten. Eine ausführliche Beschreibung der Voraussetzungen und Diskussion der rechtlichen Grundlagen zu ihrer Beurteilung findet sich im Anhang.

[111] Werden diese Einzelwahrscheinlichkeiten kombiniert, ergibt sich daraus die Gesamtwahrscheinlichkeit eines erfolgreichen *Lawful Access* durch eine ausländische Behörde, und es lässt sich beurteilen, wie wahrscheinlich die im konkreten Fall gewählten Gegenmassnahmen den *Lawful Access* verhindern. Hierfür wurde eine Excel-Tabelle als Hilfsmittel entworfen, die sich mit beispielhaften Daten hier abrufen lässt (das Excel darf – unter Quellenangabe – auch im Rahmen einer entgeltlichen Beratung verwendet werden;[122] Updates werden online angeboten[123]). Um die Excel-Tabelle für den konkreten Fall zu verwenden, müssen die ins Auge gefassten Gegenmassnahmen definiert und danach für jede der Voraussetzungen deren Eintrittswahrscheinlichkeit trotz Gegenmassnahme geschätzt werden (weitere Hinweise dazu, insbesondere zur Frage, wie die Prozentwerte zu verstehen sind, finden sich im Excel). Diese Einschätzung sollte unter Beteiligung der diversen Fachbereiche des jeweiligen Betriebs (Fach, Recht, Datensicherheit, Datenschutz, etc.) und der Entscheider erfolgen, also nicht nur durch einen Datenschutzspezialisten, denn es muss letztlich die Risikoeinschätzung des jeweiligen Betriebs reflektieren. Das Excel zeigt die Gesamtwahrscheinlichkeit an, die den Entscheidern einerseits Grundlage für deren Risikoentscheid ist und andererseits dokumentiert, wie diese Beurteilung zustande gekommen ist (zur Frage, was die Wahrscheinlichkeit genau bedeutet, siehe N 131 ff.).

[112] Das Excel bietet ferner die Möglichkeit, die Wahrscheinlich eines ausländischen *Lawful Access* durch Nachrichtendienste abzubilden, die mit ihren Zugriffen nicht einer Rechtsweggarantie wie im Falle des US CLOUD Act unterliegen und daher anders beurteilt werden müssen. Es handelt sich hier um Bestimmungen wie etwa die Section 702 des US-amerikanischen Foreign Intelligence Surveillance Act (FISA), der auch im kürzlichen «Schrems II»-Entscheid des EuGH vom 16. Juli 2020 (C-311/18) thematisiert wurde und im EWR zur Aufhebung des «Privacy Shield» führte. Das Excel erlaubt sowohl die Einschätzung und Darstellung der Wahrscheinlichkeit eines *Lawful Access* im Zuge der von den USA betriebenen Kabelaufklärung (Überwachungsprogramm «Upstream») als auch ihrer «Online-Rasterfahndung» bei grossen Online-Anbietern in den USA

[122] Es wird unter einer Creative Commons «Namensnennung – Keine Bearbeitungen 4.0 International» Lizenz zur Verfügung gestellt. Diese Lizenz erlaubt die kommerzielle Nutzung unter Nennung der Urheberschaft, nicht jedoch Bearbeitungen (weitere Informationen sind hier http://creativecommons.org/licenses/by-nd/4.0/ abrufbar).

[123] Unter https://www.rosenthal.ch.

(Überwachungsprogramm «Downstream»). Ersteres spielt erfahrungsgemäss dank des Einsatzes von starker Verschlüsselung im B2B-Bereich in der Regel keine Rolle, während letzteres bei Beteiligung eines US-Providers zwar grundsätzlich denkbar ist, die Datenvorkommen der meisten hier relevanten B2B-Anwendungen nach bisheriger Information nicht das Ziel des «Downstream»-Überwachungsprogramms sind. Die hier ermittelte Wahrscheinlichkeit wird im Excel zur bereits berechneten Wahrscheinlichkeit eines herkömmlichen *Lawful Access* hinzugezählt.

[113] Hier ein Auszug aus dem Excel (weggelassen wurde die Beurteilung der Wahrscheinlichkeit eines nachrichtendienstlichen Zugriffs ohne Rechtsweggarantie sowie die Festlegung, für welche Daten und Anwendung die Beurteilung durchgeführt wird und die Beurteilung, wie wahrscheinlich es ist, dass eine ausländische Behörde sich überhaupt dafür interessiert, auf die Daten des Cloud-Providers zuzugreifen statt diese direkt beim betreffenden Unternehmen herauszuverlangen; dazu N 116 ff.):

Schritt 3: Wahrscheinlichkeit, dass eine ausländische Behörde den Anspruch über den Provider erfolgreich durchsetzt				
Voraussetzung für einen Taterfolg[5]		**Eintrittswahrscheinlichkeit**[6)9)] * **		
a)	Die Behörde weiss um den vom Unternehmen beigezogenen Provider und dessen Subunternehmer (Voraussetzung Nr. 1)	100%		100%
b)	Wenn er dem Kunden Supportleistungen erbringt, kann der Provider oder einer seiner Subunternehmer sich technisch Zugriff auf die Daten im Klartext verschaffen ... (Voraussetzung Nr. 2)	100%	100.00%	100%
	... und kann nach den von der Behörde gewünschten Daten suchen bzw. sie finden (Voraussetzung Nr. 3)	100%		
c)	Der Provider oder einer seiner Subunternehmer kann sich ausserhalb eines Support-Falls technisch Zugriff auf Daten im Klartext verschaffen … (Voraussetzung Nr. 2)	100%	100.00%	
	... und kann nach den von der Behörde gewünschten Daten suchen bzw. sie finden (Voraussetzung Nr. 4)	100%		
d)	Der Provider, einer seiner Subunternehmer oder seine Mutter befindet sich im Zuständigkeitsbereich der Behörde (Voraussetzung Nr. 4)	100%		100%
e)	Die Behörde ist nach ihrem Recht befugt, diesem Provider, Subunternehmer oder der Muttergesellschaft zu befehlen, sich technischen Zugang zu den Daten zu verschaffen und diese ihr herauszugeben (Basis ist vorliegend Art. 18 Abs. 1 CCC, wie z.B. im US CLOUD Act umgesetzt)[7] (Voraussetzung Nr.5)	40%		40%
f)	Wenn der ausländischen Behörde Daten herausgegeben würden, so würde dies zur Strafbarkeit von Mitarbeitern des Providers oder seiner Subunternehmer in der Schweiz führen, deren Verfolgung in der Schweiz auch möglich und realistisch wäre[8)9)] (Voraussetzung Nr. 6)	80%		20%
g)	Dem Unternehmen gelingt es nicht, die relevanten Daten rechtzeitig in Sicherheit zu bringen bzw. dem Zugriff des Providers zu entziehen (Voraussetzung Nr. 7)	90%		90%
Restrisiko eines erfolgreichen Lawful Access durch eine ausländische Behörde über den Provider (angesichts der Gegenmassnahmen[10]):				7.20%

[114] Die Berechnungen sind nicht kompliziert (mehrheitlich Verwendung des Additions- und Multiplikationssatzes der Wahrscheinlichkeitsmathematik), das Modell hat seine Schwächen und über die einzelnen Wahrscheinlichkeitsbewertungen wird sich immer streiten lassen. Die Methodik ist jedoch simpel, transparent und hat sich in der Praxis als leicht verständlich erwiesen. Sie hat den Vorteil, dass sie durch die Verwendung von Zahlen statt – wie von Juristen gewohnt – Worten wesentlich eingängiger und in ihren Ergebnissen klarer ist, und sie macht deutlich, dass das relevante Risiko sich aus einer Gesamtheit von Faktoren ergibt, die *zusammen* und nicht isoliert betrachtet werden müssen. Die Praxiserfahrung hat gezeigt, dass eben diese Verkettung der Umstände, die erfüllt sein müssen, häufig ausser Acht gelassen wird. Sie lässt sich intuitiv auch nicht wirklich fassen. Darum bietet sich die Darstellung in Form von Zahlen besonders an, da sie das Zusammenspiel der Faktoren aufzeigt und so zu einer Versachlichung der Diskussion beiträgt. Auf die genauen Werte kommt es dabei gar nicht mehr an; entscheidend sind die Grössenordnungen.

3. Berücksichtigung der getroffenen «Gegenmassnahmen»

[115] Um die sieben Voraussetzungen und deren Funktionsweise und Relevanz im Zusammenhang mit einem *Lawful Access* zu illustrieren und konkrete Handlungsmöglichkeiten zu ermitteln, finden sich nachfolgend knapp zwei Dutzend Beispiele möglicher technischer und organisatorischer Gegenmassnahmen. Eine ausführliche Beschreibung der Gegenmassnahmen und ihres Einflusses auf die Eintrittswahrscheinlichkeit der vorgenannten Voraussetzungen findet sich im Anhang. Die fett gedruckten Gegenmassnahmen sind mit Bezug auf den Schutz von Kundendaten aus unserer Sicht rechtlich oder technisch besonders wirksam:

a. Geheimhaltung des vom Unternehmen gewählten Providers;
b. Totalverschlüsselung der Kundendaten («Hold your own key», HYOK);
c. Vom Unternehmen selbst generierter und verwalteter Schlüssel («Bring your own key», BYOK);
d. **Schaffung einer «sicheren Zone» durch nur dem Kunden zugängliche virtuelle Server**;
e. **Schaffung einer «sicheren Zone» durch Entschlüsselung erst im Prozessor**;
f. **Schaffung einer «sicheren Zone» durch eine andere Methode**;
g. **Das Unternehmen hat die alleinige Hoheit über das Directory, d.h. Verwaltung von Benutzern und Zugangsberechtigungen (ungeachtet etwaiger «Hintertüren»)**;
h. **Nur das Unternehmen kann bestimmen, welche Personen/Rollen (auch seitens des Providers) Zugang zum Schlüssel erhalten (ungeachtet etwaiger «Hintertüren»)**;
i. Zusicherung, dass Support keinen Zugang zu Kundendaten im Klartext erfordert;
j. **Zugriff auf Kundendaten im Klartext nur bei Einzelfreigabe durch Kunden («Lockbox»)**;
k. **Shoulder Surfing bei Zugriff auf sichere Zone im Supportfall**;
l. Kündigungsrecht bei erhöhtem Risiko eines *Lawful Access* (inkl. Abzug aller Daten ohne Rückbehalt durch den Provider nach der Beendigung);
m. **Provider (Vertragspartner) mit Sitz in der Schweiz**;
n. Zusicherung des Providers, seine Dienstleistung nicht im Ausland zu erbringen;
o. **Zweckbindung aller im Rahmen der Leistungserbringung zur Kenntnis genommenen Kundendaten**;
p. Keine Hintertüren oder vergleichbare Programmierungen;
q. Pflicht des Providers, sich gegen Herausgabebefehle gerichtlich zur Wehr zu setzen;
r. **Herausgabe an Behörden nur, soweit der Provider nach Schweizer Recht dazu verpflichtet ist**;
s. **Vertrag mit dem Provider untersteht Schweizer Recht**;
t. Zusicherung, dass Subunternehmer Kundendaten nicht im Klartext sehen können;
u. **Überbindung der Pflichten des Providers auf dessen Subunternehmer**;
v. Organisatorische Massnahmen beim Provider zur Verhinderung eines Zugriffs auf Kundendaten im Klartext durch den Subunternehmer;
w. Organisatorische Massnahmen beim Provider zur Verhinderung eines Zugriffs auf Kundendaten im Klartext durch die Muttergesellschaft;

x. Vertragliche Pflicht, Kundendaten auch vor der Muttergesellschaft geheim zu halten, soweit sie kein Subunternehmer ist;

y. **Verpflichtung des Providers und der Subunternehmer zur Bearbeitung der Daten nur in der Schweiz, soweit das Unternehmen im Einzelfall nichts anderes vorsieht**;

z. **Verpflichtung des Providers und der Subunternehmer, die Daten in der Schweiz zu speichern («data at rest»)**.

[116] Alle Gegenmassnahmen kommen erfahrungsgemäss in Cloud-Projekten in der einen oder anderen Form zum Einsatz. Nicht alle Massnahmen passen jedoch für jedes Projekt und nicht alle werden von allen Providern akzeptiert. Es sind auch keineswegs alle der Gegenmassnahmen erforderlich; einige sind ohnehin alternativer Natur. Ebenso sind andere Massnahmen denkbar, die eine gleichwertige Wirkung haben können. So trifft es z.B. nicht wie von kantonalen Datenschützern mitunter vertreten zu, dass nebst Verschlüsselung zwingend Schweizer Recht als Vertragsstatut und ein Schweizer Gerichtsstand nötig ist, um sich angemessen zu schützen. Ersteres hat zwar einen Effekt, doch darf dieser nicht überbewertet werden. Die konkrete Ausgestaltung der Massnahmen kann ebenfalls variieren und daher eine unterschiedliche Wirksamkeit aufweisen. Diese wird auch von den technischen und rechtlichen Entwicklungen über Zeit abhängen. Die Einschätzung der Wirksamkeit der einzelnen Massnahmen und davon abgeleitet die Wahrscheinlichkeit, dass die eine oder andere der sieben Voraussetzungen erfüllt sind, ist allerdings keine exakte Wissenschaft. Weil die Wahrscheinlichkeiten aber in ihrer Gesamtheit beurteilt werden, kann bei den einzelnen Werten ohne Weiteres auch nur grob geschätzt werden.

4. Berücksichtigung des Interesses ausländischer Behörden an den Daten

a. Grundsatz

[117] Nebst der Frage, wie wahrscheinlich es ist, dass eine ausländische Behörde einen *Lawful Access* erfolgreich durchführen kann, muss ebenso die Frage gestellt werden, wie wahrscheinlich es ist, dass die Behörde sich überhaupt für die Daten interessiert bzw. ein Interesse daran hat, sich um deren Herausgabe zu bemühen – und dieses Interesse so gross ist, dass versucht wird, diese auf dem Wege eines *Lawful Access* zu bewerkstelligen.

[118] Diese Frage lässt sich nicht einheitlich beurteilen. Auch die Beurteilungsmethode wird je nach Branche und Betriebe variiert werden müssen. Bestimmte Unternehmen werden selbst immer wieder das Ziel von behördlichen Untersuchungen sein, während andere für Behörden primär in Bezug auf die Daten ihrer Kunden von Interesse sein werden. Und es gibt solche, die aufgrund ihrer Ausgestaltung und Aktivitäten kaum je Ziel von behördlichen Ersuchen sein werden. Während eine Schweizer Bank aufgrund ihrer eigenen Geschäften wie auch den Geschäften ihrer Kunden regelmässig mit ausländischen Offenlegungsersuchen oder -befehlen konfrontiert sein mag, sind es andere Amts- und Berufsgeheimnisträger nicht. Ein Schweizer Anwalt wird zum Beispiel mit Bezug auf seine Mandatsakten tendenziell nicht im Fokus von Herausgabebemühungen aus den USA sein, da seine Unterlagen prozessrechtlich in den USA in der Regel ohnehin nicht verwertet werden dürften (*legal privilege*); es macht also keinen Sinn, sie auf dem Umweg über den Cloud-Provider zu beschaffen, da sie trotzdem unverwertbar bleiben. Lagert ein Schweizer Strassenverkehrsamt seine Zulassungsdaten in der Cloud ab, so dürfte dies eine aus-

ländische Behörde so gut wie gar nicht interessieren. Es scheint zudem völkerrechtlich nur schwer vorstellbar, dass die Behörde eines ausländischen, zivilisierten Staats versuchen würde, *auf dem Rechtsweg* ihres eigenen Landes an die Daten einer Schweizer Behörde zu gelangen, welche diese für amtliche Zwecke in der Schweiz bearbeitet. Ein Krankenhaus in der Schweiz wiederum wird zwar regelmässig Anfragen von *Schweizer* Behörden haben, die irgendwelche Unterlagen wollen, doch wie die Praxiserfahrung zeigt, kaum je in den Fokus einer ausländischen Behörde geraten, die an irgendwelche Daten von Patienten (oder Mitarbeitern) gelangen möchte, weil sie gegen diese ermittelt. Darum ist die enorme Zurückhaltung der kantonalen Datenschutzbehörden gegenüber einer Auslagerung von Patientendaten in die Cloud wegen Zugriffsrisiken ausländischer Behörden bei sachlicher Betrachtung nicht wirklich nachvollziehbar. Auch die Art der Daten ist zu berücksichtigen: Der *vergangene* E-Mail-Verkehr einer Geschäftsleitung eines Finanzinstituts wird für eine ausländische Behörde, die mögliches Fehlverhalten dieses Unternehmens untersucht, von Interesse sein. Dieselbe Behörde wird möglicherweise schon nach ihrem eigenen Recht in den meisten Fällen hingegen keine Berechtigung haben, die laufenden Videokonferenzen, welche das Unternehmen abhält, abzuhören – oder es wird sie nicht interessieren.

[119] Nebst der Wahrscheinlichkeit, dass eine ausländische Behörde an Daten eines Schweizer Betriebs in der Cloud gelangen will, muss auch die Folgefrage berücksichtigt werden, wie wahrscheinlich es ist, dass ein solches Ansinnen sich in der einen oder anderen Weise erledigt, bevor es überhaupt zur Frage eines Zugriffs auf den Provider und zur obigen Wahrscheinlichkeitsrechnung kommt. Das hier präsentierte Risikobeurteilungsmodell kann auch diese Umstände widerspiegeln, und zwar unterteilt nach Land bzw. Region, weil hier naturgemäss nicht nur die USA eine Quelle solcher behördlichen Begehren sein kann, sondern zum Beispiel auch EU-Mitgliedsstaaten. In manchen Fällen wird es sogar wahrscheinlicher, dass nicht US-Behörden auf Daten von Schweizer Betrieben zugreifen möchten, sondern Behörden aus Deutschland, Frankreich oder anderen Ländern Europas. Hierbei kann berücksichtigt werden, wie wahrscheinlich es ist, solche Behörden unter Hinweis auf Schweizer Recht und die Möglichkeiten der Rechts- und Amtshilfe von ihren Vorhaben abzubringen oder sie auf andere Kanäle zu lenken.

[120] Die Erfahrung aus der Praxis machen jedenfalls deutlich, dass sich die Frage des ausländischen *Lawful Access* über einen Cloud-Provider in manchen Branchen realistischerweise kaum je stellen wird. Diese Eintrittswahrscheinlichkeit muss in der Gesamtbeurteilung ebenfalls berücksichtigt werden und reduziert die (für den Risikoentscheid zum Gang in die Cloud relevante) Gesamtwahrscheinlichkeit eines erfolgreichen *Lawful Access* massiv.

b. Wahrscheinlichkeit eines Lawful Access Falls

[121] Es gibt verschiedene Möglichkeiten, wie die Wahrscheinlichkeit des Falls, in welchem sich die Frage eines *Lawful Access* stellt, so eingeschätzt werden kann, dass eine sinnvolle Gesamtaussage möglich ist. Nachfolgend ist nur eine mögliche Vorgehensweise beschrieben.

[122] Startpunkt ist die Definition der *Anwendung*, um die es geht (z.B. E-Mail-Server, Videokonferenzlösung, Shares, virtueller Rechner, Backuplösung), die *Daten*, deren Offenlegung im Fokus steht (z.B. Bankkundendaten, Patientendaten) und um welche Daten es nicht geht (z.B. Mitarbeiterdaten, die sich ebenfalls in der Anwendung befinden können), sowie der *Betrachtungszeitraum* (z.B. drei oder fünf Jahre; mehr macht wohl keinen Sinn). Letzteres basiert auf dem Gedanken, dass die Vertretbarkeit der Cloud-Lösung regelmässig neu evaluiert werden sollte, weil sich die eingesetzte Technik, aber auch die Bedrohungen laufend weiterentwickeln. Ändert sich die Risi-

kolage über Zeit, können Daten in der Cloud auch wieder verschoben oder es können zusätzliche Massnahmen getroffen werden – vielleicht auch Massnahmen, die es ursprünglich noch nicht gab, wie z.B. neue Verschlüsselungsverfahren.

[123] In einem nächsten Schritt wird die Frage gestellt, welches Interesse eine ausländische Behörde an den in der betreffenden Anwendung bearbeiteten Daten haben wird. Geht es einem Unternehmen um Kundendaten, die in seinen E-Mails enthalten sind, hat das Unternehmen keinen geschäftlichen Bezug zu den USA und bearbeitet es auch keine Personendaten von Personen mit Bezug zu den USA, so dürfte das Interesse der US-Behörden an den fraglichen Daten schlimmstenfalls sehr gering sein. Darauf aufbauend wird im Beurteilungsmodell als erstes geschätzt, in wie vielen Fällen pro Jahr die Behörden im betreffenden Land versuchen dürften, auf dem Rechtsweg (direkt über das Unternehmen oder indirekt über die Schweizer Behörden oder den Provider) an die Daten heranzukommen, weil sie der Ansicht sind, dass sie einen Anspruch darauf haben. Die Chancen einer juristischen Abwehr sind hier noch nicht zu berücksichtigen. Als Grundlage können dabei die Erfahrungswerte der vergangenen Jahre berücksichtigt werden, aber auch allgemeine, die Wahrscheinlichkeit eines solchen Vorstosses steigernde oder senkende Umstände. Hierbei sind auch solche Fälle zu berücksichtigen, von denen das Unternehmen zunächst nichts weiss, weil die ausländische Behörde von Anfang an versucht, indirekt (z.B. über eine Schweizer Behörde oder einen Provider) an die Daten zu gelangen. Mehrfachanfragen in derselben Sache sollen jeweils nur als ein einziger Fall gezählt werden, jedenfalls wenn ihre rechtliche Zulässigkeit und Relevanz aus Sicht der ausländischen Behörde einheitlich und durch dieselbe Stelle beurteilt wird.

[124] In einem zweiten Schritt wird der Anteil der Fälle geschätzt, in welchem es um die Verfolgung von Fallkonstellationen geht, die nach dem jeweiligen Landesrecht zum *Lawful Access* berechtigen. Unter der US CLOUD Act sind dies beispielsweise nur schwere Straftaten, nicht aber beispielsweise zivilrechtliche Ansprüche oder aufsichtsrechtliche Abklärungen. Dieser Aspekt darf dementsprechend bei der Beurteilung der Erfolgschancen in späteren Prüfungsschritten zum US CLOUD Act nicht mehr berücksichtigt werden, um Doppelzählungen in der Wahrscheinlichkeitsberechnung zu vermeiden.

[125] In einem dritten Schritt ist zu schätzen, wie wahrscheinlich die ausländische Behörde von Ihrem Vorhaben durch Argumente nach deren Recht abgebracht werden kann, wobei zu berücksichtigen ist, dass das Unternehmen womöglich von gewissen Fällen gar keine Kenntnis erhält. Ein solches Argument könnte beispielsweise die Berufung auf ein *Legal Privilege* sein oder das Argument, dass das Unternehmen bzw. seine Mitarbeiter sich strafbar machen würde (z.B. wegen Art. 271 StGB oder Verletzung des Berufsgeheimnisses), wenn die Daten offengelegt würden (notabene direkt oder indirekt über den Provider). Die Praxiserfahrung zeigt dabei, dass ausländische Behörden auf solches Vorbringen durchaus eingehen, wenn sie den Eindruck haben, dass sie ernsthafter Natur sind. Das Risiko der Strafbarkeit in Folge einer Offenlegung ist auch in der Beurteilung der Chancen eines *Lawful Access* zu beurteilen, dort jedoch aus der Warte des Providers.

[126] In einem vierten Schritt zu schätzen, in wie vielen der verbleibenden Fälle es möglich sein wird, die Daten trotz allem zu liefern, so etwa auf dem Weg der Rechtshilfe (etwa indem der Behörde verdeutlicht wird, dass sie die Daten auf diesem Weg schneller erhält als wenn sie es über den Provider versuchen würde). Hierbei ist zu berücksichtigen, dass sich die Wahrscheinlichkeiten aus dem dritten und vierten Schritt nicht «überlappen», falls die beiden Wahrscheinlichkeiten für die Berechnung der Gesamtwahrscheinlichkeit multipliziert werden sollen.

[127] In einem fünften Schritt ist schliesslich zu schätzen, in wie vielen Fällen das Interesse der ausländischen Behörde so gross sein wird, dass sie die Mühen eines *Lawful Access* über den Provider auf sich nimmt. Dies wird nicht in allen Fällen so sein.

[128] Das Ergebnis wird die durchschnittliche Zahl von Fällen pro Jahr sein, in welchen sich das Thema eines *Lawful Access* stellt. Diese kann mit der Anzahl Jahre des Beurteilungszeitraums multipliziert werden und schliesslich mit der Wahrscheinlichkeit, dass ein versuchter *Lawful Access* durch eine ausländische Behörde auch gelingt. Das Ergebnis ist die Gesamtwahrscheinlichkeit, dass es im Beurteilungszeitraum zu einem *Lawful Access* kommt. Anhand dieser Angabe kann wiederum berechnet werden, wieviel Zeit vergehen muss, damit ein erfolgreicher ausländischer *Lawful Access* und damit eine unerlaubte Offenbarung statistisch gesehen auf jeden Fall stattfindet oder nach wie vielen Jahren die Wahrscheinlichkeit eines erfolgreichen *Lawful Access* 50:50 ist. Im Excel werden diese Dinge berechnet und dargestellt.

5. Was das Ergebnis bedeutet

[129] Das Ergebnis ist letztlich keine Vorhersage, *dass* ein Fall eintreten wird oder nicht, sondern eine Aussage zum Risiko, die auf Schätzungen basiert. Fehlen uns in einem Bereich die Erfahrungswerte aus der Vergangenheit, muss sich die Bestimmung der Eintrittswahrscheinlichkeit eines bestimmten, künftigen Ereignisses freilich *immer* mit einer Schätzung begnügen. Diese Schätzung basiert naturgemäss auf gewissen Annahmen und subjektiven Wertungen und ist in diesem Sinne immer auch von unterschiedlichen Verzerrungseffekten beeinflusst, so etwa vom «*motivational bias*» (wenn ein bestimmtes Ergebnis bevorzugt wird) oder dem «*cognitive bias*» (wenn wir unbewusst fehlendes Faktenwissen durch subjektive Eindrücke wettmachen).[124] Trotzdem macht dieses Vorgehen Sinn und entspricht den Regeln der Kunst, denn «Risiko» ist – so der allgemeine Konsensus – das Produkt von Eintrittswahrscheinlichkeit und Schadenshöhe.[125] Im vorliegenden Fall wird die Schadenshöhe – die Folgen der unbefugten Offenbarung von Berufsgeheimnissen – pauschal als maximal angenommen, so dass wir uns nur noch mit der Eintrittswahrscheinlichkeit befassen. Eine Risikobeurteilung ohne Schätzung geht somit nicht. Ihr Ergebnis ist eine *statistische Aussage*, nicht mehr und nicht weniger.

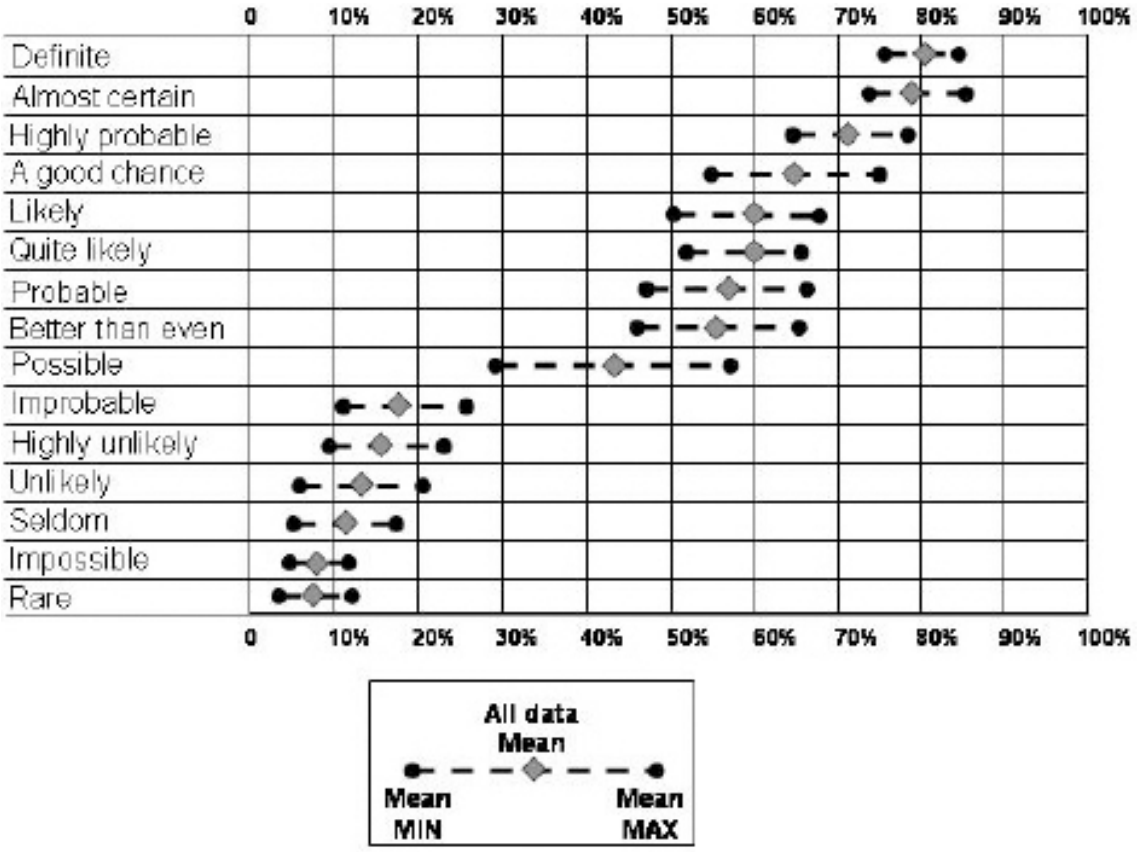
[130] Es bleibt die Gretchenfrage, welches gesamthafte Restrisiko eines *Lawful Access* für ein Cloud-Projekt akzeptabel ist. Aus rechtlicher Sicht wird im Bereich von berufsgeheimnisgeschützten Daten typischerweise auf die Schranken der Strafbarkeit der Entscheidungsträger abgestellt werden. Im Bereich des Bankgeheimnisses wird maximal jenes Risiko akzeptiert, das noch kein fahrlässiges Verhalten indiziert. Die getroffenen Gegenmassnahmen müssen einen *Lawful Access* durch eine ausländische Behörde somit «höchstwahrscheinlich» ausschliessen. Im Bereich der «normalen» Berufsgeheimnisse genügt es hingegen, den Eventualvorsatz zu vermeiden. Hier darf mehr als ein bloss theoretisches Risiko eines *Lawful Access* bestehen, aber es darf nicht so gross sein, dass der Entscheider nicht mehr darauf vertrauen konnte, dass es schon nicht zur unerlaubten Offenbarung gegenüber einer ausländischen Behörde kommt.

---

124 https://www.pmi.org/learning/library/assessing-risk-probability-impact-alternative-approaches-8444 (kontrolliert am 3. Juli 2020).

125 David A. Hillson, David T. Hullet, Assessing Risk Probability: Alternative Approaches, in: PMI Global Congress Proceedings, Prag 2004, S. 1 (http://www.projectrisk.com/white_papers/Assessing_Risk_Probability-_Alternative_Approaches.pdf), kontrolliert am 3. Juli 2020.

[131] Ab welchem Prozentwert dem so ist, wurde bisher nicht entschieden, und wird es womöglich nie werden. So eingängig Zahlen sind, so sehr zwingen sie den Betrachter dazu, trotz der Unschärfe der Materie klar Stellung zu beziehen. In der juristischen Praxis wird daher eine *qualitative* Umschreibung der Wahrscheinlichkeit der quantitativen Ausdrucksweise regelmässig vorgezogen. Sie erlaubt mehr Unschärfe. Allerdings gibt es auch hier keinen einheitlichen Ansatz, wie eine Studie aus dem Jahr 2004 und ihr Update aus dem Jahre 2005 zeigt (eine von ihr für Risikobeurteilungen vorgeschlagene sprachliche Umschreibung des Resultats wird auch im Excel verwendet). Untersucht wurde, wie unterschiedlich bestimmte quantitative Wahrscheinlichkeiten je nach Quelle mit Worten umschrieben wurden:[126]



[132] Nicht alle Bezeichnungen, wie sie von der Studie erhoben wurden, erscheinen sofort nachvollziehbar. Es wird trotz allem deutlich, dass vielerorts ein Ereignis mit einer Eintrittswahrscheinlichkeit von zehn Prozent oder weniger bereits als eher theoretisch betrachtet wird. Dies entspricht auch der folgenden Einteilung, die recht verbreitet ist:[127]

126 David A. Hillson, David T. Hullet (Fn. 125), Exhibit 1, sowie das Update von David A. Hillson, Describing probability: The limitations of natural language, in: PMI Global Congress Proceedings, Edinburgh 2005, Exhibit 4 (https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556), kontrolliert am 2. August 2020.

127 Vgl. etwa statt vieler http://apppm.man.dtu.dk/index.php/Impact_and_Probability_in_Risk_Assessment und http://www2.mitre.org/work/sepo/toolkits/risk/StandardProcess/definitions/occurence.html, kontrolliert am 3. Juli 2020.

Quantitative Wahrscheinlichkeit		Qualitative Umschreibung
Relativ	**Numerisch**	
Sehr tief	0.1 / 10%	Höchst unwahrscheinlich
Tief	0.3 / 30%	Unwahrscheinlich
Mässig	0.5 / 50%	Möglich
Hoch	0.7 / 70%	Wahrscheinlich
Sehr hoch	0.9 / 90%	Sehr wahrscheinlich

[133] Werte unter zehn Prozent erscheinen demnach vergleichsweise ungefährlich, soweit nur das strafrechtliche Risiko der Offenbarung beachtet wird. In der Praxis können freilich andere rechtliche und reputative Aspekte ebenfalls relevant sein, und selbst bei einer eher theoretischen Wahrscheinlichkeit kann Eventualvorsatz gegeben sein, wenn andere Umstände hinzukommen.[128] In diesem Zusammenhang kann sogar die subjektive Wahrnehmung der Person des Dienstleisters von Bedeutung sein: Ein Provider, der in Sachen Datenschutz keinen besonders guten Ruf geniesst, wird auch bezüglich *Lawful Access* womöglich als grösseres Risiko beurteilt als andere Provider, auch wenn es für diesen Schluss keinen sachlichen Grund geben mag, weil sich das Risiko eines *Lawful Access* nach anderen Kriterien bemisst. Auch werden sich viele statistisch weniger Geübte unter dem Prozentwert des Excel nicht viel vorstellen können. Darum wurde der Wert im Excel um die Aussage erweitert, all wieviele Jahre es mit einer 50- oder 90-prozentigen Wahrscheinlichkeit mindestens zu einem *Lawful Access* kommen wird. Wenn sich dann bei einem Wert von 10% ergibt, dass dies nur alle 33 oder 109 Jahre der Fall sein wird, der Cloud-Entscheid aber einstweilen nur für einen Zeitraum von fünf Jahren gefällt wird, erscheint selbst ein vermeintlich hoher Wert von 10% plötzlich als ein eher theoretisches Risiko und macht auch die vorne zitierten sprachlichen Bezeichnungen der Statistiker und Risikospezialisten verständlicher. In einem konkreten Fall wurde der Autor überdies mit der Frage konfrontiert, ob in Bezug auf den US CLOUD Act das akzeptable Restrisiko nicht ausnahmsweise Null sein müsse. In rein rechtlicher Hinsicht kann eine solche Frage nicht ernst gemeint sein, denn alles im Leben birgt Restrisiken; wer auf die Cloud verzichtet und seine IT anders löst, geht damit andere Risiken ein, die gesamthaft womöglich grösser sind. Dass die Frage trotzdem gestellt wird, macht allerdings deutlich, wie sehr das Thema von Emotionen und Unsicherheit geprägt ist. Umso mehr ist zu hoffen, dass dieser Beitrag etwas zur Versachlichung der Diskussion und – wie der Psychologe sagen würde – zur Dissonanzreduktion punkto Cloud beiträgt.

Anhang:

Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail

Zum Anhang

---

128 BGE 131 IV 1, Erw. 2.2 für den Fall einer HIV-Ansteckung.

David Rosenthal, lic. iur., Partner, VISCHER AG, Zürich/Basel/Genf, Schweiz, Lehrbeauftragter an der Universität Basel und der Eidgenössischen Technischen Hochschule Zürich, david@rosenthal.ch.