

Cloud Solutions
Frühlingssemester 2019

Das Recht in der Cloud

Ein Überblick über die geltenden Bestimmungen

Version: 0.2, Datum: 18. Mai 2019

Modulverantwortlicher:

Mirko Stocker
HSR, Rapperswil



erstellt von:

David Loosli
HSR Rapperswil

Inhaltsverzeichnis

1 Einleitung	4
2 Anwendbares Recht	5
2.1 Vertragliche Regelung	5
2.2 Nationales Privatrecht	5
2.3 Internationales Privatrecht	6
2.4 Zusammenfassung	6
2.4.1 Grundprinzip	6
2.4.2 Blick über die Grenze	7
2.4.3 Ausnahme Fallbeispiel	7
3 Schweizerisches Recht	8
3.1 Öffentliches Recht und Privatrecht	8
3.2 Datenschutzrecht	10
3.2.1 Datenschutz	10
3.2.2 Datensicherheit	12
3.2.3 Blick über die Grenze	13
3.2.4 Zusammenfassung	14
3.3 Handels- und Wirtschaftsrecht	16
3.3.1 Gesellschaftsrecht	16
3.3.2 Steuerrecht	18
3.3.3 Zusammenfassung	19
3.4 Immaterialgüterrecht	21
3.4.1 Urheberrecht	21
3.4.2 Markenrecht	22
3.4.3 Patentrecht	23
3.4.4 Blick über die Grenze	23
3.4.5 Zusammenfassung	24
3.5 Allgemeines Vertragsrecht	26
3.6 Schuldbetreibungs- und Konkursrecht	28
3.7 Haftpflichtrecht	30
3.8 Branchenspezifische Regelwerke	31
3.8.1 Banken und Versicherungen	31
3.8.2 Anwaltstätigkeit	32
3.8.3 Weitere Branchen	32
4 Fazit	33

5 Anhang	37
A Kantonale Merkblätter ZH Cloud	37
B FINMA Rundschreiben 2008/21 und 2018/3	57
C Kundendaten im Konkursverfahren (DSB ZH)	105

1 Einleitung

Während das Auslagern von Daten und Rechenkapazität in die Cloud aus technischer Sicht sehr viele Möglichkeiten und Chancen bietet, bringt dies aus juristischer Sicht einige (Rechts-)Unstimmigkeiten und (Rechts-)Unsicherheiten mit sich. Die meisten dieser Probleme entspringen der nicht auf die rechtliche Handhabe von Cloudcomputing ausgerichteten „Architektur“ der historisch gewachsenen Gesetzgebung. So findet sich erstens auch in der Schweiz kein eigenständiges Gesetz zum Thema des Cloudcomputing, sondern es müssen eine Vielzahl von Bestimmungen in verschiedenen Gesetzesstexten zur Beurteilung solcher Fälle herangezogen werden. Zweitens stellt sich aufgrund der Internationalisierung der Datenverarbeitung in der Cloud die Frage nach dem anwendbaren Recht und somit insbesondere welches Land für die Beurteilung einer juristischen Angelegenheit zuständig ist. Als dritter Problemkreis sei erwähnt, dass die Gesetzgebung der technischen Entwicklung stets hinterher hinkt. Dies führt dazu, dass bis anhin einerseits nur sehr wenige Gerichtsurteile die Auslegung nicht ganz eindeutiger Bestimmungen respektive eine Richtung für Abwägungsentscheide enthaltende Regelungen festlegen und andererseits gesetzliche Regelungen neuster technischer Errungenschaften (noch) gänzlich fehlen.

Dieses kurze Skript soll Interessierten mit einer technischen Ausbildung einen Überblick über die zu beachtenden Regelungen im Bereich des Cloud Computing geben und dadurch eine gewisse Sensibilisierung mit Blick auf juristischen Fragestellungen bewirken, ohne zu sehr auf die einzelnen Gesetze und Artikel einzugehen. Dieser Absicht entsprechend erhebt dieses Dokument keinen Anspruch auf Vollständigkeit - ganz im Gegenteil wird bewusst und explizit beispielsweise auf tatsächlich ereignete Fallbeispiele ¹ oder auf die Erläuterung der unzähligen Ausnahmeregelungen verzichtet, um eine stark vereinfachte Merkliste für Personen ohne juristischen Hintergrund ableiten zu können. Diese Merkliste soll sodann als Hilfswerkzeug zur Beurteilung der Frage dienen, ob in einem konkreten Fall ein auf das Themengebiet Cloud spezialisierter Juristinnen und Juristen oder Anwältinnen und Anwälte herangezogen werden sollte.

Ebenfalls nicht Teil dieses Skripts ist die Beurteilung von Service Level Agreements, welche im Rahmen einer separaten Vorlesung in diesem Modul bereits näher betrachtet wurden. Allerdings ist die Einhaltung und Durchsetzbarkeit dieser Bestimmungen der SLA auch für die Erfüllung der gesetzlichen Rahmenbedingungen von grosser Bedeutung.

¹ Auch wenn die Fallbeispiele an tatsächliche Fälle angelehnt sind und somit gewisse Ähnlichkeiten zu tatsächlichen Fällen aufweisen können.

2 Anwendbares Recht

Die Festlegung des anzuwendenden Rechts, d.h. welche nationale Gesetzgebung und welche nationalen Gerichte für die Beurteilung einer Streitigkeit zuständig sind, dürfte in vielen Fällen sowohl der schwierigste als auch derjenige Entscheid mit den grössten Auswirkungen sein und ist zwingend vorab zu klären.

2.1 Vertragliche Regelung

Grundregel - Grundsätzlich gelten zuerst die vertraglich vereinbarten Regelungen zwischen dem Cloud Anbieter und dem Kunden. Im Zusammenhang mit dem Thema des anwendbaren Rechts und dem Gerichtsstand gilt es zu beachten, dass diese - zumindest für die meisten Rechtsfragen - ebenfalls vertraglich festgelegt werden können. Durch die explizite Vereinbarung von Schweizer Recht als anwendbares Recht und einem Gerichtsstand in der Schweiz ¹ kann somit bereits ein beachtlicher Teil der Rechtsunsicherheit eliminiert werden.

Ausnahmen - Finden sich keine oder nur unzureichende vertragliche Regelungen zwischen dem Cloud Anbieter und dem Kunden oder liegen Sachverhalte vor, die keine Gerichtsstandsvereinbarung zu lassen ², so kommen entweder bei rein nationalen Streitigkeiten die Schweizer Gesetzgebung und Gerichte zum Zuge oder bei internationalen Angelegenheiten die umfassenden und gerade im Cloud Computing komplexen Regelungen des internationalen Privatrechts zur Anwendung.

2.2 Nationales Privatrecht

Grundregel - Besitzt eine rechtliche Auseinandersetzung keinerlei Auslandsberührungen, so wird diese entsprechend dem sog. Territorialitätsprinzip nach Schweizer Recht durch ein Schweizerisches Gericht beurteilt. Im Grundsatz gilt, dass auch auf nationaler Ebene die vertraglich vereinbarten Regelungen den allgemeinen gesetzlichen Bestimmungen vorgehen, sofern sie nicht im Widerspruch zu geltendem Recht stehen (e.g. Sittenwidrigkeit, zwingende Bestimmungen im Datenschutz). Welche Rechtsgebiete und Regelungen es beim Thema Cloud zu berücksichtigen gilt, wird im nachfolgenden Kapitel aufgezeigt.

Ausnahmen - Die wichtigste und in den meisten Fällen nur schwierig nachvollziehbare Ausnahme zum Territorialitätsprinzip dürfte die extraterritoriale Wirkung von gesetzlichen Bestimmungen von nicht direkt beteiligten Drittstaaten sein. In solchen Fällen beurteilt ein Drittstaat entgegen der Zuständigkeit

¹ In vielen Fällen wird hier der Wohnort respektive bei Gesellschaften der im Handelsregister eingetragene Sitz des Kunden vereinbart. Den Sitz jeder in der Schweiz eingetragenen Unternehmung ist dem Handelsregister zu entnehmen und kann online unter <https://www.zefix.ch> abgefragt werden.

² Als Beispiel sei das anwendbare Schuldbetreibungs- und Konkursrecht im Falle des Konkurses des Cloud Anbieters erwähnt.

nationaler Gerichte und der Anwendbarkeit von nationalem Recht eine Angelegenheit nach dem eigenen Recht des Drittstaates, wobei die Durchsetzbarkeit solcher Urteile durch Schweizer Behörden nicht in jedem Fall gegeben ist. Insbesondere im Bereich des Cloud Computing dürfte diese Ausnahme jedoch je länger je mehr an Bedeutung gewinnen, wobei für Schweizer Unternehmen vor allem die mögliche Anwendbarkeit von US-Recht (e.g. Patriot Act) und EU-Recht (e.g. Datenschutzgesetz) frühzeitig erkannt werden muss.

2.3 Internationales Privatrecht

Grundregel - Sobald rechtliche Beziehungen ohne vertragliche Regelungen einen internationalen Charakter aufweisen, wird die Angelegenheit sehr viel komplizierter. In diesen Fällen kann erst aufgrund des konkreten Sachverhaltes erörtert werden, welche Gerichte und Gesetzgebungen die Streitigkeit beurteilen soll. Dazu sind im Beispiel der Schweiz neben dem Bundesgesetz über das Internationale Privatrecht (IPRG) auch Bilaterale und Multilaterale Verträge und Übereinkommen zwischen der Schweiz und Drittstaaten (e.g. Lugano Übereinkommen LugÜ, Haager Übereinkommen) zu berücksichtigen, bevor der Gerichtsstand und das anwendbare Recht oder gar die anwendbaren Regelungen bestimmt werden können.

Ausnahmen - Auch in diesem Fall gilt es zu beachten, dass selbst bei der Festlegung des anwendbaren Rechts und des Gerichtsstandes die Problematik der extraterritorialen Wirkung von Gesetzen anderer Staaten in Betracht gezogen werden müssen.

2.4 Zusammenfassung

2.4.1 Grundprinzip

Aufgrund der Komplexität der internationalen Regelungen und der sich daraus ergebenden Rechtsunsicherheit sollte somit folgende Regel beachtet werden.

Merkbox

das gilt es zu beachten

Sämtliche Schweizer Unternehmen sollten beim Going To Cloud einen eigenen, auf ihre Bedürfnisse abgestimmten Vertrag mit dem Cloud Provider abschliessen, welcher Schweizerisches Recht als **anwendbares Recht** und Schweizerische Gerichte als **Gerichtsstand** festlegt.

2.4.2 Blick über die Grenze

Da es sich bei einem Going to Cloud in aller Regel um eine langfristige betriebliche Umstrukturierung handelt, lohnt es sich trotz einer entsprechenden Gerichtsstandsklausel, einen Blick auf rechtliche Entwicklungen ausserhalb der Schweiz zum Thema Cloud zu werfen. Dies vor dem Hintergrund, dass der Schweizerische Gesetzgeber oftmals aufgrund wirtschaftlicher Überlegungen dazu gezwungen ist, neue rechtliche Bestimmung insbesondere aus der Europäischen Union in die nationale Gesetzgebung einfließen zu lassen respektive diese nahezu unverändert zu übernehmen.

2.4.3 Ausnahme Fallbeispiel

Das nachfolgende Fallbeispiel der extraterritorialen Wirkung der seit dem 28. Mai 2018 ihre Wirkung entfaltenden Datenschutz-Grundverordnung (DSGVO) der EU soll jedoch zeigen, dass selbst eine solche Vereinbarung keine vollumfängliche Rechtssicherheit garantieren kann.

Sachverhalt: Eine kleine Schweizer Weinhandlung verwendet für ihren Online Shop eine e-Commerce Solution, welche neben der Schweizer Währung auch die Möglichkeit bietet, die Preise der Produkte auf dem Online Shop in Euro anzuzeigen. Die von einer grösseren Weinhandlung übernommenen Allgemeinen Bestimmen enthalten zudem Lieferangaben für ausländische Kunden und eine Gerichtsstandsklausel für Zürich mit Schweizer Recht als anwendbares Recht. Das Unternehmen besitzt ausschliesslich Schweizer Kunden und verwendet für seine Kundendaten einen Schweizer Cloud Anbieter (bspw. APPUiO).

Fragestellung: Anwendbares und zu berücksichtigendes Recht?

Beurteilung: Im Grundsatz gilt zwar Schweizer Recht, allerdings beurteilen Europäische Gerichte die Anwendbarkeit des DSGVO nach dem sog. Marktortprinzip, so dass aufgrund der möglichen Umstellung auf Euro Preisangaben und den Lieferangaben der AGBs die entsprechenden, strengerer Datenschutzbestimmungen der EU extraterritorial ihre Wirkung entfalten. Dies kann bei Nichteinhaltung zu drastischen Strafen für die kleine Schweizer Weinhandlung führen. Allerdings dürfte sich dieses Problem mit der kommenden Anpassung des Schweizerischen Datenschutzgesetzes an das EU Recht etwas abschwächen.

3 Schweizerisches Recht

Im vorangegangenen Kapitel wurde aufgezeigt, dass sich aufgrund der sehr komplexen Materie des Internationalen Privatrechts eine Festlegung des Gerichtsstands und des anwendbaren Rechts für Schweizer Unternehmen lohnt. Deshalb werden im Folgenden nur die gesetzlichen Bestimmungen des Schweizerischen Rechts näher betrachtet werden, welche Berührungspunkte mit der Thematik der Cloud aufweisen.

3.1 Öffentliches Recht und Privatrecht

Grundregel - Eine erste grosse Trennung in der „Architektur“ der Schweizerische Gesetzgebung ist diejenige zwischen Privatrecht und öffentlichem Recht. Während das öffentliche Recht das Verhältnis zwischen dem Staat und seinen Bürgerinnen und Bürgern regelt (sog. Subordinationstheorie, bspw. Verwaltungsrecht [Bildungswesen, Baurecht etc.], Strafrecht, Steuerrecht, Strassenverkehrsrecht u.v.m.), legt das Privatrecht diejenigen Regeln fest, welche zwischen Privatpersonen - darunter fallen sowohl natürliche Personen (i.e. Menschen) als auch juristische Personen (i.e. Unternehmen) - zu berücksichtigen sind (bspw. Zivilgesetzbuch, Obligationenrecht und div. Sondergesetze und Erlasse). Diese Trennung besitzt auch Auswirkungen auf das Thema des Cloud Computing:

- *Öffentliches Recht*: Während die privatrechtlichen Bestimmungen einen Mindeststandard für das Auslagern von Daten in die Cloud festlegen, gehen die meisten Behörden und öffentlich-rechtlichen Institutionen einen Schritt weiter. So finden sich beispielsweise im Kanton Zürich verschiedenste kantonale Verordnungen und Merkblätter zu diesem Thema, welche weitaus strengere Vorschriften und ausführliche Checklisten festlegen (vgl. Anhang A) und sogar gewisse kryptographische Algorithmen vorschreiben. Aufgrund der Vielzahl dieser Bestimmungen ist im Bereich des Öffentlichen Rechts stets anhand des konkreten Falles zu entscheiden, weshalb nachfolgend nur noch auf das Privatrecht eingegangen wird.
- *Privatrecht*: Für privatrechtliche Fragestellungen im Bereich des Cloud Computing gilt es verschiedenste Gesetze zu berücksichtigen - die wichtigsten Gesetzestexte werden in diesem Skript näher betrachtet.

Merkbox

das gilt es zu beachten

Für Institutionen und Behörden des Öffentlichen Rechts sind neben den vertraglichen Regeln zwingend die entsprechenden (verschärften) Regelungen zum Thema Cloud zu berücksichtigen. Subjekte des Privatrechts unterstehen den nachfolgenden Bestimmungen (gesetzliche Mindestanforderungen).

Ausnahmen - Die Abgrenzung zwischen Öffentlichem Recht und Privatrecht ist leider nicht wirklich trennscharf. So statuiert beispielsweise Artikel 178 Absatz 3 der Bundesverfassung die Möglichkeit des Staates, öffentliche Aufgaben unter gewissen Voraussetzungen an Private zu übertragen¹. Diese Privatpersonen oder privaten Unternehmen unterstehen sodann je nach Ausgestaltung der rechtlichen Beziehung in vielerlei Hinsicht Öffentlichem Recht². Des Weiteren existieren Organisationen, die auf den ersten Blick als privatrechtliches Unternehmen qualifiziert werden könnten, jedoch dem öffentlichen Recht unterstehen. Als Beispiel sei an dieser Stelle die FINMA erwähnt, welche als unabhängige Behörde über den schweizerischen Finanzmarkt hoheitliche Befugnisse über Banken, Versicherungen, Börsen, Effektenhändler, kollektive Kapitalanlagen, deren Vermögensverwalter und Fondsleitungen sowie Vertriebsträger und Versicherungsvermittler besitzt. Ein Bundesgerichtsentscheid aus dem Jahre 2016³ bestätigt demnach auch, dass die Angestellten der FINMA als Beamten und Beamten gelten und somit das Amtsgeheimnis zu wahren haben.

Fallbeispiel - Das nachfolgende Fallbeispiel soll die Ausnahme der Übertragung öffentlicher Aufgaben an Privatunternehmen illustrieren. Es gilt die **Annahme**, dass diese Übertragung grundsätzlich erlaubt sei (i.e. genügende gesetzliche Grundlage, öffentliches Interesse und die Beaufsichtigung seien erfüllt).

Sachverhalt: Die Steuersoftware mit der Möglichkeit der Online Einreichung der Steuererklärung wird durch ein privates Unternehmen programmiert. Zur Vereinfachung für den Steuerprüfer werden einige Berechnungen bereits durch den Servern des Unternehmens ausgeführt, bevor die Daten an das Steueramt weitergereicht werden. Aufgrund der gestiegenen Anforderungen an die Rechenleistung möchte das Unternehmen nun in die Cloud und hat bereits erste Abklärungen vorgenommen, um den geltenden privatrechtlichen Grundlagen zu genügen.

Fragestellung: Untersteht das Unternehmen dem Privatrecht?

Beurteilung: Im Grundsatz ist dies zu bejahen. Nun stellt sich jedoch bezüglich der Steuersoftware die Frage, ob mit den Berechnungen und den erhobenen Steuerdaten bereits eine Übertragung einer öffentlichen Aufgabe an das Privatunternehmen stattgefunden hat. Wird diese Frage bejaht, so dürfte - unabhängig vom Kanton - das Unternehmen diesbezüglich den (strengeren) Vorschriften des Öffentlichen Rechts unterstehen und somit würden die bisherigen Abklärungen **nicht** genügen.

¹ vgl. <https://www.egovernment.ch/.../ubertragung-von-offentlichen-aufgaben-an-private/>, letztmals besucht: 18. Mai 2019

²Zur Abwägung, ob eine bestimmte Rechtslage dem öffentlichen Recht oder dem Privatrecht unterliegt, finden sich diverse Abhandlungen und Publikationen. Details zu dieser Abgrenzung finden sich bspw. in einem Artikel in der Zeitschrift recht - *Was sind öffentliche Aufgaben?*, Bernhard Rütsche, recht 2013, Heft 4, Seite 153 ff., zu finden unter https://www.unilu.ch/.../Ruetsche_recht_OeffentlicheAufgaben_2014.pdf, letztmals besucht: 18. Mai 2019

³Bundesgerichtsentscheid 6B 182/2016, https://entscheide.weblaw.ch/cache.php?link=10.11.2015_SK.2015.35

3.2 Datenschutzrecht

Durch die Auslagerung von Daten in die Cloud nimmt ein Unternehmen zwangsläufig einen gewissen Kontrollverlust bezüglich der Datenbearbeitung in Kauf. Die wichtigsten Regelungen, die es diesbezüglich zu beachten gilt, finden sich im Schweizerischen Datenschutzgesetz⁴.

3.2.1 Datenschutz

Grundregel - Das Datenschutzgesetz DSG bezweckt im Grundsatz den Schutz der Persönlichkeit von bestimmten oder bestimmbaren natürlichen (d.h. Menschen) und juristische Personen (i.e. Unternehmen), über welche Daten erhoben und bearbeitet werden. Grundsätzlich findet das Gesetz auf sämtliche Personendaten Anwendung (auch solche auf den eigenen Servern!), wobei für besonders schützenswerte Personendaten noch strengere Vorschriften gelten. Unter dem Begriff *bearbeiten* ist nach Artikel 3 lit. e jeder Umgang mit Personendaten zu verstehen unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Sollen nun bestimmte Daten in der Cloud bearbeitet werden, so ist in einem ersten Schritt zu prüfen, ob es sich tatsächlich um Personendaten handelt. Allerdings gilt es zu berücksichtigen, dass der Begriff der Personendaten auch in der Schweiz sehr weit gefasst ist - nach EU Richtlinien fällt beispielsweise selbst das Sammeln von Browser Fingerprint Daten unter das Datenschutzgesetz.

Merkbox

das gilt es zu beachten

Die Datenbearbeitung muss Personendaten im Sinne des Datenschutzrechtes betreffen. Ansonsten sind die Merkboxen in diesem Abschnitt für die Auslagerung von Daten in die Cloud **nicht** zwingend zu berücksichtigen.

In einem zweiten Schritt gilt es sodann die Voraussetzungen nach Artikel 10a des Datenschutzgesetzes zu prüfen. Demnach ist eine Auslagerung von Personendaten an einen Dritten (i.e. der Cloud Anbieter) dann zulässig, wenn **(a)** der Dritte die Daten nur so bearbeitet, wie dies auch der Cloud Kunde tun dürfte; **(b)** keine Geheimhaltungspflicht (bspw. Anwaltsgeheimnis etc.) dies verbietet; und **(c)** die Datensicherheit gewährleistet ist.

Merkbox

das gilt es zu beachten

Der Vertrag muss sowohl die genau Art der Datenverarbeitung als auch den Rahmen der Datensicherheit mit entsprechenden Überprüfungs- und Durchsetzungsmöglichkeiten festhalten.

⁴<https://www.admin.ch/opc/de/classified-compilation/19920153/index.html>, letztmals besucht: 18. Mai 2019

Grundsätzlich gilt auch für diese Gesetzgebung das Territorialitätsprinzip (vgl. Kapitel 2). Allerdings ist zu beachten, dass selbst für einen Schweizer Cloud Anbieter nicht der Sitz in der Schweiz für die Beurteilung der Zulässigkeit der Auslagerung an Dritte massgebend ist, sondern der tatsächliche Ort der Datenbearbeitung (insbesondere Serverstandorte und Datencenter). Auch ausländische Unternehmen mit Sitz ausserhalb der Schweiz, deren Server in der Schweiz stehen oder die Personendaten von in der Schweiz lebenden Personen sammeln, fallen unter das Schweizer Datenschutzgesetz.

Merkbox

das gilt es zu beachten

Der Vertrag muss sämtliche möglichen Orte der Datenverarbeitung (i.d.R. Serverstandorte) aufführen und eine Pflicht des Cloud Anbieters zur Auskunftserteilung und Meldung von Standortwechseln festlegen.

Den betroffenen Personen stehen verschiedene Rechte bezüglich der über sie abgespeicherten Daten zu. Darunter fallen ein Auskunftsrecht, die Richtigkeit der Daten, Anspruch auf angemessene Datensicherheit, Verhältnismässigkeit u.v.m. Um diese Ansprüche auch gegenüber dem Cloud Anbieter geltend machen zu können, muss der Cloud Kunde ein entsprechendes Weisungsrecht vereinbaren.

Merkbox

das gilt es zu beachten

Ein vertraglich festgehaltenes Weisungsrecht gegenüber dem Cloud Anbieter ist zwingend erforderlich.

Ausnahmen - Die im Bereich des Cloud Computing wohl wichtigste Ausnahme findet sich in Artikel 6 des DSG, wonach Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Diese Bestimmung besitzt eine enorme Auswirkung bei der Auswahl des Cloud Anbieters, da beispielsweise die USA grundsätzlich⁵ als Land qualifiziert wird, welches über **kein** angemessenes Datenschutzniveau verfügt (IBM, Azure, Amazon u.v.m.)⁶. Eine weitere Kategorie von Ausnahmen bilden Spezialregelungen für besondere Geheimhaltungspflichten (Anwaltsgeheimnis, Bankengeheimnis u.s.w.). Die erste Ausnahme ist derart wichtig, dass sie eine eigene Merkbox erhält:

⁵ Selbstverständlich gibt es auch in diesem Fall Ausnahmen von der Ausnahme, insbesondere Artikel 6 Absatz 2 und das Label „unter bestimmten Voraussetzungen“ der Länderliste des EÖDB unter <https://www.edoeb.admin.ch/.../staatenliste.pdf>, wobei bis 2017 die USA in der Länderliste noch explizit als mit ungenügendem Schutz qualifiziert wurde (und dies nach Meinung vieler Fachexperten auch hätte bleiben sollen).

⁶ Mehr zum Thema Datenschutz und USA findet sich in der Masterarbeit *Cloud Computing – Eine rechtliche Gewitterwolke?* von Eric T. Neuenschwander ab Seite 17.

Merkbox

das gilt es zu beachten

Das Datenschutzniveau an den Standorten der Datenverarbeitung des Cloud Anbieters muss im Mindesten dem Datenschutzniveau der Schweiz entsprechen. Die USA verfügt grundsätzlich **nicht** über einen entsprechenden Datenschutz!

3.2.2 Datensicherheit

Grundregel - Im Zusammenhang mit dem Datenschutz muss zwingend auch das Thema Datensicherheit angesprochen werden. Artikel 7 des Datenschutzgesetzes bestimmt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Die Konkretisierung dieses Artikels findet sich einerseits in der Verordnung zum Bundesgesetz über den Datenschutz VDSG und andererseits in verschiedenen Weisungen der Behörden. Die von Artikel 8 und 9 der Datenschutzverordnung verlangten Massnahmen werden zu einem grossen Teil vom bereits in der Vorlesung erläuterten Service Level Agreement (SLA) abgedeckt - darunter fallen insbesondere die Datentrennung (i.e. public vs. private Cloud), Verfügbarkeit, Zugriffsrechte, etc. Allerdings müssen an dieser Stelle zwei Aspekte noch genauer betrachtet werden:

- *Kontrolle des Cloud Anbieters*: Grundsätzlich ist der Cloud Kunde nach Artikel 10a des DSG dazu verpflichtet, den Cloud Anbieter bezüglich der Einhaltung der Vereinbarungen zu kontrollieren. Während die Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) lautet, die entsprechende Einhaltung der vertraglichen Regeln periodisch vor Ort beim Cloud Anbieter zu prüfen, wird in der Lehre davon ausgegangen, dass regelmässige Reportings des Cloud Anbieters ausreichen sollten. Eine Konkretisierung durch einen Gerichtsentscheid findet sich diesbezüglich jedoch nicht.
- *Verschlüsselung*: Die vorgenannten Artikel implizieren die Pflicht zur „genügenden“ Verschlüsselung von Personendaten, d.h. Klartextspeicherung in einer Datenbank mit Zugriffskontrolle dürfte in der Regel nicht ausreichen. Zudem wird in den meisten Fällen nicht in Betracht gezogen, dass ein Cloud Anbieter grundsätzlich kein Interesse an einer Verschlüsselung der Daten besitzt - dadurch würde sein oftmals vereinbartes Recht an den persönlichen Daten ihrer Kunden wirkungslos ⁷. Ebenfalls Abhilfe schafft die Verschlüsselung der Personendaten in sämtlichen bereits beschriebenen (e.g. extraterritoriale Wirkung) und nachfolgend erläuterten Problembereichen (Schuldbetreibungs- und Konkursrecht u.s.w.). Die Verschlüsselung der Daten sollte jedoch nicht durch den Cloud Anbieter sondern den Cloud Kunden selbst vorgenommen werden. Denn eine Vereinbarung zur Verschlüsselung der Personendaten durch den Cloud Anbieter löst zwar das Problem der Zugriffe unbefugter Dritter, nicht jedoch beispielsweise die Verwertung im Konkursfall (vgl. dazu Abschnitt 3.6).

⁷ Details zu diesen Überlegungen finden sich unter <https://www.admin.ch/.../medienmitteilungen.msg-id-60444.html> und in der Masterarbeit *Cloud Computing – Eine rechtliche Gewitterwolke?* von Eric T. Neuenschwander auf den Seiten 20, 30.

Obwohl in diesem Skript der juristische Aspekt des Going to Cloud beleuchtet werden soll, sind an dieser Stelle noch einige technische Überlegungen zum Thema Verschlüsselung festzuhalten. In der juristischen Literatur wird jeweils nur von Verschlüsselung der Daten gesprochen, ohne eine technische Differenzierung vorzunehmen. Während die Verschlüsselung von *data at rest* aufgrund des Verbleibs der Schlüssel beim Cloud Kunden unproblematisch erscheint, findet sich jedoch bei der Standardkommunikation (d.h. *data at transfer*) und der Verarbeitung der Daten in der Cloud (i.e. *data in use*) die Problematik, dass der Private Key auch in der Cloud abgespeichert werden muss. Eine Untersuchung dieser Problematik könnte für zukünftige Anwendungen durchaus interessant sein.

Merkbox

das gilt es zu beachten

Der Vertrag muss zwingend die Pflicht des Cloud Anbieters zu einem regelmässigen Reporting bezüglich der Einhaltung der Vereinbarungen beinhalten.

Ausnahmen - Die wohl wichtigste Ausnahme in diesem Bereich findet sich zum Thema Verschlüsselung der Daten. In verschiedenen Spezialgesetzen, Weisungen und internen Richtlinien sowohl zu öffentlichrechtlichen als auch privatrechtlichen Organisationen finden sich strengere Bestimmungen zur Verschlüsselung der Personendaten - so hält die FINMA bezüglich Bankkundendaten fest, dass „eine wirksame und zeitgemäss Verschlüsselung“ nötig sei und „die Reidentifikation aufgrund der Entschlüsselung mit Hilfe des **geheimen** Schlüssel“ erfolgen müsse⁸. Letzteres impliziert meines Erachtens, dass der private Schlüssel stets in der Schweiz beim Cloud Kunden (i.e. der Bank) zu verbleiben hat.

3.2.3 Blick über die Grenze

Mit der am 28. Mai 2018 in Kraft getretenen Datenschutz-Grundverordnung (DSGVO) versucht die Europäischen Union, der sich aufgrund der vermehrten Nutzung von Online Diensten (e.g. Online Shops, Google Dienste, Facebook etc.) und Cloud Lösungen stark veränderten Situation im Bereich des Datenschutzes auch rechtlich anzupassen. Nach einem Jahr der Anwendbarkeit der neuen Verordnung lassen sich bereits erste, auch den durchschnittlichen Internet-User betreffende Auswirkungen feststellen, wobei nachfolgend zwei davon näher betrachtet werden sollen:

- *Facebook Custom Audience*: FCA ist ein Werbeverfahren, über welches Facebook und Instagram Usern zielgerichtet Werbung angezeigt werden kann. Aus technischer Sicht verwendet das Verfahren die Hashes von (verschlüsselten) Kundendaten eines Unternehmens, um diese mit eigenen, gehaschten Nutzerdaten zu vergleichen und so eine Werbezielgruppe erstellen zu

⁸FINMA Rundschreiben 2008/21 Operationelle Risiken - Banken, vgl. Anhang B

können. Der Bayerische Verwaltungsgerichtshof bestätigte nun basierend auf der DSGVO, dass der Einsatz von Facebook Custom Audience durch ein Unternehmen trotz Hashwerten (analog zum Browser Fingerprint) ohne Einwilligung des Nutzers respektive Kunden gegen das Datenschutzrecht verstößt und somit unzulässig sei⁹. Dieser Entscheid dürfte sowohl aus juristischer als auch wirtschaftlicher Sicht die bisher grösste Tragweite aufweisen¹⁰.

- *Cookie Hinweise:* Den meisten dürfte aufgefallen sein, dass sämtliche Webseiten, welche Cookies verwenden, seit dem Inkrafttreten der Verordnung einen entsprechenden Hinweis anzeigen müssen. Grund dafür ist unter anderem die Qualifizierung eines Browser Fingerprint als personenbezogene Daten, wodurch ein entsprechendes Tracking unter die DSGVO fällt. Auch Schweizer Unternehmen sehen sich dazu gezwungen, entsprechende Meldungen auf ihren Webseiten zu publizieren. Details zum Umfang dieser Cookie Hinweise finden sich unter anderem auf der CookieBot Webseite¹¹.



Abbildung 3.1: Cookie Bot Webseite mit Beispiel Hinweis

3.2.4 Zusammenfassung

Grundprinzip - Einerseits kratzen die vorangegangenen Erläuterungen des Datenschutzgesetzes der Schweiz nur an der Oberfläche der gesamten Thematik und andererseits besteht in vielerlei Hinsicht

⁹ <https://datenschutzbeauftragter-dsgvo.com/dsgvo-entscheidung-einsatz-facebook-custom-audience>, letztmals besucht: 18. Mai 2019

¹⁰ vgl. dazu auch die Richtlinien zu FCA unter <https://www.activemind.de/magazin/facebook-custom-audiences-datenschutzbehoerde> sowie das Überprüfungsmerkblatt des Bayerischen Landesamtes für Datenschutzaufsicht (i.e. Merkblatt), letztmals besucht: 18. Mai 2019

¹¹ <https://www.cookiebot.com/de/cookie-hinweis>, letztmals besucht: 18. Mai 2019

aufgrund fehlender Urteile und der aktuellen Änderungen der Gesetzgebung eine gewisse Rechtsunsicherheit in diesem Gebiet. Zusammenfassend und als Faustregel sei deshalb an dieser Stelle auf die Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) verwiesen:

Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) die Daten sind, umso eher ist von einer Auslagerung der Daten in die Cloud abzusehen, und desto strikter und umfassender müssen die (Datenschutz-) Sicherheitsvorkehrungen und deren Kontrolle sein.

Fallbeispiel - Das nachfolgende, wohl auch bei Informatikerinnen und Informatikern bekannte und ausnahmsweise konkrete Fallbeispiel soll die Auslegung des Begriffs der Personendaten und die Folgen illustrieren.

Sachverhalt: Seit August 2009 bietet Google im Internet den Dienst *Street View* für die Schweiz an. Es handelt sich dabei um eine Funktion in Google Maps, mit welcher sich virtuelle Rundgänge namentlich durch Strassen und Plätze unternehmen lassen. Auf den Bildern wurden Gesichter von aufgenommenen Personen und Kennzeichen von Fahrzeugen automatisch verwischt (sog. Blurring). Mehrere Personen, die sich durch einzelne Bilder in ihren Persönlichkeitsrechten verletzt fühlten, wandten sich gegen die Publikation an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Dieser hielt die automatische Bearbeitung der Bilder mit einer Anonymisierungssoftware für ungenügend, weil lediglich ein Teil der Gesichter und Kennzeichen verwischt wurde.

Fragestellung: Sind nicht perfekt verwischte Bilder von Personen und Autokennzeichen als Personendaten im Sinne des DSG zu qualifizieren?

Beurteilung: Das Bundesgericht in seinem Urteil ([BGE 138 II 346](#)) bestätigte die Meinung des EDÖB, dass das Fotografieren und die anschliessende Übermittlung der Bilder zur Weiterbearbeitung in die USA eine Bearbeitung von Personendaten darstelle, welche die Persönlichkeitsrechte der betroffenen Personen verletze, wenn es sich um Daten aus deren Privatbereich handle. Die Verwendung von Bildern der näheren Umgebung des Lebensmittelpunkts einer Person sei unzulässig, da die Betroffenen trotz unkenntlich gemachtem Gesicht identifiziert werden könnten. Der Betrieb von Google Street View stelle nur dann keine Persönlichkeitsverletzung dar, wenn eine angemessene Unkenntlichmachung gewährleistet sei, sodass ein Personenbezug verneint werden könne. Falls die automatische Verwischung in diesem Bereich nicht funktioniere, könne eine betroffene Person aufgrund der Zoom-Funktionen individualisiert dargestellt und identifiziert werden, was die Persönlichkeitsrechte der Betroffenen verletze ¹².

¹²Details und Auswirkungen des Entscheides finden sich unter <https://www.edoeb.admin.ch/.../bundesgerichtentscheid-zu-google-street-view-erkennnisse-fuer.html>

3.3 Handels- und Wirtschaftsrecht

Unter dem Begriff des Handels- und Wirtschaftsrechts wird eine Menge von Gesetzen und Regelungen zusammengefasst, welche einen direkten Bezug zur Wirtschaft aufweisen. Darunter fallen insbesondere die gesetzlichen Bestimmungen des Gesellschaftsrechts als Teil des OR mit den von den Unternehmen in ihren verschiedenen Gesellschaftsformen (i.e. Aktiengesellschaft AG, GmbH etc.) zu berücksichtigenden Regeln, aber auch das Steuerrecht besitzt verschiedene Berührungspunkte.

3.3.1 Gesellschaftsrecht

Grundregel - Das Gesellschaftsrecht befasst sich mit der Gründung, der Organisation der einzelnen Organen (i.e. Verwaltungsrat, Gesellschafterversammlung etc.), den Beteiligungsgrundsätzen (i.e. Erhöhung des Aktienkapitals etc.) und der Auflösung der verschiedenen Unternehmensformen (i.e. Kollektiv-, Aktiengesellschaft, Einzelunternehmen, Gesellschaft mit beschränkter Haftung GmbH etc.). Allen Formen gemeinsam ist die Pflicht zur Buchführung nach Artikel 957 OR, sofern das Unternehmen im Handelsregister eingetragen wurde respektive werden musste. Die Verarbeitung solcher aus dem Gesellschaftsrecht vorgeschriebener Dokumente (i.e. Gründungsurkunden, Statuten, Gesellschafterverträge, Finanz- und Betriebsbuchhaltung) ist gemäss Artikel 957a Absatz 5 OR grundsätzlich auch in elektronischer Form zulässig und umfasst nach Artikel 957a Absatz 3 OR alle schriftlichen Aufzeichnungen auf Papier oder in elektronischer oder vergleichbarer Form, die notwendig sind, um den einer Buchung zugrunde liegenden Geschäftsvorfall oder Sachverhalt nachvollziehen zu können ¹³.

Merkbox

das gilt es zu beachten

Die Datenbearbeitung muss Geschäfts- und Buchführungsdaten im Sinne des Obligationenrechts betreffen. Ansonsten sind die Merkboxen in diesem Abschnitt für die Auslagerung von Daten in die Cloud **nicht** zwingend zu berücksichtigen.

Während die Möglichkeiten der elektronischen Verarbeitung solcher Daten grundsätzlich bereits durch das Thema der Digitalisierung ausgelotet werden, sind bei einem allfälligen Going to Cloud noch zwei weitere Problembereiche zu berücksichtigen: die Aufbewahrungspflicht und die offensichtlichen Berührungs punkte mit dem Datenschutzgesetz. Nach Artikel 958f OR sind die Geschäftsbücher und die Buchungsbelege sowie der Geschäftsbericht und der Revisionsbericht während zehn Jahren aufzubewahren, wobei die Aufbewahrungsfrist mit dem Ablauf des Geschäftsjahres beginnt. Die Aufbewahrung der Daten darf nach Absatz 3 der Bestimmung auch elektronisch erfolgen, sofern die Daten jederzeit wieder lesbar gemacht werden können. Diese sehr allgemein gehaltenen Regelungen zur Aufbewahrungspflicht werden in der Verordnung über die Führung und Aufbewahrung der Geschäftsbücher Ge-BÜV noch differenziert festgelegt. Im Zusammenhang mit Cloud Computing ist insbesondere Artikel 9

¹³ Darunter können gemäss der allgemeinen Lehre auch eMails fallen, was es bei der Umstellung von einer intern betriebenen eMail-Software auf einen eMail-Cloud-Service zu beachten gilt.

Absatz 1 lit. b GeBüV zu berücksichtigen - nach diesem Artikel ist eine Aufbewahrung gesellschaftsrechtlicher Daten auf veränderbare Informationsträger nur dann zulässig, wenn

- (1) technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren),
- (2) der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z. B. durch Zeitstempel),
- (3) die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden, und
- (4) die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie die entsprechenden Hilfsinformationen (z.B. Protokolle und Log Files) ebenfalls aufbewahrt werden.

Während die Verfügbarkeit der Daten bereits durch das Service Level Agreement abgedeckt werden sollte, muss der Cloud Kunde entweder selbstständig die obgenannten Verfahren implementieren oder allfällige Massnahmen und Möglichkeiten mit dem Cloud Provider besprechen sowie vertraglich festhalten. Es sei noch angemerkt, dass eine vorsätzliche oder fahrlässige Verletzung der Aufbewahrungspflicht auch strafrechtlich relevant ist (u.a. Artikel 325 Strafgesetzbuch StGB).

Merkbox

das gilt es zu beachten

Der Vertrag zwischen dem Cloud Provider und dem Kunden muss zwingend allfällige Massnahmen zur Aufbewahrungspflicht beinhalten. Sofern der Cloud Kunde die Massnahmen selbstständig implementiert, ist im Minimum eine vereinfachte BackUp und Download Möglichkeit archivierter gesellschaftsrechtlicher Daten zu vereinbaren.

Der zweite Punkt, welcher im Zusammenhang mit gesellschaftsrechtlichen Daten angesprochen werden muss, sind die Berührungspunkte im Bereich der Finanz- und Betriebsbuchhaltung¹⁴ mit dem Datenschutzgesetz. Sowohl die Finanz- als auch die Betriebsbuchhaltung beinhalten naturgemäß Kundendaten (bspw. auf Rechnungen, Lagervorgängen etc.) und unterliegen somit den Bestimmungen des Datenschutzes. Dies wird bei einem Gang in die Cloud oftmals vergessen.

Ausnahme - Die wohl wichtigste Ausnahme zur gesellschaftsrechtlichen Aufbewahrungspflicht betrifft Daten, die im Zusammenhang mit Grundstücken und Liegenschaften zu Eigentum stehen. Solche Daten müssen nicht nur über 10 Jahre hinweg, sondern über 20 Jahre ab dem Ende des jeweiligen

¹⁴Die Finanzbuchhaltung soll Aufschluss über die finanzielle Situation des Unternehmens liefern und ist nach aussen hin relevant (d.h. für die Steuerbehörden). Es müssen die rechtlichen Bestimmungen zur Buchführung eingehalten werden. Demgegenüber wird die Betriebsbuchhaltung nur intern zur Entscheidungsfindung im Management eingesetzt und ist deshalb viel detailliert als die Finanzbuchhaltung.

Geschäftsjahres aufbewahrt werden. Besitzt somit eine Gesellschaft eine eigene respektive eigene Liegenschaft(en) oder verwaltet solche, müssen bis zu 21 Jahre alte Unterlagen aufbewahrt, gefunden und auch wieder gelesen werden können.

3.3.2 Steuerrecht

Grundregel - Unter dem Begriff des Steuerrechts wird eine Vielzahl von Vorschriften sowohl auf Bundesebene als auch auf kantonaler Ebene zur Abgabepflicht von Unternehmen gegenüber Staat, Kantonen und Gemeinden zusammengefasst. Darunter fallen insbesondere die Einkommen- und Vermögenssteuer, aber auch die Mehrwertsteuer und weitere Abgabepflichten.

Merkbox

das gilt es zu beachten

Bei den betroffenen Daten muss es sich um steuerrechtlich relevante Informationen handeln. Ansonsten sind die Merkboxen in diesem Abschnitt für die Auslagerung von Daten in die Cloud **nicht** zwingend zu berücksichtigen.

Analog zum Gesellschaftsrecht ist auch in diesem Rechtsgebiet im Zusammenhang mit dem Cloud Computing insbesondere auf die Auskunfts- und Aufbewahrungspflicht für steuerliche Daten hinzuweisen. Nach Artikel 126 des Bundesgesetzes über die direkte Bundessteuer (DBG) muss beispielsweise sichergestellt sein, dass auf Verlangen der Veranlagungsbehörde mündlich oder schriftlich Auskunft erteilt werden kann und Geschäftsbücher, Belege und weitere Bescheinigungen sowie Urkunden über den Geschäftsverkehr während zehn Jahren vorgelegt werden können. Zudem gelten bezüglich der Archivierung die Vorschriften aus dem Gesellschaftsrecht analog.

Merkbox

das gilt es zu beachten

Der Vertrag zwischen dem Cloud Provider und dem Kunden muss zwingend allfällige Massnahmen zur Aufbewahrungspflicht beinhalten. Sofern der Cloud Kunde die Massnahmen selbstständig implementiert, ist im Minimum eine vereinfachte BackUp und Download Möglichkeit archivierter steuerrechtlicher Daten zu vereinbaren.

Ausnahmen - Neben der bereits erwähnten Ausnahme der 20 Jahre dauernden Aufbewahrungsvorschrift im Zusammenhang mit Grundstücken und Liegenschaften gilt es im Steuerrecht zudem zu berücksichtigen, dass grundsätzlich der Kanton die Steuerhoheit besitzt und somit auch eigene Fristen erlassen kann. So gilt im Kanton Zürich beispielsweise eine Aufbewahrungspflicht während 15 anstatt 10 Jahren.

3.3.3 Zusammenfassung

Grundprinzip - Während die rechtlichen Vorschriften im Bereich des Gesellschafts- und Steuerrechts mit Blick auf die Aufbewahrungspflicht in der Cloud relativ eindeutig sind, dürften in diesem Themenbereich die technischen Lösungen als Hauptproblematik im Vordergrund stehen.

So nutzen beispielsweise viele Unternehmen zur Erstellung ihrer Buchhaltung und Einreichung ihrer Steuerunterlagen entweder die offizielle kantonale Steuersoftware oder Software eines Drittanbieters. Da die Daten auch in 10 bis 20 Jahren noch gelesen werden müssen, empfiehlt es sich die Software ebenfalls zu archivieren, wobei allfällige Abhängigkeiten (i.e. Betriebssystem etc.) zu berücksichtigen sind. Dies muss zwingend auch für Buchhaltungs- und Steuersoftware möglich sein, die von einem Cloud Anbieter in Form von Software as a Service zur Verfügung gestellt wird. In letzterem Fall sollten unbedingt auch eine Risikoabschätzung bezüglich des Lock In Effekts und der Portabilität sowie die bereits erwähnten lizenzirechtlichen Abklärungen vorgenommen werden.

Fallbeispiel - Anstelle eines Fallbeispiels soll mit den nachfolgenden Darstellungen verdeutlicht werden, was „20 Jahre lesbar“ aus Sicht der Praxis bedeutet. Dazu die wichtigsten beiden Errungenschaften aus dem EDV Bereich des Jahres 1997:

- *Power Macintosh G3*: Desktop Variante mit 233 MHz Prozessor, 32 MB RAM, Floppy Disk und 4 GB Harddisk sowie Mac OS 8 für 2'400 Dollar¹⁵ (entspricht einer heutigen Kaufkraft von rund 3'500 bis 4'000 CHF).



Abbildung 3.2: Power Macintosh G3, Desktop

¹⁵https://everymac.com/systems/apple/powermac_g3/specs/powermac_g3_233_dt.html, letztmals besucht: 18. Mai 2019

- *CD-RW*: von Philips mit 650 MB für rund 40 Dollar - leider waren die entsprechend benötigten CD-RW Recorder für KMU's mit einem Preis von damals weit über 10'000 Dollar kaum erschwinglich ¹⁶.



Abbildung 3.3: Philips Compact Disc Recorder CDR870, allerdings 1998

Diese beiden im Jahr 1997 auf den Markt gebrachten Produkte zeigen, dass beispielsweise eine noch der Aufbewahrungspflicht unterliegende Liegenschaftenabrechnung von damals ohne weitere Vorkehrungen heutzutage wohl kaum noch gelesen werden kann. Überlegt sich ein Unternehmen, seine gesellschafts- und steuerrechtlichen Daten nur noch elektronisch zu speichern, ist zwingend auch ein Organisationskonzept zu erstellen, welches die im Zusammenhang mit dem Thema Aufbewahrung stehenden Pflichten berücksichtigt.

¹⁶ <https://www.philips.com/a-w/research/technologies/cd/cd-family.html>, letztmals besucht: 18. Mai 2019

3.4 Immaterialgüterrecht

Immaterialgüterrechte sind Schutzrechte für Schöpfungen technischer, ästhetischer oder kennzeichengesetzlicher Natur, die dem Inhaber ein exklusives Nutzungs- und Verfügungsrecht über sein Werk vermitteln. Die Schweizerische Gesetzgebung unterscheidet verschiedene Arten solcher Schöpfungen und regelt diese in den unterschiedlichen Gesetzesbeständen des Patentrechts, des Urheberrechts, des Designrechts, des Kennzeichenrechts, des Firmenrechts und des Markenrechts. Im Bereich der Cloud dürften vorwiegend die nachfolgend beschriebenen rechtlichen Regelungen zur Anwendung kommen.

3.4.1 Urheberrecht

Grundregel - Die Artikel 2 bis 5 des Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte URG umschreiben diejenigen Werke, welche durch das Urheberrecht geschützt werden. Im Grundsatz gilt, dass „sämtliche Schöpfungen der Literatur und Kunst mit individuellem Charakter“ in den Anwendungsbereich des URG fallen. Nach Artikel 2 Abs. 2 URG sind zudem Computerprogramme explizit auch als Werke im Sinne des Urheberrechts zu qualifizieren. Allerdings schützt das Urheberrecht nur die konkrete Implementierung (d.h. den Programm Code), nicht aber ein Verfahren, das einem Computerprogramm zugrunde liegt. Ohne gegen das Urheberrecht zu verstossen, ist es also möglich, dieselbe Idee in einem anderen Computerprogramm umzusetzen oder eine Software mit einer gewissen Funktionalität nachzuprogrammieren. Geniesst ein Werk urheberrechtlichen Schutz, so stehen den Rechteinhabern verschiedene ausschliessliche Nutzungsrechte bis 70 Jahre respektive 50 Jahre bei Computersoftware nach dem Tod des Urhebers zur Verfügung ¹⁷.

Merkbox

das gilt es zu beachten

Bei den beurteilten, in der Cloud abgelegten Daten muss es sich um urheberrechtlich geschützte Werke handeln. Ansonsten sind die Merkboxen in diesem Abschnitt für die Auslagerung von Daten in die Cloud **nicht** zwingend zu berücksichtigen.

Im Zusammenhang mit dem Cloud Computing sind insbesondere das Vervielfältigungsrecht und das Recht auf Zugänglichmachung gemäss Artikel 10 Abs. 2 URG relevant. Diese beiden Schutzrechte erlauben es dem Urheber von Computersoftware, im Rahmen einer lizenzierten Vereinbarung einer Drittperson gewisse Nutzungsrechte für das Computerprogramm und entsprechende Kopien zu veräußern. Den meisten Informatikerinnen und Informatikern dürfte nun auch bereits die Problematik bei der Auslagerung solcher lizenziertener Software respektive bei der Nutzung von entsprechenden Angeboten des Cloud Providers im Sinne von Software as a Service ersichtlich sein. Aufgrund des Wildwuchses im Bereich von Softwarelizenzen lässt sich an dieser Stelle jedoch keine allgemein gültige

¹⁷ Weitere Informationen in verständlicher Form finden sich auf der Seite des Eidgenössischen Instituts für Geistiges Eigentum IGE unter <https://www.ige.ch/de.html>.

Beurteilung der Zulässigkeit der Abspeicherung oder zur Verfügung Stellung in der Cloud vornehmen. Es ist vielmehr zu prüfen, ob eine konkrete Lizenzvereinbarung die Softwarenutzung beispielsweise an bestimmte Lokalitäten oder gar Hardware bindet.

Merkbox

das gilt es zu beachten

Im Rahmen des Going to Cloud ist zwingend zu prüfen, ob und unter welchen Voraussetzungen geschäftlich genutzte Software oder sonstige urheberrechtlich geschützten Werke in der Cloud abgelegt und genutzt werden dürfen.

Ausnahmen - Die wichtigsten beiden Ausnahmen zum Vervielfältigungsrecht und für die Nutzung von urheberrechtlich geschützten Werken in der Cloud sind der geschäftliche Eigengebrauch nach Artikel 19 URG und die vorübergehende Speicherung nach Artikel 24a URG. Die erste Ausnahme lässt das Erstellen von Kopien zum Eigengebrauch zu - so ist es nach herrschender Lehre und Rechtsprechung¹⁸ beispielsweise zulässig, in einem Firmen internen Wiki urheberrechtlich geschützte Werke zu speichern und zu verbreiten. Allerdings fällt die Nutzung Software nach Artikel 19 Abs. 4 URG explizit **nicht** unter diese Bestimmung. Die zweite Ausnahme betrifft die beispielsweise bei der Netzwerkübertragung technisch notwendige Vervielfältigung von urheberrechtlich geschützten Werken. Treffen die vier Bedingungen von Artikel 24a kumulativ zu¹⁹, so ist die Vervielfältigung selbst von Software zulässig.

3.4.2 Markenrecht

Grundregel - Obwohl im Zusammenhang mit dem Thema des Cloud Computing dem Markenrecht zumindest im Grundsatz wohl keine allzu grosse zusätzliche Bedeutung zukommt, sei es der Vollständigkeit halber an dieser Stelle noch kurz erläutert. Eine Marke im rechtlichen Sinn umfasst den gewerblichen Schutz eines Kennzeichens, mit dem ein Unternehmen seine Waren oder Dienstleistungen von solchen anderer Unternehmen unterscheidet. Grundsätzlich können alle grafisch darstellbaren Zeichen Marken im Sinne des Gesetzes sein. Um in den Genuss des Markenschutzes zu kommen, muss das Kennzeichen in einem sog. Markenregister eingetragen werden. In der Schweiz eingetragene Marken können über das elektronische Register [Swissreg](#) und international eingetragene Marken über die [Madrid Express Datenbank](#) abgefragt werden. In der Schweiz verleiht der Markenschutz dem Inhaber das ausschliessliche Recht, seine Marke zur Kennzeichnung von Waren oder Dienstleistungen zu gebrauchen. Der Markeninhaber kann somit anderen verbieten, ein identisches oder ähnliches Zeichen für gleiche oder gleichartige Waren oder Dienstleistungen zu verwenden. Dieses Recht kann weitergegeben werden, beispielsweise durch Lizenzen oder durch Verkauf. Selbstverständlich sind solche Markenverletzungen unabhängig von der Ablage der Daten in der Cloud zu vermeiden.

¹⁸vgl. dazu BGE 133 III 473

¹⁹Diese Voraussetzungen sind namentlich Vervielfältigungen, die **(a)** flüchtig sind, **(b)** integraler und wesentlicher Teil eines technischen Verfahrens darstellen, **(c)** ausschliesslich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder einer rechtmässigen Nutzung dienen und **(d)** keine eigenständige wirtschaftliche Bedeutung haben.

Ausnahmen - Einziger Spezialfall mit Berührungs punkt zum Cloud Computing stellt die wohl doch eher selten auftretende Konstellation dar, in welcher sich ein Unternehmen für einen ausländischen Cloud Provider entscheidet und aufgrund einer ungenügenden Zugriffskontrolle (oder aber auch bewusst) eine zwar in der Schweiz auf ihren Namen eingetragene, im Ausland jedoch durch ein anderes Unternehmen geschützte Marke für ihre Produkte weiterverwendet.

3.4.3 Patentrecht

Grundregel - Patente dienen dem Schutz technischer Erfindungen, also neuen (d.h. eindeutig weiter als der aktuelle Stand der Technik) und nicht naheliegenden Lösungen technischer Problemstellungen. Als technische Erfindungen kommen sowohl Produkte als auch Verfahren in Frage, die gewerblich nutzbar sein müssen. Somit sind Computerprogramme als solche vom Patentschutz grundsätzlich ausgeschlossen, sofern es sich nicht um eine Computer implementierte Erfindung handelt. Eine Computer implementierte Erfindung (CIE) ist eine Erfindung, zu deren Ausführung ein Computer, ein Computer netz oder eine sonstige programmierbare Vorrichtung eingesetzt wird und die mindestens ein Merkmal aufweist, das ganz oder teilweise mit einem Computerprogramm realisiert wird. Sie weist einen technischen Charakter auf und ist somit im Prinzip patentierbar. Sofern eine Erfindung patentrechtlich geschützt werden kann, ist diese ebenfalls in ein entsprechendes Register einzutragen. Eingetragenen Patente geniessen ein ausschliessliches Recht zur gewerblichen Nutzung durch den Rechteinhaber. Auch in diesem Fall ergeben sich abgesehen von den allgemein zu vermeidenden Patentverletzungen für das Cloud Computing keine offensichtlichen Besonderheiten.

Ausnahmen - Auch im Bereich des Patentrechts lässt sich im Zusammenhang mit dem Cloud Computing nur ein Spezialfall mit einer allerdings wohl geringen Bedeutung für Cloud Kunden finden. Verletzt der Cloud Provider durch die Verwendung einer bestimmten, patentrechtlich geschützten Cloud Technologie (d.h. eine Computer implementierte Erfindung) das Exklusivrecht eines anderen Anbieters, so kann der Cloud Kunde als Teilnehmer einer mittelbaren Patentverletzung qualifiziert werden - und dies einzig gestützt auf seine Nutzung der Cloud des fehlbaren Cloud Providers ²⁰. Allerdings kann dieses Risiko durch eine vertragliche Regelung nicht wegbedungen werden. Eine gewisse Sicherheit bietet diesbezüglich nur eine möglichst umfassende Risikoabklärung im Rahmen des Evaluationsprozesses zum Cloud Anbieter.

3.4.4 Blick über die Grenze

Nach den Änderungen im Bereich des Datenschutzes treibt die Europäische Union nun auch rechtliche Anpassungen mit Blick auf das Immaterialgüterrecht voran. So steht in den kommenden Monaten und Jahren mit der Reform des Urheberrechtes eine weitere grosse Veränderung der rechtlichen Situation insbesondere für die Nutzung des Internets an. Kontrovers werden dabei insbesondere der Artikel 11 bezüglich des Leistungsschutzrecht für Presseverleger und der Artikel 13 zur Haftbarkeit

²⁰ https://www.nkf.ch/wAssets-nkf2/docs/publikationen/clara_ann_gordon/Patentschutz-und-zukuenftige-Trends.pdf, letz-
mals besucht: 18. Mai 2019

von Plattformen diskutiert ²¹.

Entsprechend Artikel 11 des neuen Urheberrechtes dürften nach dessen Inkrafttreten Online Zitate nur noch einzelne Worte oder kurze Texte umfassen, sofern dem Urheber keine entsprechenden Lizenzgebühren bezahlt worden sind. So sollen insbesondere die grossen Suchmaschinen, Social Media und Video Plattformen gezwungen werden, für die Präsentation der Ergebnisse entsprechende Abgaben zu bezahlen. Artikel 13 geht insofern noch einen Schritt weiter, als dass die betroffenen Plattformen für sämtliche Urheberrechtsverletzungen (insbesondere nach Artikel 11 und auch solche ihrer User) haftbar gemacht werden.

Nach Ansicht des Autors dieses Skripts sind die obgenannten Bestimmungen aus verschiedensten Gründen enorm problematisch und mit Bezug auf eine allfällige Umsetzung im Schweizerischen Recht wohl bis zu einem bestimmten Grad auch unzulässig. Dazu einige juristische und wirtschaftliche Überlegungen: **(a)** Artikel 11 würde beispielsweise die Suchmaschinen dazu zwingen, entweder entsprechende Lizenzen zu erwerben oder Suchergebnisse komplett zu entfernen. Denn eine Suchmaschine mit Suchergebnissen ohne inhaltliche Beschreibung entbehrt jeglichem Sinn. Werden die Suchergebnisse von der Suchmaschine komplett entfernt, so würde dies insbesondere für die Medienberichterstattung wohl einige Verluste bedeuten - bezahlen die Suchmaschinenanbieter jedoch die entsprechenden Lizenzgebühren, dürften diese Kosten mit an Sicherheit grenzender Wahrscheinlichkeit dem Nutzer überbunden werden. In diesem Zusammenhang ebenfalls schwierig dürfte das konkrete Abrechnen der Gebühren sein. **(b)** Noch problematischer scheint der Artikel 13, der indirekt eine technische Lösung durch die Plattform im Sinne eines Upload Filters vorschreiben würde. Solchen technischen Lösungen ist jedoch inhärent, dass auch Beiträge, welche tatsächlich keine Urheberrechtsverletzung beinhalten, als problematisch qualifiziert und nicht publiziert werden könnten (e.g. Satire, Repliken auf Artikel, u.v.m.). Dies würde jedoch einer Zensur gleichkommen und somit eindeutig verschiedensten rechtsstaatlichen Grundpfeilern (i.e. Meinungs-, Informations- und Pressefreiheit) widersprechen.

3.4.5 Zusammenfassung

Grundprinzip - Im Bereich der Immaterialgüterrechte sind im Zusammenhang mit dem Thema Cloud insbesondere die dem Urheberrecht entspringenden Lizenzrechte für die Nutzung und Verteilung geschützter Software zu berücksichtigen. In einigen speziellen Konstellationen können auch marken- und patentrechtliche Abklärungen nötig sein, die jedoch durch entsprechende Spezialistinnen und Spezialisten erkannt und geprüft werden müssen.

Fallbeispiel - Der nachfolgende Fall soll nochmals den Unterschied zwischen Software und anderen urheberrechtlich geschützten Werken verdeutlichen.

²¹<https://www.zeit.de/digital/internet/2019-02/eu-urheberrecht-leistungsschutzrecht-uploadfilter-europaeisches-parlament>,
<https://www.e-recht24.de/artikel/urheberrecht/10954-eu-leistungsschutzrecht-gefahr-oder-rettung.html> u.v.m., letztmals besucht: 18. Mai 2019

Sachverhalt: Ein Schweizer Unternehmen, welches an verschiedenen Standorten Aluminiumteile für die Raumfahrt und Autoindustrie herstellt, möchte ein für sämtliche Standorte zugängliches, auf einer Cloud Plattform zur Verfügung gestelltes Wiki erstellen. Neben Reparaturanleitungen, Prozessbeschrieben und Konfigurationsanweisungen für ihre CAD Maschinen soll das Wiki auch eine Download Plattform für entsprechende CAD Software bereit stellen.

Fragestellung: Darf eine solche Plattform überhaupt erstellt werden? Und falls ja, darf diese auch über einen Cloud Anbieter zur Verfügung gestellt werden?

Beurteilung: Während das Bereitstellen der wohl urheberrechtlich geschützten Werke über die Wiki Plattform aufgrund der Bestimmung zum geschäftlichen Eigengebrauch nach Artikel 19 URG unter der Voraussetzung, dass der Cloud Provider eine Zugangskontrolle gewährleisten kann, grundsätzlich zulässig ist, kann die Beurteilung der Zulässigkeit der Download Plattform erst anhand der konkreten Lizenzverträge beurteilt werden. Selbst bei Vorliegen einer konkreten Lizenz ist deren Beurteilung nicht immer einfach und die Gerichte unterschiedlicher Länder können bei der gleichen Lizenz auch zu unterschiedlichen Ergebnissen kommen. Dazu zwei Beispiele aus der Praxis - eines zum Thema der Hardwarebeschränkung und ein anderes aus dem Bereich der Einsatzbeschränkung. **(a)** Die Apple EULA zum Betriebssystem Mac OS X ²² enthält in Abschnitt I. eine Nutzungsbeschränkung, wonach die Software nur auf Apple Hardware installiert und ausgeführt werden darf. Eine diesbezügliche juristische Abklärung der rechtlichen Lage vor einigen Jahren kam jedoch zum Schluss, dass diese Nutzungseinschränkung in der Schweiz nach damaligem Recht insbesondere aufgrund des Bundesgesetzes über den unlauteren Wettbewerb UWG und der Qualifikation der Apple EULA als AGB nicht zulässig und deshalb ohne Wirkung sei. Gleichermaßen dürfte für die umliegenden europäischen Ländern gelten. Demgegenüber wird diese Bestimmung in den USA als zulässig angesehen und entsprechende Urteile auch gerichtlich vollzogen. **(b)** Ende 2017 untersagte NVIDIA in ihrer neusten EULA zu den Geforce Treibern den Endkunden, die Software in Rechenzentren einzusetzen. Dies dürfte insbesondere für Cloud Provider mit Deep Learning Diensten grosse Auswirkungen haben, da NVIDIA Geforce- und Titan Grafikkarten nicht mehr eingesetzt werden dürfen ²³. Inwiefern eine solche Einschränkung der Nutzung nach Schweizer Recht zulässig ist, bleibt den Gerichten überlassen.

²²<https://www.apple.com/legal/sla>, letztmals besucht: 18. Mai 2019

²³<https://www.golem.de/news/treiber-eula-nvidia-untersagt-deep-learning-auf-geforces-1712-131848.html>, letztmals besucht: 18. Mai 2019

3.5 Allgemeines Vertragsrecht

Grundregel - Die Verträge zwischen einem Cloud Provider und einem Kunden können sehr unterschiedlich gestaltet sein, weshalb eine abstrakte Qualifizierung - d.h. eine allgemeine Einordnung in die Vertragswelt des Schweizerischen Obligationenrechts - nicht möglich ist. Je nach Ausgestaltung kann es sich um einen Innominatvertrag mit u.a. mietvertraglichen, auftragsrechtlichen oder auch werkvertragsähnlichen Komponenten handeln. Die herrschende Lehre scheint sich jedoch einig zu sein, dass es dem Cloud Anbieter grundsätzlich erlaubt ist, ein Subunternehmen (i.c. ein Sub-Provider) beizuziehen. Aufgrund der bisherigen Darstellung der rechtlichen Situation in der Cloud muss der Cloud Anbieter jedoch zwingend dazu verpflichtet werden, sämtliche vereinbarte Pflichten zwischen ihm und dem Kunden auch auf seinen Subunternehmer zu überbinden.

Merkbox

das gilt es zu beachten

Der Cloud Anbieter ist vertraglich zu verpflichten, sämtliche Pflichten gegenüber dem Kunden auch auf Subunternehmen zu überbinden, mit der Pflicht zur Weiterüberbindung.

Ausnahme - Die wichtigste Ausnahme bezüglich Subunternehmen des Providers betrifft die Bearbeitung von Personendaten. Aufgrund der strengereren Vorschriften mit Blick auf das Datenschutzniveau eines Landes sind die vertraglichen Regelungen zwischen dem Cloud Anbieter und den Kunden diesbezüglich noch strenger zu gestalten. Das EDÖB rät in einem solchen Fall sogar dazu, dem Cloud Anbieter vertraglich die Weitergabe der Datenbearbeitung an Drittunternehmen zu verbieten ²⁴.

Merkbox

das gilt es zu beachten

Im Falle von Personendaten im Sinne des Datenschutzgesetzes sind mit dem Cloud Anbieter vertragliche Datenschutzgarantien abzuschliessen, ebenfalls mit der Pflicht zur Weiterüberbindung.

Fallbeispiel: Das nachfolgende Beispiel soll den etwas speziellen Ausdruck „mit der Pflicht zur Weiterüberbindung“ illustrieren.

Sachverhalt: Ein Schweizer Bekleidungsunternehmen möchte aufgrund seines immensen Wachstums in den letzten Jahren seine gesamten IT Ressourcen an ein Cloud Provider auslagern. Aufgrund der ebenfalls betroffenen Kundendaten entschliesst sich das

²⁴https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/internet_und_computer/cloud-computing/erlauterungen-zu-cloud-computing.html, letztmals besucht: 18. Mai 2019. Ob der Cloud Anbieter eine solch strenge Verpflichtung in der Praxis eingehen wird, erscheint mehr als nur fraglich, da ihm dadurch jegliche Flexibilität bei der Bewältigung von Arbeitslastspitzen genommen würde.

Unternehmen, einen entsprechenden Vertrag mit einem europäischen Cloud Anbieter abzuschliessen. Der Vertrag enthält unter anderem eine vertragliche Datenschutzgarantie, welche vom Cloud Anbieter auch auf seine Subunternehmen zu überbinden ist.

Fragestellung: Ist eine solche Bestimmung zum Schutz der Personendaten ausreichend?

Beurteilung: Obwohl der Ansatz grundsätzlich gut ist, fehlt in der Bestimmung die - um es in der Sprache der Informatik zu formulieren - rekursive Pflicht zur Weiterüberbindung. Mit anderen Worten könnte ein Subunternehmen mit der aktuellen Vertragsgestaltung ein weiteres Sub(sub)unternehmen (bspw. in den USA) beauftragen, ohne dass diesem die vertraglichen Datenschutzgarantien aufgebrummt werden müssen. Selbstverständlich kann der Cloud Kunde gegenüber seinem direkten Vertragspartner bei Nichteinhaltung der Datenschutzgarantien Regress nehmen - es ist jedoch als Cloud Kunde wichtig, zu verstehen, dass letztlich dennoch er als Auftraggeber gegenüber den betroffenen Personen für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist und eine Pflicht zur Weiterüberbindung der Datenschutzgarantien und Absicherung durch eine Konventionalstrafe zumindest die Aufmerksamkeit des Cloud Anbieters und seiner Subunternehmen fördert.

3.6 Schuldbetreibungs- und Konkursrecht

Grundregel - Im Gegensatz zu den meisten anderen Rechtsgebieten, ist eine Gerichtsstandsvereinbarung und eine vertragliche Festlegung des anwendbaren Rechts nicht möglich²⁵. Somit stellt sich als erstes die Frage nach dem anwendbaren Insolvenzrecht. Grundsätzlich bestimmt sich dieses nach dem Sitz des Cloud Anbieters, wobei nochmals darauf hingewiesen sei, dass im Internationalen Privatrecht gerade bei speziellen organisatorischen Strukturen (bspw. verschiedene Serverstandorte, verschiedene Tochtergesellschaften) auch andere Beurteilungen in Betracht fallen können. Nachfolgend soll nur der Konkurs nach dem Schweizerischen Schuldbetreibungs- und Konkursrecht SchKG näher betrachtet werden.

In einem Konkurs nach Schweizer Recht steht dem Gläubiger grundsätzlich ein sog. Aussonderungsanspruch für bewegliche Sachen in seinem Eigentum zu, welche sich im Besitz des Konkursiten befinden. Dieser Anspruch ermöglicht es dem Gläubiger, diese Sachen vor dem Konkurs zu retten. Nach herrschender Lehre und der konstanten Rechtsprechung des Bundesgerichts besteht dieser Aussonderungsanspruch jedoch nur für bewegliche Sachen und somit **nicht** für elektronische Daten, die der Gläubiger (i.c. der Cloud Kunde) beim sich im Konkurs befindlichen Cloud Anbieter gespeichert hat. Somit stellt sich nur noch die Frage, ob das Konkursamt die Daten des Cloud Kunden auch verwerten (d.h. an Dritte verkaufen) kann. Während ein Teil der Lehre und auch der kantonalen Konkursämter verneint, betrachten andere (u.a. der Kanton Zürich) die Verwertung der Daten grundsätzlich als zulässig. Eine einheitliche Regelung findet sich jedoch nicht, weshalb in einem Vertrag zwischen dem Cloud Anbieter und dem Kunden zwingend die nachfolgenden Bestimmungen festgehalten werden müssen.

Merkbox

das gilt es zu beachten

Vertraglich muss zwingend festgehalten werden, dass sämtliche gespeicherten Daten vertraulich sind und der Cloud Anbieter auf ein allfälliges Retentionsrecht bezüglich der verwertbaren Daten des Cloud Kunden verzichtet. Zudem ist ein Verwertungsverbot der Daten und ein Verfahren für die Löschung derjenigen festzulegen.

Ausnahmen - Selbst durch die vorgenannten Vertragsbestimmungen lässt sich nicht jegliches Restrisiko vermeiden. So beurteilt der Kanton Zürich die Verwertbarkeit der Kundendaten des in Konkurs geratenen Cloud Anbieters nicht nach vertraglichen Aspekten, sondern im Rahmen einer Interessenabwägung zwischen der Vertraulichkeit und der Datenverwertung²⁶. Demgegenüber anerkennt der Gesetzgeber in Luxemburg ein Aussonderungsrecht für eindeutig zuordenbaren Daten im Konkurs²⁷.

²⁵vgl. dazu auch Kapitel 2

²⁶vgl. dazu das Positionspapier des Datenschutzbeauftragten ZH im Anhang C

²⁷Details dazu finden sich in der Masterthesis *Cloud Computing – Eine rechtliche Gewitterwolke?* von Eric T. Neuenschwander ab Seite 29 (inkl. Fussnoten).

Fallbeispiel - Aufgrund des Fehlens von Gerichtsurteilen soll anstelle eines Fallbeispiels aufgezeigt werden, dass sich der Gesetzgeber (i.c. die Politik) der Problematik von Cloud Daten in der Konkursmasse durchaus bewusst ist. So hat Nationalrat Marcel Dobler von der FDP vor einem Jahr eine parlamentarische Initiative angestossen, welche die Herausgabe von Kundendaten im Konkursfall rechtlich verbindlich regeln soll²⁸. Nach der einstimmigen Unterstützung der Initiative durch die Kommission für Rechtsfragen des Nationalrates gab am 15. April 2019 auch die Kommission des Ständerates ihre Zustimmung. Aufgrund des in der Schweiz etwas trügen Gesetzgebungsprozesses dürfte es jedoch noch einige Jahre dauern, bis die entsprechend entworfenen Gesetze tatsächlich in Kraft treten werden. Der aktuelle Stand der Initiative kann auf der offiziellen Bundesseite eingesehen werden²⁹.



The screenshot shows the FDP website header with links for Kontakt, Medien, Shop, DE | FR | IT, and a search bar. Below the header, there's a navigation menu with AKTUELL, PARTEI, PERSONEN, POSITIONEN, and KAMPAGEN. The main content area features a post from Marcel Dobler dated 3. May 2018. The post title is "Cloud-Speicher: Die Datenherausgabe im Konkurs muss geregelt werden". It includes a short text about data storage and a sidebar with Marcel Dobler's profile picture, name, and political affiliation.

Abbildung 3.4: FDP Homepage zur parlamentarischen Initiative von NR Marcel Dobler

²⁸Details dazu finden sich auf der Homepage der FDP unter <https://www.fdp.ch/aktuell/.../> und im Artikel der Netwoche unter <http://www.netwoche.ch/news/2018-05-08/.../>.

²⁹<https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170410>, letztmals besucht: 18. Mai 2019

3.7 Haftpflichtrecht

Grundregel - Die allgemeinen Grundlagen der vertraglichen Haftung zwischen Cloud Provider und Cloud Kunde finden sich in den Artikel 97 ff. des Obligationenrechts (OR). Grundsätzlich darf und wird der Cloud Provider die allgemeine vertragliche Haftung wegbedingen. Zudem zeigt sich aufgrund der bereits erläuterten zu berücksichtigenden Gesetzesartikel, dass der Einhaltung des Service Level Agreement eine viel grössere Bedeutung zukommt, als derjenigen der allgemeinen Haftung. Bezuglich der Absicherung, Durchsetzbarkeit (i.e. Konventionalstrafen) und Schadensberechnung wird auf die Vorlesung zum entsprechenden Thema verwiesen. Allerdings ist festzuhalten, dass im Hauptvertrag zwingend Bezug auf das SLA genommen werden muss.

Merkbox

das gilt es zu beachten

Der Hauptvertrag muss das Service Level Agreement inklusive dessen Durchsetzbarkeit etc. zwingend als intergrierenden Vertragsbestandteil festlegen.

Ausnahme - In der Schweizerischen Gesetzgebung kann die Haftung nicht vollständig wegbedungen werden. Nach Artikel 100 Abs. 1 OR sind Freizeichnungsklauseln nichtig, wenn sie die Haftung für rechtswidrige Absicht oder grobe Fahrlässigkeit ausschliessen. Übersetzt bedeutet dies grundsätzlich, dass die Haftung bei vorsätzlichen Handlungen (bspw. dem absichtlichen Löschen von Daten des Kunden) oder grobfahrlässigen Tätigkeiten (bspw. Stromstecker des Servers ziehen) durch den Cloud Provider nicht ausgeschlossen werden kann. Eine allfällige solche Bestimmung im Vertrag gilt als nichtig, d.h. sie wird nach Artikel 20 Abs. 2 des OR grundsätzlich einfach als „wie nicht im Vertrag geregelt“ betrachtet.

Merkbox

das gilt es zu beachten

Der Vertrag darf die allgemeine Haftung nicht vollständig wegbedingen - ansonsten ist zumindest die jeweilige Bestimmung nichtig.

Fallbeispiel - Leider konnte kein einziger gerichtlicher Entscheid gefunden werden, der die Abgrenzung zwischen Service Level Agreement und der allgemeinen Haftung aufzeigen kann und von welchem ein Fallbeispiel hätte abgeleitet werden können. Es sei jedoch nochmals darauf hingewiesen, dass im Rahmen der SLA messbare Leistungskriterien und entsprechende (Konventional-)Strafen betragsmäßig definiert werden müssen.

3.8 Branchenspezifische Regelwerke

Zum Schluss sind noch einige Erläuterungen zu speziell geregelten Berufsgattungen nötig. All diesen Berufsgattungen gemeinsam ist eine explizite Regelung in verschiedenen Spezialgesetzen sowie die gesetzliche Verankerung eines sog. Berufsgeheimnisses. Diesen Spezialregelungen gilt es bei einem Gang in die Cloud besondere Beachtung zu schenken.

Merkbox

das gilt es zu beachten

Untersteht ein Unternehmen branchenspezifischen Gesetzen oder sieht das Gesetz für den entsprechenden Unternehmertyp ein Berufsgeheimnis vor, sind einerseits die Spezialgesetze, allfällige Erlassen von Aufsichtsbehörden und interne Richtlinien zwingend von einem Juristen oder Anwalt zu prüfen und daraus abgeleitete Richtlinien zu beachten. Andererseits gilt es, die Zertifizierungen des Cloud Providers zu berücksichtigen.

3.8.1 Banken und Versicherungen

Für diese Branchen gelten insbesondere das Bundesgesetz über die Banken und Sparkassen (Bankengesetz) und das Bundesgesetz über den Versicherungsvertrag (VVG). Sämtliche Unternehmen dieser Branchen unterstehen der Eidgenössischen Finanzmarktaufsicht FINMA, welche den gesetzlichen Auftrag hat, die entsprechenden Unternehmen zu bewilligen, zu überwachen und das Aufsichtsrecht gesetzeskonform durchzusetzen. Zudem kann die FINMA - sofern ein Gesetz dies vorsieht - auch zusätzliche Massnahmen in Form von Verordnungen und Weisungen erlassen.

Im Bereich des Cloud Computing ist insbesondere das per 1. April 2018 in Kraft getretene Rundschreiben 2018/3 betreffend Outsourcing bei Banken und Versicherungen von Bedeutung, welches unter anderem eine verschärzte Kontroll- und Aufsichtspflicht und eine Inventarisierung der ausgelagerten Funktionen vorschreibt (vgl. Anhang B). Auf die in den Medien viel diskutierte Meldepflicht für die Auslagerung von Client Identifying Data (CID, d.h. Name, Vorname, Telefonnummern, Post- und E-Mail-Adressen oder Passnummer³⁰) ins Ausland wurde jedoch trotz Bankengeheimnis nach Artikel 47 des Bankengesetz verzichtet³¹.

Für diese Branchen besonders interessant sind Cloud Provider, welche die ISO 27001 Zertifizierung besitzen und die FINMA Richtlinien explizit erfüllen. Ein Beispiel für einen entsprechend ausgerüsteten Cloud Provider ist der Anbieter APPUiO, welcher im Rahmen der Vorlesung Cloud Solutions im Jahr 2017 näher betrachtet wurde.

³⁰vgl. dazu auch den Abschnitt 3.2.1 zum Thema Personendaten und Datenschutz

³¹Artikel Inside IT vom 6. Dezember 2017, <https://www.inside-it.ch/articles/49607>, letztmals besucht: 18. Mai 2019

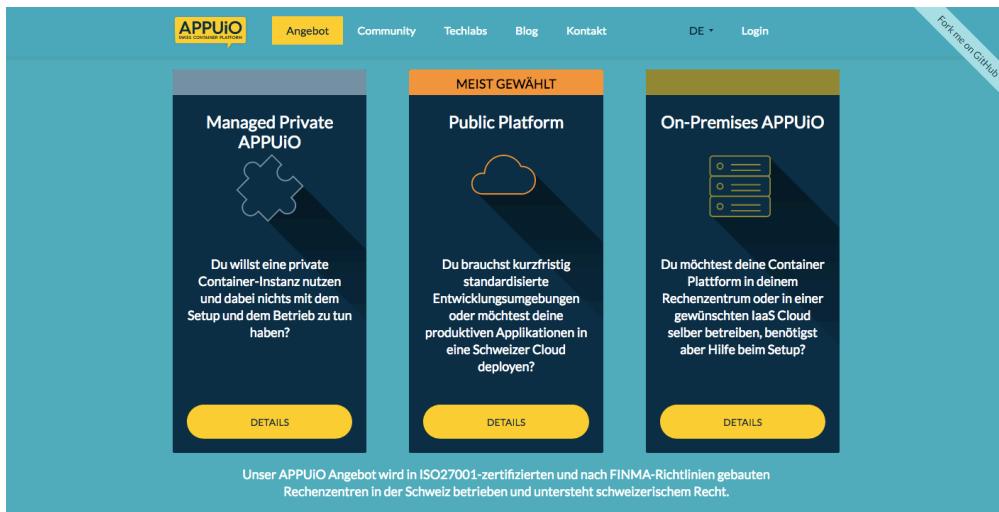


Abbildung 3.5: APPUiO Cloud ISO Zertifizierung und FINMA Richtlinien

3.8.2 Anwaltstätigkeit

In einer vergleichbaren Situation wie die Banken und Versicherungen befinden sich Anwaltskanzleien. Sie unterstehen insbesondere dem Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (BGFA) und unterliegen nach Artikel 13 BGFA einem sowohl die Anwältinnen und Anwälte als auch deren Hilfspersonen umfassenden Berufsgeheimnis. Im Gegensatz zu den Banken und Versicherungen wird die Aufsicht jedoch nicht auf Bundesebene sondern durch kantonale Aufsichtsbehörden vollzogen. Wichtige Richtlinien und Hinweise zum Thema Cloud Computing im Anwaltsbereich finden sich zudem auf der Homepage des Schweizerischen Anwaltsverbandes SAV³².

3.8.3 Weitere Branchen

Ebenfalls ähnliche Strukturen und Regelungen gelten für die privatrechtlichen Berufsgattungen der Ärztinnen und Ärzte, Psychologinnen und Psychologen oder Spitäler. Der Vollständigkeit halber sei an dieser Stelle nochmals auf öffentlichrechtliche Organisationen (i.e. Gerichte, Amtsträger, Steuerämter u.v.m.) hingewiesen, bei denen die strengeren öffentlichrechtlichen Regelungen oftmals einem Amtsgeheimnis entspringen.

³²bspw. https://www.sav-fsa.ch/...titel_umzug-einer-kanzlei-in-die-cloud, letztmals besucht: 18. Mai 2019

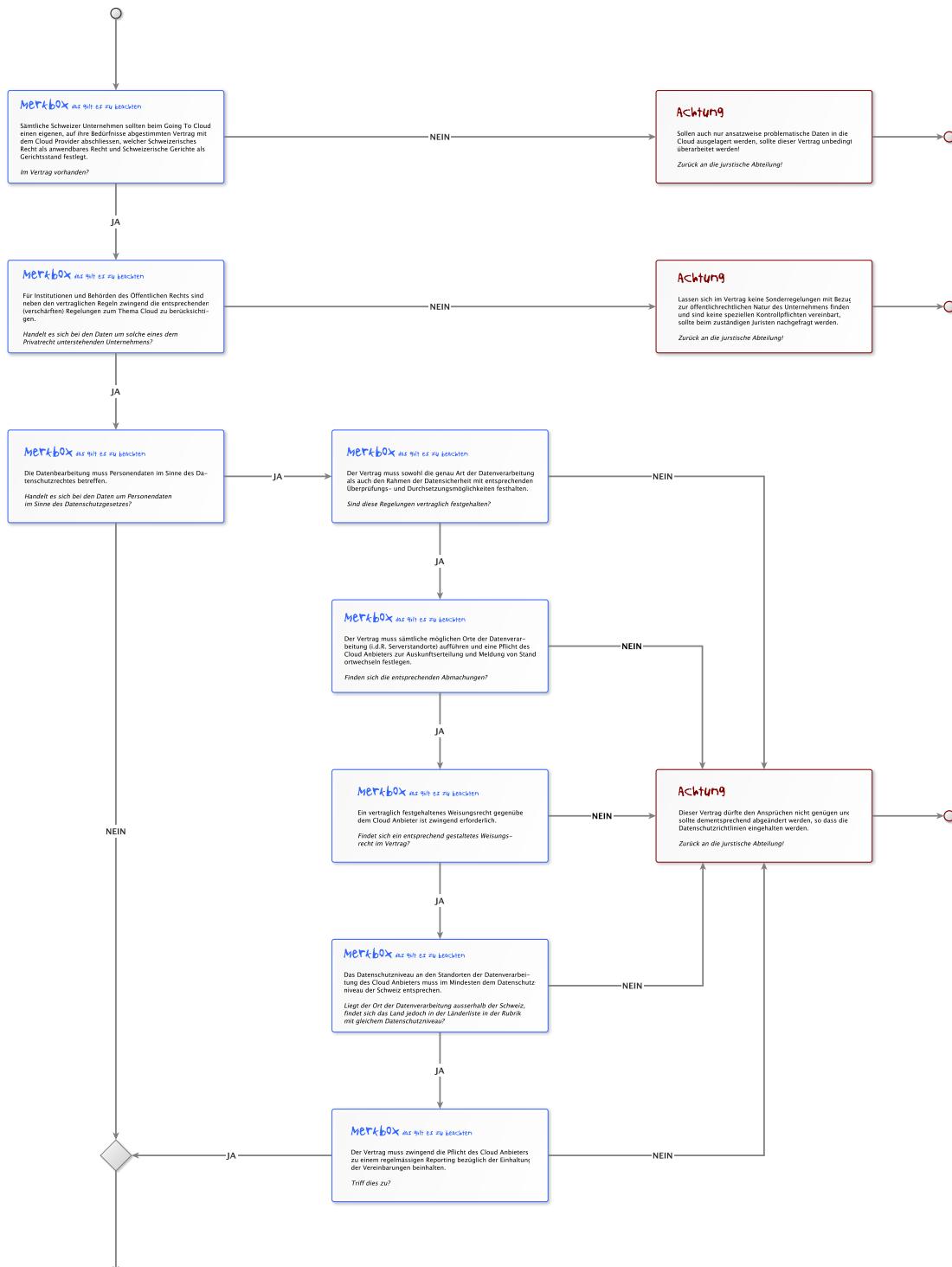
4 Fazit

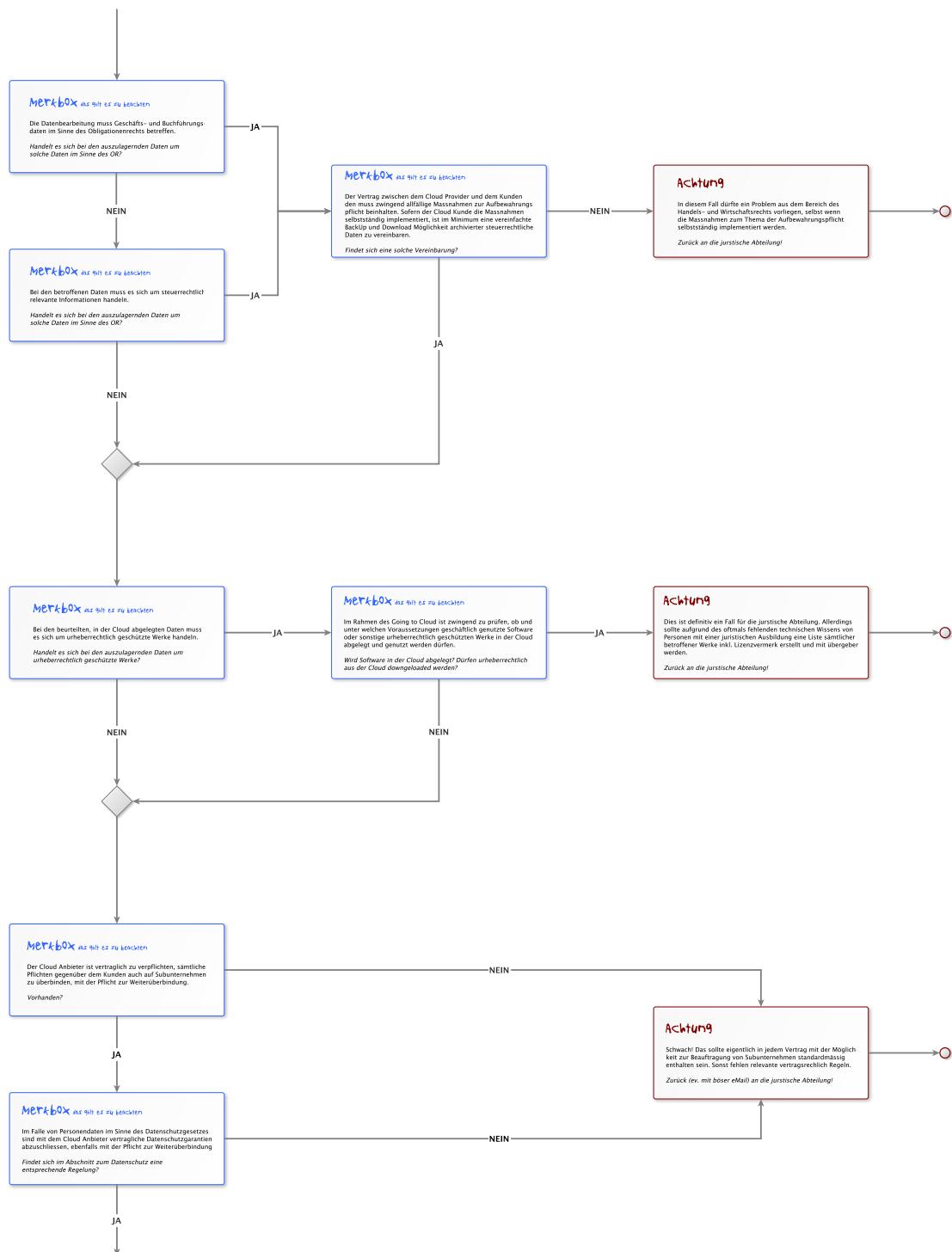
Die vorangegangenen Kapitel dürften viele Leserinnen und Leser davor zurückschrecken lassen, ihre Daten in die Cloud auszulagern. Meines Erachtens ist Zurückhaltung oder gar Angst bezüglich der Auslagerung von Daten in die Cloud fehl am Platz - einerseits überwiegen in vielen Fällen die wirtschaftlichen Vorteile und andererseits lässt sich das rechtliche Risiko eines Going to Cloud durch das Berücksichtigen der erarbeiteten Merkboxen (zusammengetragen in nachfolgendem Flussdiagramm) und einen entsprechend abgesicherten Vertrag mit dem Cloud Provider stark minimieren. Zudem dürfen rund 95% der in Frage stehenden Daten eines nicht unter Spezialregelungen fallenden Unternehmens erst gar nicht in den Geltungsbereich einer der vorgenannten Gesetze fallen. Für die übrigen 5% der Daten ist sodann aufgrund einer umfassender Risikoabschätzungen zu entscheiden, ob eine Separation und ein Verbleib der Daten beim Kunden oder eine Ablage der Daten in der Cloud mit entsprechend ausgearbeitetem Vertrag die sinnvollere Lösung darstellt.

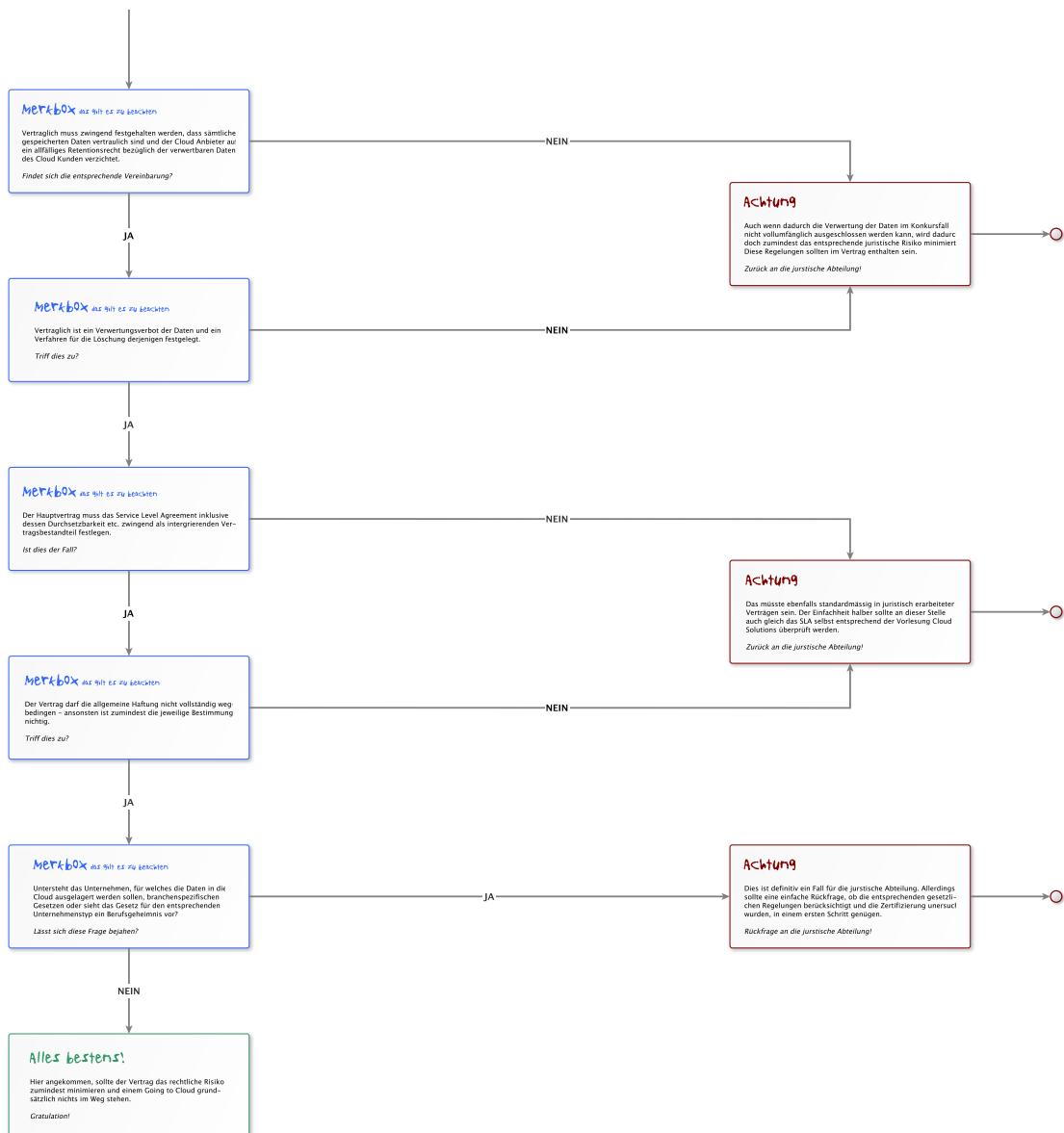
Trotzdem möchte ich an dieser Stelle nochmals die beiden meiner Ansicht nach heikelsten Themen ansprechen:

- Aus juristischer Sicht die grösste Problematik dürfte im Bereich des Konkursrechtes und der Verwertung von Kundendaten eines Cloud Providers im Rahmen des Konkurses liegen. Diese unbefriedigende Situation scheint der Gesetzgeber respektive die Politik jedoch erkannt zu haben. Eine klare diesbezügliche Regelung ist meiner Meinung nach zwingend und so zeitnah wie möglich nötig.
- Das nach zweite problematische Themengebiet der Verschlüsselung entspringt nicht alleine den juristischen Vorschriften, sondern vielmehr einem fehlenden technischen Verständnis des Gesetzgebers respektive einer fehlenden Kommunikation zwischen der Informatik und der juristischen Welt. Nahezu sämtliche juristischen Probleme könnten durch eine Verschlüsselung der Daten in der Cloud und Verbleib der privaten Schlüssel beim Cloud Kunden ausgemerzt werden. Viele juristische Abhandlungen nehmen dementsprechend auch genau darauf Bezug, ohne die technischen Probleme dahinter anzusprechen - denn mit den Standardverschlüsselungssystemen ist dies logisch gesehen schlachtweg nicht möglich und alternative Verfahren wie die homomorphe Verschlüsselung (d.h. das Rechnen mit verschlüsselten Daten) stecken noch in den Kinderschuhen.

Zum Schluss sei nochmals erwähnt, dass eine umfassende juristische Abklärung eines konkreten Falles zum Thema Auslagerung in die Cloud nicht die Aufgabe einer Informatikerin oder eines Informatikers sondern einer Juristin oder eines Juristen respektive einer Anwältin oder eines Anwalts mit entsprechender Spezialisierung ist. Sollte trotzdem einmal ein Cloud Vertrag auf dem Bürotisch einer Informatikabteilung landen, kann mit nachfolgendem Diagramm jedoch zumindest abgeschätzt werden, ob der Vertrag zurück in die juristische Abteilung wandern sollte oder nicht.







5 Anhang

A Kantonale Merkblätter ZH Cloud

Leitfaden

Bearbeiten im Auftrag

Inhalt

1	Einleitung	2
2	Bearbeiten im Auftrag.....	2
2.1	Allgemeines	2
2.2	Arten des Bearbeiten im Auftrag	3
2.2.1	Inanspruchnahme von Informatikleistungen	3
2.2.2	Datenbearbeitung durch Dritte	4
2.2.3	Inanspruchnahme von Dienstleistungen	4
3	Abgrenzung zum Bearbeiten im Auftrag	4
3.1	Selbstständige Aufgabenerfüllung	4
3.2	Bearbeiten von Personendaten innerhalb einer Verwaltungseinheit.....	5
4	Gesetzliche Grundlagen und Voraussetzungen	5
4.1	Gesetzliche Grundlagen	5
4.2	Kein Entgegenstehen rechtlicher Bestimmungen	5
4.3	Kein Entgegenstehen vertraglicher Vereinbarungen	6
4.4	Verantwortlichkeit	6
4.5	Schriftlicher Vertrag	7
5	Bearbeiten im Auftrag im Ausland	7
6	Vorgehen	7
6.1	Prüfen, ob rechtliche oder vertragliche Bestimmungen entgegenstehen	8
6.2	Prüfen, ob die Sensitivität der Daten dem Bearbeiten im Auftrag entgegensteht....	8
6.3	Auswahl des Auftragnehmers	8
6.4	Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB.....	9
6.5	Umsetzung der Massnahmen	9
7	Checkliste Vorgehen.....	10
8	Anhang 1 – Überblick AGB und Vertragsbestimmungen	11
9	Anhang 2 – Überblick Informationssicherheitsmassnahmen	12

1 Einleitung

Dieser Leitfaden richtet sich an die öffentlichen Organe des Kantons Zürich, die das Bearbeiten von Informationen Dritten übertragen. Das Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](#)) spricht von einem Bearbeiten im Auftrag.

Im Folgenden werden die rechtlichen, organisatorischen und technischen Anforderungen von § 6 IDG und § 25 Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](#)) präzisiert und das Vorgehen aufgezeigt. Es wird auf die im Praxiskommentar zum § 6 IDG¹ gemachten Ausführungen und Zitate abgestützt.

Folgende Dokumente stehen zum Thema Bearbeiten im Auftrag zur Verfügung:

- Checkliste Vorgehen (Ziff. 7 dieses Leitfadens)
- Überblick AGB und Vertragsbestimmungen (Anhang 1 dieses Leitfadens)
- Übersicht Informationssicherheitsmassnahmen (Anhang 2 dieses Leitfadens)
- Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen ([AGB Auslagerung Informatikleistungen](#))
- Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte ([AGB Datenbearbeitung durch Dritte](#))
- [Datenschutzrechtliche Vertragsbestimmungen](#)
- [Übersicht Verschlüsselung der Daten im Rahmen der Auslagerung](#)
- [Muster Geheimhaltungserklärung](#)
- [Merkblatt Cloud Computing](#)
- [Merkblatt privatum Cloud Computing im Schulbereich](#)
- [Merkblatt Dienste Dritter auf Websites](#)
- [Merkblatt Online-Speicherdienste](#)

2 Bearbeiten im Auftrag

2.1 Allgemeines

Ein Bearbeiten im Auftrag im Sinne von § 6 IDG liegt vor, wenn ein öffentliches Organ Informationen, das heisst Sach-, Personen- oder besondere Personendaten durch Private oder andere öffentliche Organe bearbeiten lässt. Man spricht auch von Auslagerung, Outsourcing, Auftragsbearbeitung oder Datenbearbeitung durch Dritte. Unter «Bearbeiten» fällt jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Zugänglichmachen oder Vernichten (§ 3 Abs. 5 IDG).

¹ VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl / Beat Rudin, (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich / Basel / Genf 2012.

2.2 Arten des Bearbeiten im Auftrag

Je nach Art der durch den Auftragnehmer zu bearbeitenden Informationen und Inhalt des Auftrags sind drei Arten des Bearbeitens im Auftrag zu unterscheiden:

- Inanspruchnahme von Informatikleistungen
- Datenbearbeitung durch Dritte
- Inanspruchnahme von Dienstleistungen ausserhalb der ersten beiden Kategorien

2.2.1 Inanspruchnahme von Informatikleistungen

Beispiele der Inanspruchnahme von Informatikleistungen sind:

- Betrieb, Wartung der IT-Infrastruktur (Netzwerk, Server, Anwendungen)
- Wartung von Software
- Hosting von Webangeboten und Services (Websites, Analysetools)
- Inanspruchnahme von Cloud Services

Die datenschutzrechtlichen Anforderungen werden in den [AGB Auslagerung Informatikleistungen](#) konkretisiert.

Werden Wartungsverträge abgeschlossen, im Rahmen derer der Auftragnehmer keine Daten bei sich bearbeitet und speichert, finden die folgenden Bestimmungen der AGB Auslagerung Informatikleistungen keine Anwendung:

- Ziff. 5 Bekanntgabe von Informationen
- Ziff. 7 Informationszugangsgesuche
- Ziff. 8 Teile der Informationssicherheit wie das Unterhalten eines Sicherheitsmanagements und die Trennung der Informationsbestände (dies bedeutet nicht, dass der Auftragnehmer seine Informationen nicht schützen muss, sondern nur, dass in Bezug auf dieses Auftragsverhältnis diese Anforderungen nicht aufgezeigt werden müssen)
- Ziff. 9 Audit durch Externe und Kontrolle durch den Auftraggeber (da die Daten beim Auftraggeber verbleiben und er direkte Kontrolle über diese innehaltet)
- Ziff. 13 Cloud Computing
- Ziff. 17 Vertragsauflösung (Übertragung der Daten kommt bei einem Wartungsvertrag ohne Datenhaltung des Auftragnehmers nicht zur Anwendung)

Weitere Informationen

- [Merkblatt Cloud Computing](#)
- [Merkblatt privatum Cloud Computing im Schulbereich](#)
- [Übersicht Verschlüsselung der Daten im Rahmen der Auslagerung](#)

2.2.2 Datenbearbeitung durch Dritte

Beispiele, bei denen das Bearbeiten von Informationen durch Auftragnehmer in dem Sinne im Zentrum steht, dass «ein Produkt» aus Informationen des öffentlichen Organs für das öffentliche Organ entsteht, sind:

- Auftrag einer Gemeinde an ein Anwaltsbüro zwecks Formulierung eines Beschlusses
- Auftrag zur Durchführung von Bildungsprogrammen
- Auslagerung des Inkassos ausstehender Rechnungen
- Beratungen im Sinn von Stellungnahmen, Gutachten

Die datenschutzrechtlichen Anforderungen werden in den [AGB Datenbearbeitung durch Dritte](#) konkretisiert.

2.2.3 Inanspruchnahme von Dienstleistungen

Beispiele der Inanspruchnahme von Dienstleistungen, die nicht ohne Informationen des öffentlichen Organs erbracht werden können, deren Hauptinhalt jedoch Eigenleistungen des Auftragnehmers sind und im Rahmen derer das Bearbeiten der Informationen des öffentlichen Organs nicht Schwerpunkt ist, sind:

- Coaching
- Wartung von Geräten
- Druck und Versand von Steuerrechnungen
- Durchführung von Workshops und Weiterbildungen
- Beratungen allgemeiner Art

Der Vertragsinhalt richtet sich nach der Sensitivität und dem Schutzbedarf der Informationen und muss im Einzelfall bestimmt werden. Musterformulierungen finden sich in den [datenschutzrechtlichen Vertragsbestimmungen](#).

3 Abgrenzung zum Bearbeiten im Auftrag

3.1 Selbstständige Aufgabenerfüllung

Kein Bearbeiten im Auftrag im Sinne von § 6 IDG ist, wenn Organisationen und Personen des öffentlichen und privaten Rechts selbstständig öffentliche Aufgaben erfüllen, weil sie damit betraut wurden (§ 3 Abs. 1 lit. c IDG). Beispiele:

- Spitäler mit kantonalen Leistungsaufträgen gemäss Spitalliste
- Selbstständige öffentlich-rechtliche Anstalten des Kantons, beispielsweise das Universitätsspital
- Private Beratungsstellen gemäss § 13 lit. c Sozialhilfegesetz ([LS 851.1](#))

3.2 Bearbeiten von Personendaten innerhalb einer Verwaltungseinheit

Das Bearbeiten von Personendaten innerhalb einer im Anhang 2 VOG RR ([LS 172.11](#)) definierten Verwaltungseinheit fällt nicht unter die Voraussetzungen von § 6 IDG. Diese Verwaltungseinheiten erfüllen als Ganzes eine gesetzliche Aufgabe und unterstehen demselben Weisungs- und Aufsichtsrecht. Das Abschliessen eines Vertrags erübrigt sich.

4 Gesetzliche Grundlagen und Voraussetzungen

4.1 Gesetzliche Grundlagen

Für das Bearbeiten im Auftrag gelten folgende gesetzliche Grundlagen:

- IDG ([LS 170.4](#))
- IDV ([LS 170.41](#))
- Gesetz über die Auslagerung von Informatikdienstleistungen ([LS 172.71](#))
- Informatiksicherheitsverordnung ([LS 170.8](#))

4.2 Kein Entgegenstehen rechtlicher Bestimmungen

Dem Bearbeiten im Auftrag dürfen keine rechtlichen Bestimmungen entgegenstehen. Zu denken ist vorab an Geheimnispflichten wie das Amts- oder Berufsgeheimnis. Werden die Informationen verschlüsselt und verbleibt das Schlüsselmanagement beim Auftraggeber, kann auch bei umfassenden Geheimnispflichten ausgelagert werden.

Amtsgeheimnis (Art. 320 StGB)

Das Amtsgeheimnis steht einer Auslagerung grundsätzlich nicht entgegen, denn die Auftragnehmer werden zu Hilfspersonen der Verwaltung. In dieser Funktion unterstehen sie derselben Schweigepflicht wie das öffentliche Organ.

Dennoch müssen verschiedene Faktoren wie die Art der von der Auslagerung betroffenen Daten (Personendaten oder besondere Personendaten) sowie das Datenschutzniveau des Landes, in welches ausgelagert werden soll, berücksichtigt werden. Allenfalls sind besondere vertragliche und/oder technische Sicherheitsvorkehrungen umzusetzen. Siehe dazu die [Übersicht Verschlüsselung der Daten im Rahmen der Auslagerung](#).

Berufsgeheimnis (Art. 321 StGB)

Ob das Berufsgeheimnis auch für Auftragnehmer gilt, ist umstritten. Deshalb sind bei solchen Bearbeitungen im Auftrag spezifische Massnahmen zum Schutz der Daten umzusetzen. Vorbehalten bleiben Datenbearbeitungen durch Dritte, bei denen die Kenntnisnahme der Informationen für die Leistungserbringung durch den Berufsgeheimnisträger unabdingbar ist. Dies kann beispielsweise bei der Wartung von medizinischen Geräten der Fall sein.

Ansonsten sind folgende Varianten möglich:

- Die Daten werden verschlüsselt.
Siehe dazu die [Übersicht Verschlüsselung der Daten im Rahmen der Auslagerung](#).
- Die datenbearbeitenden Personen werden in die funktionale Hierarchie des Auftraggebers eingebunden, wie dies § 3 Abs. 1 Gesetz über die Auslagerung von Informatikleistungen für die kantonale Verwaltung festhält. Dazu werden Mitarbeitende des Auftragnehmers explizit für die konkrete Datenbearbeitung bestimmt, dem Kontroll- und Weisungsrecht des Auftraggebers unterstellt und mittels einer [Geheimhaltungsklärung](#) an das Amts- und/oder Berufsgeheimnis gebunden.
Musterformulierung für den Vertrag: Die Mitarbeitenden des Auftragsnehmers (Namen) unterstehen dem Weisungsrecht des öffentlichen Organs (Name). Sie unterstehen dem Berufsgeheimnis ([Art. 321 StGB](#)).
- Es wird vorgängig die Einwilligung der Betroffenen eingeholt, beispielsweise bei Auslagerungen des Inkassos mittels Hinweis auf einem Anmeldeformular.

Andere Geheimnispflichten

Es gibt eine Vielzahl von weiteren gesetzlich verankerten Schweigeplichten:

§ 71 GG ([LS 131.1](#)), § 120 StG ([LS 631.1](#)), § 47 SHG, Art. 11 OHG ([SR 312.5](#)), Art. 73 StPO ([SR 312](#)). Es ist im Einzelfall zu beurteilen, ob die Schweigeplicht einer Auslagerung entgegensteht.

Andere rechtliche Bestimmungen

Gewisse Aufgaben können nicht ausgelagert werden, beispielsweise die Vornahme von Zwangsmassnahmen durch die Polizei.

4.3 Kein Entgegenstehen vertraglicher Vereinbarungen

Vertragliche Vereinbarungen können einem Bearbeiten im Auftrag entgegenstehen oder dieses nur unter bestimmten Auflagen zulassen. Beispielsweise dürfen Subauftragnehmer bei Einbezug der AGB Auslagerung Informatikleistungen nach Abschluss des Vertrags nur mit schriftlicher Zustimmung des öffentlichen Organs beauftragt werden.

4.4 Verantwortlichkeit

Das öffentliche Organ bleibt für ausgelagerte Datenbearbeitungen verantwortlich, auch wenn das Bearbeiten im Ausland stattfindet, beispielsweise bei der Inanspruchnahme von Cloud Services (§ 6 Abs. 2 IDG). Es muss in der Lage sein, die Pflichten zum Schutz der Informationen wahrzunehmen.

Für den Auftragnehmer bedeutet dies insbesondere, dass er die Informationen nur so wie das öffentliche Organ bearbeiten darf und dass er dieselben Sicherheitsanforderungen in Bezug auf die Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität erfüllen muss.

4.5 Schriftlicher Vertrag

Verträge müssen schriftlich abgeschlossen werden, es sei denn, das Bearbeiten im Auftrag ist gesetzlich geregelt (§ 25 Abs. 1 IDV). Sind vom Bearbeiten im Auftrag besondere Personendaten betroffen, muss der Auftrag durch die vorgesetzte Stelle genehmigt werden (§ 25 Abs. 3 IDV). Dem Bearbeiten im Auftrag unter Inanspruchnahme von Informatiksystemen und -anwendungen mit strategischer Bedeutung für die kantonale Verwaltung muss der Regierungsrat zustimmen (§ 1 Abs. 3 Gesetz über die Auslagerung von Informatikdienstleistungen).

5 Bearbeiten im Auftrag im Ausland

Wenn das Bearbeiten im Auftrag im Ausland stattfindet, nehmen die Risiken für das öffentliche Organ und für die von der Datenbearbeitung betroffenen Personen zu. Ausländische rechtliche Bestimmungen können die Bekanntgabe der Informationen erzwingen oder den Rechtsschutz vereiteln. Diese Risiken müssen durch zusätzliche Massnahmen analog denjenigen in § 19 IDG und § 22 IDV minimiert werden.

Ein dem schweizerischen Datenschutz angemessenes Schutzniveau wird denjenigen Staaten attestiert, welche das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europaratkonvention 108, [SR_0.235.1](#)) unterzeichnet und ratifiziert haben. Eine [Liste dieser Staaten](#) findet sich beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. In diesen Fällen müssen keine zusätzlichen Informationssicherheitsmassnahmen implementiert werden.

Je nach Land können auch andere Mechanismen greifen. So können sich beispielsweise amerikanische Firmen für das [Swiss-US Privacy Shield](#) zertifizieren lassen. Wenn sie auf der Liste des US Departement of Commerce verzeichnet sind, gilt dies als angemessener Schutz. Im Rahmen einer Selbstzertifizierung verpflichten sie sich, die vorgegebenen datenschutzrechtlichen Grundsätze einzuhalten.

Bei besonderen Personendaten oder anderen sensitiven Informationen sollte jedoch ein Bearbeiten im Ausland aufgrund der hohen Risiken unterlassen werden. Wenn dennoch auf gewisse Dienste nicht verzichtet werden kann, sind die Informationen durch spezielle Massnahmen wie beispielsweise die Verschlüsselung zu schützen.

6 Vorgehen

Fünf Schritte zu einem datenschutzkonformen Bearbeiten im Auftrag:

1. Prüfen, ob rechtliche oder vertragliche Bestimmungen entgegenstehen
2. Prüfen, ob die Sensitivität der Informationen der Auslagerung entgegensteht

3. Auswahl des Auftragnehmers
4. Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB
5. Umsetzung der Massnahmen

6.1 Prüfen, ob rechtliche oder vertragliche Bestimmungen entgegenstehen

Die auszulagernden Informationen sind auf Geheimhaltungspflichten zu überprüfen. Es ist zu entscheiden, ob diese einem Bearbeiten im Auftrag entgegenstehen. Allenfalls sind geeignete Massnahmen wie die Verschlüsselung umzusetzen.

Weiter sind andere rechtliche oder vertragliche Vorbehalte in Bezug auf ein Bearbeiten im Auftrag zu berücksichtigen.

Wenn die Daten im Ausland bearbeitet werden, ist zu prüfen, ob die Verantwortung noch wahrgenommen respektive die Kontrolle noch ausgeübt werden kann. Es ist zu prüfen, ob der entsprechende Staat über ein der Schweiz gleichwertiges Datenschutzniveau verfügt oder ob zusätzliche Massnahmen umgesetzt werden müssen.

6.2 Prüfen, ob die Sensitivität der Daten dem Bearbeiten im Auftrag entgegensteht

Das öffentliche Organ muss die Risiken in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität analysieren, die Informationen einer Schutzstufe zuordnen und die Informationssicherheitsmassnahmen definieren. Die Informationen dürfen nicht unberechtigten Dritten zugänglich sein, verloren gehen und unbefugt abgeändert werden können. Aus diesen Beurteilungen resultieren die Massnahmen und somit die Anforderungen an den Auftragnehmer.

Grundsätzlich gilt für die Anforderungen die Kaskade Sachdaten, Personendaten, besondere Personendaten. Je sensitiver die Informationen, desto umfangreicher sind die rechtlichen, organisatorischen und technischen Anforderungen, die das öffentliche Organ und somit auch der Auftragnehmer zu erfüllen haben.

6.3 Auswahl des Auftragnehmers

Stehen dem Bearbeiten im Auftrag keine Geheimhaltungspflichten entgegen, ist der Schutzbedarf bestimmt und sind die Massnahmen definiert, kann ein Auftragnehmer ausgewählt werden. Das öffentliche Organ ist verpflichtet, die analog [Art. 55 OR](#) auferlegten Sorgfaltspflichten zu treffen. Zertifizierungen nach anerkannten Datenschutz- und Informationssicherheitsstandards oder Kontrollberichte von unabhängigen Dritten können bei der Auswahl behilflich sein.

6.4 Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB

Die Verträge für ein Bearbeiten im Auftrag müssen:

- schriftlich abgeschlossen werden (§ 25 Abs. 1 IDV). Das Akzeptieren der AGB genügt, sofern sie die datenschutzrechtlichen Anforderungen erfüllen und nicht einseitig abgeändert werden können.
- durch die vorgesetzte Stelle genehmigt werden, falls besondere Personendaten betroffen sind (§ 25 Abs. 3 IDV)
- vom Regierungsrat bewilligt werden, falls Informatiksysteme und Anwendungen mit strategischer Bedeutung für die kantonale Verwaltung betroffen sind (§ 1 Abs. 1 Gesetz über die Auslagerung von Informatikdienstleistungen)

Der Inhalt eines Vertrags respektive der [AGB](#) umfassen insbesondere:

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich)
- Verfügungsmacht (muss beim öffentlichen Organ liegen)
- Zweckbindung (Daten dürfen nur für Vertragszwecke bearbeitet werden)
- Bekanntgabe von Informationen
- Geheimhaltungsverpflichtungen
- Rechte Betroffener (Auskunft)
- Informationssicherheitsmassnahmen
- Kontrollmöglichkeit des öffentlichen Organs oder externer Prüfstellen
- Unterauftragsverhältnisse (Offenlegung, Änderung nur mit Bewilligung)
- Entwicklung und Wartung
- Orte der Datenbearbeitung (Schweiz oder bei Bearbeiten im Ausland gleichwertiges Datenschutzniveau oder zusätzliche Massnahmen)
- Cloud Computing (den zusätzlichen Risiken angepasste Massnahmen)
- Geschäftsgeheimnis
- Werbung
- Sanktionen
- Vertragsdauer und Voraussetzungen der Vertragsauflösung
- Haftung
- Verhältnis zu anderen geltenden AGB
- Anwendbares Recht (schweizerisches Recht)
- Gerichtsstand (schweizerischer Gerichtsstand)

6.5 Umsetzung der Massnahmen

Die Umsetzung der im Vertrag festgehaltenen Massnahmen muss durch das öffentliche Organ periodisch kontrolliert werden. Bei grossen Anbietern wird dies in der Regel nicht möglich sein. In diesen Fällen können Auditberichte von unabhängigen Prüfstellen in Anspruch genommen werden.

7 Checkliste Vorgehen

1. Bestimmen der Art und des Umfangs der auszulagernden Datenbearbeitung
 - Art der Informationen (Sachdaten, Personendaten, besondere Personendaten)
 - Art des Bearbeiten im Auftrag (Informatikleistung, Datenbearbeitung durch Dritte, Inanspruchnahme anderer Dienstleistungen)
 - Umfang
2. Prüfen, ob rechtliche Bestimmungen dem Bearbeiten im Auftrag entgegenstehen
 - Amtsgeheimnis
 - Berufsgeheimnis
 - Andere Geheimnispflichten
 - Andere rechtliche Bestimmungen
 - Auslagerung ins Ausland: angemessenes Datenschutzniveau

→ Eventuell Massnahmen bestimmen / auf das Bearbeiten im Auftrag verzichten
3. Prüfen, ob vertragliche Bestimmungen dem Bearbeiten im Auftrag entgegenstehen

→ Eventuell Massnahmen bestimmen / auf das Bearbeiten im Auftrag verzichten
4. Bestimmung des Schutzbedarfs und der Massnahmen

→ Siehe Übersicht Anhang 2

→ Siehe [Übersicht Verschlüsselung der Daten im Rahmen der Auslagerung](#)
5. Bestimmen des Vertragsinhalts

→ Siehe Übersicht Anhang 1
6. Auswahl der AGB
 - Informatikleistung: AGB Auslagerung Informatikleistungen
 - Datenbearbeitung durch Dritte: AGB Datenbearbeitung durch Dritte
7. Auswahl des Auftragnehmers und/oder des Produkts
8. Vertragsabschluss
 - Informatikleistung: Vertrag aushandeln, AGB ist integraler Bestandteil
 - Datenbearbeitung: Vertrag aushandeln, AGB ist integraler Bestandteil
 - Andere Dienstleistung: individuellen Vertrag aushandeln
 - Vom Auftragnehmer vorgelegte AGB: auf Inhalt anhand Anhang 1 überprüfen
9. Bearbeiten im Auftrag mit besonderen Personendaten
 - Vertrag durch vorgesetzte Stelle genehmigen
10. Bearbeiten im Auftrag mit strategischer Bedeutung für die kantonale Verwaltung
 - Zustimmung des Regierungsrats einholen
11. Umsetzung der Massnahmen periodisch kontrollieren, kontrollieren lassen, Audit-Bericht einsehen

8 Anhang 1 – Überblick AGB und Vertragsbestimmungen

Inhalt Vertrag	AGB Auslagerung Informatik- leistungen	AGB Datenbearbei- tung durch Dritte	Datenschutz- relevante Vertragsbe- stimmungen*	Im Vertrag regeln / präzisieren
Gegenstand und Umfang der Datenbearbeitung				✓
Umgang mit Personendaten	<ul style="list-style-type: none"> – Verantwortung – Verfügungsmacht – Zweckbindung – Bekanntgabe von Informationen 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓ 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓ 	
Geheimhaltungsverpflichtungen	<ul style="list-style-type: none"> – Amtsgeheimnis – andere Geheimnispflichten 	<ul style="list-style-type: none"> ✓ 	<ul style="list-style-type: none"> ✓ 	<ul style="list-style-type: none"> ✓
Rechte Betroffener	✓			
Informations sicherheitsmassnahmen	✓	✓	✓	✓
Kontrolle der Auftragserfüllung	✓	✓		
Unterauftragsverhältnisse	✓	✓		
Entwicklung und Wartung	✓			
Ort der Datenbearbeitung	<ul style="list-style-type: none"> – Schweiz – Ausland / angemessenes Datenschutzniveau – Ausland / kein angemessenes Datenschutzniveau 	<ul style="list-style-type: none"> ✓ ✓ 		<ul style="list-style-type: none"> ✓ ✓
Cloud Computing	✓			✓
Geschäftsgeheimnisse	✓	✓		
Werbung	✓	✓	✓	
Sanktionen	✓	✓	✓	✓
Vertragsdauer und Voraus- setzungen Vertragsauflösung	✓	✓	✓	✓
Haftung				✓
Verhältnis zu anderen AGB				✓
Anwendbares Recht	✓	✓	✓	
Gerichtsstand	✓	✓	✓	

* Musterformulierungen betreffend Vertragsinhalt bei individueller Gestaltung

9 Anhang 2 – Überblick Informationssicherheitsmaßnahmen

- Verschlüsselung des Transportwegs
Authentisierung mittels Benutzer-ID und Passwort
Gewährleistung der Passwort-Sicherheit
Verhinderung der Top-Risiken (OWASP) im Web
Protokollierung der Datenänderungen
Umsetzungsplanung gemäss ISO 27002
Notfallplanung
Back-up-Konzepte
Kontrolle des IT-Betriebs
Informationspflicht Auftraggeber (Schutzbedarf, Aufbewahrungsfristen)
Informationspflicht Auftragnehmer (Methoden, Prozesse, Unterauftragnehmer, besondere Vorkommnisse)
Mandantentrennung
Patch-Management
- Portabilität
- Verschlüsselung der Datenablage, Key-Management beim Auftraggeber
Zwei-Faktor-Authentisierung
- Managementsystem für Informationssicherheit (ISMS) ISO 27001 / BSI 100–1
Vollständige Protokollierung
Regelmässige Überprüfung der Anwendungen auf Schwachstellen

	Personendaten ¹	Besondere Personendaten
Auslagerung CH	■	■ ■ ■
Cloud CH	■ ■	■ ■ ■ ■
Auslagerung Ausland Cloud Ausland Angemessener Datenschutz ²	■ ■	■ ■ ■ ■
Auslagerung Ausland Cloud Ausland Kein angemessener Datenschutz	■ ■ ■	■ ■ ■ ■

¹ Sachdaten: Der Schutzbedarf der Informationen und die daraus resultierenden organisatorischen und technischen Massnahmen werden im Einzelfall ermittelt.

² [Liste der Staaten mit angemessenem Datenschutzniveau](#)



datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich
Telefon 043 259 39 99
Fax 043 259 51 38
datenschutz@dsb.zh.ch
www.datenschutz.ch



Merkblatt

Cloud Computing

1 Einleitung

Dieses Merkblatt richtet sich an die öffentlichen Organe im Kanton Zürich, die Cloud Services evaluieren oder bereits nutzen.

Die Inanspruchnahme von Cloud Services ist ein «Bearbeiten im Auftrag» (auch Auslagerung oder Outsourcing genannt) und muss den Ansprüchen an die Informationsbearbeitung ebenso genügen wie ein Outsourcing einer Informationsbearbeitung im konventionellen Sinn. Da bei der Nutzung von Cloud Services die Risiken in Bezug auf die Verletzung der Rahmenbedingungen und bei der Bearbeitung von Personendaten insbesondere in Bezug auf die Verletzung der Persönlichkeitsrechte wesentlich höher sind als bei einem konventionellen Outsourcing, ist auf einzelne, vom Gesetz geforderte Bestimmungen spezielles Augenmerk zu richten.

Ausgangspunkt der Nutzung solcher Cloud Services ist eine Risikoanalyse, welche die Anforderungen an den Cloud-Anbieter und im Weiteren den Inhalt des schriftlich zu vereinbarenden Vertrags massgeblich bestimmt. Die Cloud-spezifischen Punkte müssen detailliert geregelt und die Umsetzung der festgehaltenen Massnahmen regelmässig kontrolliert werden.

2 Cloud Computing und Outsourcing

Die Inanspruchnahme von Cloud Services ist ein «Bearbeiten im Auftrag» gemäss § 6 IDG (Gesetz über die Information und den Datenschutz) i.V.m. § 25 IDV (Verordnung über die Information und den Datenschutz) und muss sich deshalb an diesen Voraussetzungen orientieren (siehe Leitfaden [Bearbeiten im Auftrag](#)). Öffentliche Organe dürfen Cloud Services nutzen, wenn sie in der Lage sind, ihre Pflichten in Bezug auf Datenschutz und Informationssicherheit wahrzunehmen. Sie sind für die Datenbearbeitung verantwortlich.

Die der Cloud eigenen Besonderheiten und die dadurch entstehenden Risiken, beispielsweise die Nutzung einer Infrastruktur durch mehrere Beteiligte, müssen durch angemessene Ausgleichsmaßnahmen aufgefangen werden. Bei der Auswahl, der schriftlichen Vertragsgestaltung und der Umsetzung der Massnahmen müssen deshalb zusätzliche Punkte beachtet werden. Die grössten Herausforderungen bestehen in Bezug auf die Transparenz, die Kontrollen und allgemein in Bezug auf die Wahrnehmung der Verantwortung durch das öffentliche Organ.

3 Risikoanalyse und Anbieterauswahl

Die öffentlichen Organe führen für ihre Informatiksysteme und -anwendungen eine Risikoanalyse durch. Je nach Gefährdungspotenzial erfolgt die Einstufung in eine der drei Sicherheitsstufen. Anschliessend werden die Schutzziele ermittelt. Aus diesen Beurteilungen resultieren die massgebenden Faktoren für die Auswahl des Cloud-Anbieters, denn sie bestimmen die grundlegenden organisatorischen, technischen und rechtlichen Anforderungen, die dieser zu erfüllen hat.

Cloud-spezifische Risiken sind insbesondere bei den folgenden Punkten zu beachten:

- Wahrnehmung der Verantwortung durch beide Parteien
- Verlust der Kontrolle oder Verunmöglichung der Kontrollpflichten
- Durchsetzbarkeit der Löschungs- und Berichtigungsansprüche
- Gewährleistung eines gleichwertigen Datenschutzniveaus
- Umsetzung der notwendigen IT-Sicherheitsmaßnahmen
- Überprüfbarkeit der Abläufe und Prozesse
- Nachvollziehbarkeit der Datenbearbeitungen
- Datenverlust
- Datenmissbrauch
- Eingeschränkte Verfügbarkeit der Dienste
- Portabilität und Interoperabilität

Der Cloud-Anbieter hat über die rechtlichen, organisatorischen und technischen Rahmenbedingungen der angebotenen Dienstleistung zu informieren. Hilfsinstrumente können diesbezüglich Zertifikate oder unabhängige Auditberichte sein, die gewisse Aspekte der Dienstleistung transparent machen. Deren Aussagekraft hängt von der Berücksichtigung nationaler und internationaler Standards ab.

4 Vertragsgestaltung

Das öffentliche Organ muss seine Verantwortung i.S.v. § 6 IDG auch in einer Cloud-Struktur wahrnehmen können. Es ist deshalb detailliert und schriftlich in einem Vertrag festzuhalten, wer wofür im Sinne des IDG verantwortlich zeichnet (siehe Ziff. 7 Checkliste «Vorgehen» und Ziff. 8 Anhang 1 «Überblick AGB und Vertragsbestimmungen» im Leitfaden [Bearbeiten im Auftrag](#)). Den folgenden Punkten ist besondere Beachtung zu schenken.

4.1 Kontrolle

Die Kontrollrechte des öffentlichen Organs sowie unabhängiger Aufsichtsbehörden (Datenschutzbeauftragter/Finanzkontrolle) sind zu verankern. Dies betrifft insbesondere auch die Kontrollmöglichkeit vor Ort.

Weiter ist der Cloud-Anbieter zu verpflichten, regelmässig Kontrollen nach internationalen Audit-Standards durchführen zu lassen. Der Cloud-Anbieter ist zu verpflichten, die Prüfungsergebnisse unabhängiger Kontrollstellen dem öffentlichen Organ zur Verfügung zu stellen.

4.2 Rechte Betroffener

Die Gewährleistung des Auskunftsrechts von Personen über ihre gespeicherten Daten ist festzuhalten. Der Cloud-Anbieter hat die Durchsetzung der Rechte Betroffener auf Berichtigung und Löschung vertraglich zu garantieren.

4.3 Ort der Datenbearbeitung

Es ist schriftlich zu vereinbaren, dass der Cloud-Anbieter über sämtliche möglichen Datenbearbeitungsorte Auskunft erteilen muss. Ortswechsel müssen gemeldet und vom öffentlichen Organ bewilligt werden.

4.4 Gleichwertiges Datenschutzniveau

Datenbekanntgaben ins Ausland unterliegen den Bestimmungen von § 19 IDG. Diese gelten analog für die Inanspruchnahme von Cloud Services, wenn es sich um das Bearbeiten von Personendaten handelt. Sofern Cloud Services Datenbearbeitungen im Ausland beinhalten, dürfen diese nur ins Ausland ausgelagert werden, wenn ein der Schweiz gleichwertiges Datenschutzniveau besteht und/oder zusätzliche Sicherheitsmassnahmen umgesetzt werden.

4.5 Unterauftragsverhältnisse

Unterauftragsverhältnisse müssen vor Vertragsabschluss offengelegt werden. Festzuhalten ist, dass nachträgliche Vereinbarungen nur mit Kenntnis und Zustimmung des öffentlichen Organs unterzeichnet werden dürfen. Diese Unter-Auftragnehmer müssen verpflichtet werden, Weisungen des Cloud-Anbieters zu beachten.

4.6 Anwendbares Recht und Gerichtsstand

Es ist festzuhalten, dass schweizerisches Recht, insbesondere das IDG, anwendbar ist. Weiter muss ein Gerichtsstand in der Schweiz vereinbart werden.

4.7 Organisatorische und technische Sicherheitsmassnahmen

Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit müssen auch bei der Nutzung von Cloud Services gewährleistet sein. Die zu bearbeitenden Datenkategorien und deren Schutzbedarf sind vertraglich festzuhalten. Es ist zu vereinbaren, dass der Cloud-Anbieter das öffentliche Organ regelmässig über die Erfüllung der wichtigsten Massnahmen im IT-Sicherheitsbereich orientiert. Weiter muss der Cloud-Anbieter über sicherheitsrelevante Vorfälle orientieren.

Der Cloud-Anbieter muss die im Rahmen von § 7 IDG geforderten, nicht abschliessend aufgezählten Schutzziele garantieren. In einem Informationssicherheitskonzept hat er die organisatorischen und technischen Sicherheitsmassnahmen wie kryptografische Verfahren, Identity- und Accessmanagement, Notfallmanagement usw. festzuhalten (siehe Übersicht [Verschlüsselung der Daten im Rahmen der Auslagerung](#)). Beim Bearbeiten von besonderen Personendaten hat er die organisatorischen und technischen Massnahmen in einem Managementsystem für Informationssicherheit zu verwalten.

Speziell zu vereinbaren sind organisatorische und technische Massnahmen, die die Portabilität, die Interoperabilität sowie die Mandantentrennung gewährleisten (siehe Ziff. 9 Anhang 2 «Übersicht Informationssicherheitsmassnahmen» im Leitfaden [Bearbeiten im Auftrag](#)).

5 Umsetzung der Massnahmen

Das öffentliche Organ muss die Umsetzung der organisatorischen, technischen und rechtlichen Rahmenbedingungen, wie im Vertrag festgehalten, laufend überprüfen.

6 Quellenverzeichnis und weiterführende Links

Datenschutzbeauftragter des Kantons Zürich

- [Leitfaden Bearbeiten im Auftrag](#)

Privatim – Konferenz der schweizerischen Datenschutzbeauftragten

- [Merkblatt Cloud Computing im Schulbereich](#)

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Deutschland)

- [Orientierungshilfe – Cloud Computing, Version 2.0](#)

Bundesamt für Sicherheit in der Informationstechnik (BSI, Deutschland)

- [Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestanforderungen in der Informationssicherheit, Eckpunktepapier, Februar 2012](#)
- [Sichere Nutzung von Cloud-Diensten, August 2016](#)
- [Baustein B 1.17 Cloud Nutzung](#)
- [Baustein B 3.303 Speicherlösungen / Cloud Storage](#)
- [Baustein B 3.304 Virtualisierung](#)
- [Baustein Cloud Management \(Vorabversion\)](#)

Links zu weiterführenden Informationen

- Marit Hansen, [Vertraulichkeit und Integrität der Daten und IT-Systeme im Cloud-Zeitalter](#)
- Thilo Weichert, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, [Cloud Computing und Datenschutz](#)
- Datenschutzstelle Fürstentum Liechtenstein, [Cloud Computing, Häufig gestellte Fragen](#)
- European Union Agency for Network and Information Security (enisa), [Cloud Computing Risk Assessment](#)



datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh



Datenschutz mit Qualität

B FINMA Rundschreiben 2008/21 und 2018/3



Rundschreiben 2008/21 Operationelle Risiken – Banken

Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken

Referenz:	FINMA-RS 08/21 „Operationelle Risiken – Banken“
Erlass:	20. November 2008
Inkraftsetzung:	1. Januar 2009
Letzte Änderung:	22. September 2016 [Änderungen sind mit * gekennzeichnet und am Schluss des Dokuments aufgeführt]
Konkordanz:	vormals EBK-RS 06/3 „Operationelle Risiken“ vom 29. September 2006
Rechtliche Grundlagen:	FINMAG Art. 7 Abs. 1 Bst. b BankG Art. 3 Abs. 2 Bst. a und b, 3g, 4 Abs. 2 und 4, 4 ^{bis} Abs. 2 BankV Art. 12 BEHG Art. 10 Abs. 2 Bst. a BEHV Art. 19 Abs. 3, 20 Abs. 1, 29 ERV Art. 2, 89–94 FINMA-GebV Art. 5 ff.
Anhang 1:	Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV
Anhang 2:	Übersicht zur Kategorisierung von Ereignistypen
Anhang 3:	Umgang mit elektronischen Kundendaten



Adressaten		
X Banken	BankG	
X Finanzgruppen und -kongl.		
Andere Intermediäre		
Versicherer		
Vers.-Gruppen und -kongl.	VAG	
Vermittler		
X Effektenhändler	BEHG	
Handelsplätze		
Zentrale Gegenparteien		
Zentralenwahrer		
FinfraG		
Transaktionsregister		
Zahlungssysteme		
Teilnehmer		
Fondsleitungen		
SICAV		
KmG für KKA		
SICAF		
Depotbanken	KAG	
Vermögensverwalter KKA		
Vertriebssträger		
Vertreter ausl. KKA		
Andere Intermediäre		
SRO		
DUFI	GwG	
SRO-Beaufsichtigte		
Prüfgesellschaften		
Ratingagenturen	Andere	

Inhaltsverzeichnis



I. Gegenstand	Rz	1
II. Begriff	Rz	2–2.1
III. Eigenmittelanforderungen	Rz	3–116
A. Der Basisindikatoransatz (BIA, Art. 92 ERV)	Rz	3–22
B. Der Standardansatz (SA, Art. 93 ERV)	Rz	23–44
a) Mechanismus	Rz	23–27
b) Allgemeine Anforderungen (Art. 93 Abs. 3 ERV)	Rz	28–29
c) Aufgehoben	Rz	30–44
C. Institutsspezifische Ansätze (AMA, Art. 94 ERV)	Rz	45–107
a) Bewilligung	Rz	45–49
b) Zusätzliche qualitative Anforderungen	Rz	50–68
c) Allgemeine quantitative Anforderungen	Rz	69–75
d) Interne Verlustdaten (Art. 94 Abs. 2 ERV)	Rz	76–85
e) Externe Verlustdaten (Art. 94 Abs. 2 ERV)	Rz	86–88
f) Szenarioanalyse (Art. 94 Abs. 2 ERV)	Rz	89–91
g) Geschäftsumfeld und internes Kontrollsystem (Art. 94 Abs. 2 ERV)	Rz	92–97
h) Risikoverminderung durch Versicherungen	Rz	98–107
D. Partielle Anwendung von Ansätzen	Rz	108–114
E. Anpassungen der Eigenmittelanforderungen (Art. 45 ERV)	Rz	115
F. Mindesteigenmittel und Untergrenze (<i>Floor</i>)	Rz	116
IV. Qualitative Anforderungen	Rz	117–138
A. Proportionalitätsprinzip	Rz	117–118
B. Qualitative Grundanforderungen	Rz	119–134
a) Grundsatz 1: Kategorisierung und Klassifizierung von operationellen Risiken	Rz	121–127
b) Grundsatz 2: Identifizierung, Begrenzung und Überwachung	Rz	128–130

Inhaltsverzeichnis



c)	Grundsatz 3: Interne und Externe Berichterstattung	Rz	131–134
d)	Grundsatz 4: Technologieinfrastruktur	Rz	135–135.12
e)	Grundsatz 5: Kontinuität bei Geschäftsunterbrechung	Rz	136
f)	Grundsatz 6: Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken	Rz	136.1
g)	Grundsatz 7: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft	Rz	136.2-136.5
C.	Risikospezifische Qualitative Anforderungen	Rz	137–138
V.	Prüfung und Beurteilung durch die Prüfgesellschaften	Rz	139

I. Gegenstand

Dieses Rundschreiben konkretisiert die Art. 89–94 der Eigenmittelverordnung (ERV; SR 952.03) und definiert die qualitativen Grundanforderungen an das Management der operationellen Risiken beruhend auf Art. 12 BankV sowie Art. 19–20 BEHV. Es regelt im quantitativen Bereich die Bestimmung der Eigenmittelanforderungen für operationelle Risiken nach den drei zur Auswahl stehenden Ansätzen sowie die damit einhergehenden Verpflichtungen. Die qualitativen Grundanforderungen entsprechen den Basler Empfehlungen zum einwandfreien Management der operationellen Risiken.

1*

II. Begriff

Operationelle Risiken sind gemäss Art. 89 ERV definiert als die „Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen oder Systemen oder in Folge von externen Ereignissen eintreten.“ Die Definition umfasst sämtliche Rechts- bzw. Compliance-Risiken, soweit sie einen direkten, finanziellen Verlust darstellen, d.h. inklusive Bussen durch Aufsichtsbehörden und Vergleiche.

2*

Aufgehoben

2.1*

III. Eigenmittelanforderungen

A. Der Basisindikatoransatz (BIA, Art. 92 ERV)

Für Banken, die ihre Eigenmittelanforderungen für operationelle Risiken nach dem Basisindikatoransatz bestimmen, ergeben sich diese als Produkt des Multiplikators α und dem aus den vorangegangenen drei Jahren bestimmten Durchschnitt der jährlichen Ertragsindikatoren GI¹. Für die Durchschnittsbildung sind jedoch nur diejenigen Jahre zu berücksichtigen, in denen GI einen positiven Wert aufweist.

3

Die drei vorangegangenen Jahre nach Rz 3 (bzw. Rz 24) entsprechen den drei unmittelbar dem Stichtag der letzten publizierten Erfolgsrechnung vorangegangenen Einjahresperioden. Wurde beispielsweise die letzte publizierte Erfolgsrechnung per Stichtag 30. Juni 2008 erstellt, so entsprechen die zu berücksichtigenden drei Jahre den Perioden 1. Juli 2005 bis 30. Juni 2006, 1. Juli 2006 bis 30. Juni 2007 und 1. Juli 2007 bis 30. Juni 2008.

4

Damit ergeben sich die Eigenmittelanforderungen K_{BIA} als

5

¹ In den revidierten Mindeststandards des Basler Ausschusses für Bankenaufsicht („International Convergence of Capital Measurement and Capital Standards – A Revised Framework / Comprehensive Version“) vom Juni 2006 wird der Ertragsindikator als Gross Income bezeichnet.

$$K_{BIA} = \alpha \cdot \sum_{j=1}^3 \frac{\max[0, GI_j]}{\max[1, n]}$$

wobei

- α einheitlich als 15 % festgelegt ist; 6
- GI_j dem Ertragsindikator für das jeweils relevante Jahr j entspricht; und 7
- n für die Anzahl jener der drei vorangegangenen Jahre steht, in denen jeweils ein positiver Ertragsindikator GI registriert wurde. 8

Der Ertragsindikator GI berechnet sich als Summe aus den folgenden Positionen der Erfolgsrechnung gemäss Rz 125 ff. FINMA-RS 15/1 „Rechnungslegung Banken“: 9*

- Brutto-Erfolg Zinsengeschäft (Rz 131 FINMA-RS 15/1 „Rechnungslegung Banken“); 10*
- Erfolg aus dem Kommissions- und Dienstleistungsgeschäft² (Rz 139 FINMA-RS 15/1 „Rechnungslegung Banken“); 11*
- Erfolg aus dem Handelsgeschäft und der Fair-Value-Option (Rz 140 FINMA-RS 15/1 „Rechnungslegung Banken“); 12*
- Beteiligungsertrag (Rz 143 FINMA-RS 15/1 „Rechnungslegung Banken“) aus nicht zu konsolidierenden Beteiligungen; und 13*
- Liegenschaftenerfolg (Rz 144 FINMA-RS 15/1 „Rechnungslegung Banken“). 14*

Die Grundlage zur Bestimmung des Ertragsindikators GI auf konsolidierter Ebene entspricht dem Konsolidierungskreis für die Bestimmung der Eigenmittelanforderungen. 15

Erweitern sich die Struktur oder die Aktivitäten einer Bank (z.B. infolge Übernahme einer neuen Geschäftseinheit), sind die historischen Werte des Ertragsindikators GI entsprechend nach oben anzupassen. Reduktionen des Ertragsindikators GI (z.B. nach der Veräußerung eines Geschäftsbereichs) erfordern eine Bewilligung der FINMA. 16

Zur Bestimmung des Ertragsindikators GI nach Art. 91 Abs. 1 ERV können Banken anstelle der schweizerischen Rechnungslegungsvorschriften international anerkannte Rechnungsstandards verwenden, sofern die FINMA dafür die Bewilligung erteilt (vgl. Art. 91 Abs. 4 ERV). 17

Sämtliche Erträge aus Auslagerungsvereinbarungen (Outsourcing), bei denen die Bank selbst als Dienstleisterin auftritt, sind als Bestandteile des Ertragsindikators GI zu berücksichtigen (vgl. Art. 91 Abs. 2 ERV). 18

² Die Berücksichtigung des Kommissionsaufwandes nach Rz 138 FINMA-RS 15/1 „Rechnungslegung Banken“ unterliegt den Restriktionen von Rz 18.

Tritt die Bank als Auftraggeberin einer ausgelagerten Dienstleistung auf, dürfen entsprechende Aufwendungen vom Ertragsindikator GI nur dann abgezogen werden, wenn die Auslagerung innerhalb derselben Finanzgruppe erfolgt und konsolidiert erfasst wird (vgl. Art. 91 Abs. 3 ERV). 19

Aufgehoben 20*

Aufgehoben 21*

Aufgehoben 22*

B. Der Standardansatz (SA, Art. 93 ERV)

a) Mechanismus

Zur Bestimmung der Eigenmittelanforderungen haben Banken ihre gesamten Tätigkeiten den folgenden Geschäftsfeldern zuzuordnen: 23

i	Geschäftsfeld	β_i
1	Unternehmensfinanzierung/-beratung	18 %
2	Handel	18 %
3	Privatkundengeschäft	12 %
4	Firmenkundengeschäft	15 %
5	Zahlungsverkehr/Wertschriftenabwicklung	18 %
6	Depot- und Treuhandgeschäfte	15 %
7	Institutionelle Vermögensverwaltung	12 %
8	Wertschriftenprovisionsgeschäft	12 %

Tabelle 1

Für jedes Geschäftsfeld i und für jedes der drei vorangegangenen Jahre nach Rz 4 ist ein Ertragsindikator nach Rz 9–18 zu ermitteln und mit dem jeweiligen Faktor β_i gemäss Tabelle 1 zu multiplizieren. Die resultierenden Zahlenwerte sind für jedes Jahr zu addieren, wobei negative Zahlenwerte aus einzelnen Geschäftsfeldern mit positiven Zahlenwerten anderer Geschäftsfelder verrechnet werden können. Die Eigenmittelanforderungen entsprechen dem Betrag des Dreijahresdurchschnitts, wobei für die Durchschnittsbildung allfällige negative Summanden gleich null gesetzt werden müssen (vgl. Art. 93 Abs. 1 ERV). 24

Die Eigenmittelanforderungen im Standardansatz K_{SA} ergeben sich als 25

$$K_{SA} = \frac{1}{3} \cdot \sum_{j=1}^3 \max \left[0, \sum_{i=1}^8 GI_{i,j} \cdot \beta_i \right]$$

Dabei entspricht

- $G_{i,j}$ dem Ertragsindikator GI für das i-te Geschäftsfeld im jeweils relevanten Jahr j; und 26
- β_i einem als fixer Prozentsatz für das i-te Geschäftsfeld vorgegebenen, für alle Banken 27 identischen, Multiplikator.

b) Allgemeine Anforderungen (Art. 93 Abs. 3 ERV)

Aufgehoben	28*
Jede Bank muss nach Massgabe von Anhang 1 spezifische Grundsätze zur Allokation von Geschäftsaktivitäten in die standardisierten Geschäftsfelder nach Rz 23 festlegen und dafür über dokumentierte Kriterien verfügen. Die Kriterien sind regelmässig zu überprüfen und müssen den jeweils aktuellen Veränderungen der Aktivitäten der Bank angepasst werden.	

c) Aufgehoben

Aufgehoben	30*
Aufgehoben	31*
Aufgehoben	32*
Aufgehoben	33*
Aufgehoben	34*
Aufgehoben	35*
Aufgehoben	36*
Aufgehoben	37*
Aufgehoben	38*
Aufgehoben	39*
Aufgehoben	40*
Aufgehoben	41*
Aufgehoben	42*
Aufgehoben	43*
Aufgehoben	44*

C. Institutsspezifische Ansätze (AMA, Art. 94 ERV)

a) Bewilligung

Institutsspezifische Ansätze (*Advanced Measurement Approaches*, AMA) erlauben es den Banken, ihre Eigenmittelanforderungen für operationelle Risiken unter Einhaltung bestimmter Anforderungen nach einem individuellen Verfahren selbst zu quantifizieren. 45

Die Anwendung eines institutsspezifischen Ansatzes erfordert eine Bewilligung durch die FINMA. 46

Die FINMA kann von Banken vor einer Bewilligung für die Anwendung eines institutsspezifischen Ansatzes verlangen, dass über eine Zeitperiode von maximal zwei Jahren Berechnungen gestützt auf den entsprechenden Ansatz zu Test- und Vergleichszwecken durchgeführt werden müssen. 47

Verwendet eine Bank einen institutsspezifischen Ansatz, so kann ein allfälliger vollständiger oder partieller Wechsel zum Basisindikator- oder zum Standardansatz nur auf Anordnung oder mit Bewilligung der FINMA erfolgen. 48

Der Aufwand der FINMA im Zusammenhang mit dem Bewilligungsverfahren sowie mit notwendigen Prüfarbeiten nach Erteilung der Bewilligung wird den betreffenden Banken in Rechnung gestellt. 49

b) Zusätzliche qualitative Anforderungen

Banken, die einen institutsspezifischen Ansatz verwenden, müssen die qualitativen Grundanforderungen gemäss Kapitel IV.B erfüllen. 50*

Die Verwendung eines institutsspezifischen Ansatzes zur Bestimmung der Eigenmittelanforderungen für operationelle Risiken setzt zusätzlich die Erfüllung folgender weiterer qualitativer Anforderungen voraus. 51

Das Organ für die Oberleitung, Aufsicht und Kontrolle muss aktiv in die Überwachung des Ansatzes involviert sein. 52

Die Geschäftsleitung muss mit dem Grundkonzept des Ansatzes vertraut sein und ihre entsprechenden Überwachungsfunktionen wahrnehmen können. 53*

Die Bank verfügt in Bezug auf ihr Management der operationellen Risiken über ein konzeptionell solides, zuverlässiges und integer implementiertes System. 54

Auf allen Ebenen der Bank stehen ausreichende Ressourcen für das Management, die Kontrolle und die interne Revision im Zusammenhang mit dem institutsspezifischen Ansatz zur Verfügung. 55

Die Bank muss über eine unabhängige zentrale Einheit für das Management der operationellen Risiken verfügen, die für die Ausarbeitung und Implementierung von Grundsätzen des 56

operationellen Risikomanagements verantwortlich ist. Diese Einheit ist zuständig für:

- die Erstellung bankweiter Grundsätze und Verfahren für das Management und die Kontrolle operationeller Risiken; 57

- die Ausarbeitung und Anwendung der institutsspezifischen Quantifizierungsmethodik für operationelle Risiken; 58

- die Ausarbeitung und die Umsetzung eines Meldesystems für operationelle Risiken; und 59

- die Entwicklung von Strategien zur Identifikation, Messung, Überwachung sowie der Kontrolle bzw. Verminderung operationeller Risiken. 60

Das institutsspezifische Quantifizierungssystem muss eng in die täglichen Risikomanagementprozesse der Bank integriert sein. 61

Die Ergebnisse des institutsspezifischen Quantifizierungssystems sollen einen integralen Bestandteil der Risikoprofilüberwachung und -kontrolle darstellen. Beispielsweise müssen diese Informationen eine prominente Rolle in der Berichterstattung an das Management, bei der internen Eigenmittelallokation und bei der Risikoanalyse spielen. 62

Die Bank muss über Methoden zur Allokation von Eigenmitteln für operationelle Risiken auf die bedeutenden Geschäftsfelder und zur Schaffung von Anreizen zur Verbesserung des operationellen Risikomanagements in der gesamten Bank verfügen. 63

Aufgehoben 64*

Die interne Revision und die Prüfgesellschaft müssen die Prozesse für das Management operationeller Risiken und die Umsetzung des institutsspezifischen Ansatzes regelmäßig überprüfen. Diese Prüfungen sollen sowohl die Aktivitäten der einzelnen Geschäftseinheiten als auch jene der zentralen Einheit für das Management operationeller Risiken umfassen. 65

Die Validierung des Quantifizierungssystems durch die Prüfgesellschaft muss insbesondere Folgendes beinhalten: 66

- Verifikation eines zufriedenstellenden Funktionierens der bankinternen Validierungsprozesse; und 67

- Sicherstellung der Transparenz und Zugänglichkeit der Datenflüsse und Prozesse des institutsspezifischen Ansatzes. Insbesondere muss sichergestellt sein, dass die interne Revision, die Prüfgesellschaft und die FINMA auf die Spezifikationen und Parameter des Ansatzes zugreifen können. 68

c) Allgemeine quantitative Anforderungen

In Übereinstimmung mit den Basler Mindeststandards ³ spezifiziert die FINMA keinen bestimmten Ansatz, sondern lässt den Banken diesbezüglich grosse Freiräume. Dieses Rundschreiben beschränkt sich daher auf die Darstellung zentraler Anforderungen, welche zur Anwendung eines solchen Ansatzes zwingend vorausgesetzt werden. Die Prüfung der detaillierten Spezifikationen eines institutsspezifischen Ansatzes ist Gegenstand des individuellen Be willigungsprozesses. Dieser findet unter Leitung der FINMA und unter Einbezug der Prüf gesellschaft statt.	69
Unabhängig von der konkreten Ausgestaltung ihres Ansatzes muss eine Bank nachweisen können, dass dieser auch quantitativ bedeutungsvolle, mit kleiner Wahrscheinlichkeit auftretende Verlustereignisse berücksichtigt. Die aus dem Ansatz resultierende Eigenmittelanforde rung soll etwa dem 99.9 %-Quantil der Verteilungsfunktion der jeweils über ein Jahr aggregierten operationellen Verluste entsprechen.	70
Jeder institutsspezifische Ansatz muss von einem Begriff des operationellen Risikos ausgehen, der mit dem Begriff gemäss Art. 89 ERV sowie Rz 2 kompatibel ist. Er muss zusätzlich eine Kategorisierung von Verlustereignissen gemäss Anhang 2 ermöglichen.	71*
Erforderliche Eigenmittel werden sowohl für die erwarteten als auch für die unerwarteten Ver luste erhoben. Die FINMA kann jedoch einer Bank diesbezüglich Erleichterungen gewähren, wenn diese für zukünftige erwartete Verluste angemessene Rückstellungen gebildet hat.	72
Sämtliche expliziten und impliziten Annahmen betreffend Abhängigkeiten zwischen operatio nellen Verlustereignissen sowie zwischen verwendeten Schätzfunktionen müssen plausibel sein und begründet werden können.	73
Jeder Ansatz muss über bestimmte Grundeigenschaften verfügen. Dazu gehört insbesondere die Erfüllung der Anforderung zur Integration von:	74
<ul style="list-style-type: none"> • internen Verlustdaten (Rz 76–85); • relevanten externen Verlustdaten (Rz 86–88); • Szenarioanalyseverfahren (Rz 89–91); und • Faktoren des Geschäftsumfelds und des internen Kontrollsystems (Rz 92–97). 	
Eine Bank benötigt ein zuverlässiges, transparentes, gut dokumentiertes und verifizierbares Konzept für den Einbezug und die Bestimmung der relativen Bedeutung all dieser vier Input Faktoren in ihrem Ansatz. Der Ansatz muss intern konsistent sein und insbesondere die mehrfache Berücksichtigung risikomindernder Elemente (z.B. Faktoren des Geschäftsumfelds und des internen Kontrollsystems oder Versicherungskontrakte) vermeiden.	75

³ Vgl. Fussnote 1

d) Interne Verlustdaten (Art. 94 Abs. 2 ERV)

Eine Bank muss über dokumentierte Verfahren zur Beurteilung der fortlaufenden Relevanz historischer Verlustdaten verfügen. Dazu gehören insbesondere klare interne Regeln, wie die Berücksichtigung von Verlustdaten verändert werden kann (z.B. vollständige Nichtberücksichtigung auf Grund fehlender aktueller Relevanz, Skalierung auf Grund von veränderten Grössenverhältnissen oder Adjustierung in irgendeiner anderen Form). Dabei ist auch zu definieren, wer zu solchen Veränderungen bis zu welcher Dimension autorisiert ist.

76

Eine Bank muss eine Datenbank mit internen Verlustdaten verwenden. Diese muss bei der erstmaligen Verwendung des Ansatzes zu regulatorischen Zwecken einen Beobachtungszeitraum von mindestens drei Jahren umfassen. Spätestens zwei Jahre nach erstmaliger Verwendung des Ansatzes muss sich der Beobachtungszeitraum dauerhaft über mindestens fünf Jahre erstrecken.

77

Der Prozess zur Schaffung einer bankinternen Datenbank für operationelle Verluste muss die folgenden Anforderungen erfüllen:

78

- Zur Unterstützung der regulatorischen Validierung muss eine Bank sämtliche erfassten internen Verlustdaten den Geschäftsfeldern gemäss Rz 23 und den Ereignistypen gemäss Anhang 2 zuordnen können. Sie muss über dokumentierte und objektive Kriterien für diese Kategorisierung verfügen.

79*

- Die internen Verlustdaten einer Bank müssen gestützt auf einen integren und soliden Prozess umfassend gesammelt werden. Sie müssen alle materiellen Aktivitäten und Expositionen, inklusive aller relevanten Subsysteme und geographischen Lokalitäten abdecken. Bei der Verlustdatensammlung darf auf die systematische Erfassung von Verlusten unter einem bestimmten durch die FINMA festgelegten Brutto-Mindestbetrag verzichtet werden.

80

- Zu jedem Verlustereignis hat eine Bank die folgenden Informationen zu sammeln: Brutto-Verlustbetrag, Datum des Verlustereignisses und allfällige Verlustminderungen (z.B. auf Grund von Versicherungskontrakten). Für Verlustereignisse mit einem Brutto-Verlustbetrag von mindestens 1 Mio. CHF sind zudem Erläuterungen zu den Ursachen des Verlustes festzuhalten.

81

- Eine Bank muss Grundsätze für die Erfassung von Verlustereignissen definieren. Dazu gehören auch Kriterien für die Kategorisierung von Verlustereignissen aus zentralen Funktionen (zum Beispiel der EDV-Abteilung) oder von Verlustereignissen, die mehr als ein Geschäftsfeld betreffen. Im Weiteren muss geregelt sein, wie mit Serien von untereinander nicht unabhängigen Verlustereignissen umzugehen ist.

82

Verluste aufgrund operationeller Risiken, die im Kontext mit Kreditrisiken entstanden sind, und von einer Bank historisch als Kreditrisiko erfasst wurden, dürfen für die Bestimmung der erforderlichen Eigenmittel weiterhin ausschliesslich als Kreditrisikoereignis betrachtet werden. Sie müssen jedoch ab einem bestimmten durch die FINMA festgelegten Brutto-Mindestverlustbetrag trotzdem in die interne Verlustdatenbank für operationelle Risiken aufgenommen und für das Management operationeller Risiken berücksichtigt werden. Solche

83

Verlustereignisse sind analog den übrigen internen Verlustdaten zu erfassen, jedoch als in Bezug auf operationelle Risiken nicht eigenmittelrelevant zu kennzeichnen.

Äussert sich ein Verlust auf Grund eines operationellen Risikos auch in Form eines Marktrisikoverlustes, so ist das entsprechende Ereignis ebenfalls analog den übrigen Verlustereignissen zu erfassen und in den institutsspezifischen Ansatz zu integrieren. Verwendet eine Bank zur Bestimmung ihrer erforderlichen Eigenmittel für Marktrisiken ein Risikoaggregationsmodell gemäss Rz 228–365 des FINMA-RS 08/20 „Marktrisiken Banken“, so dürfen durch Ereignisse infolge operationeller Risiken entstandene Positionen weder aus der Berechnung des *Value-at-Risk*, des Stress-basierten *Value-at-Risk*, der *Incremental Risk Charge*, der *Comprehensive Risk Measure* noch aus dem *Backtesting* ausgeschlossen werden.

84*

Allfällige „negative Verluste“ (z.B. Gewinne auf Grund einer irrtümlich erworbenen Aktienposition) dürfen im institutsspezifischen Ansatz keine die erforderlichen Eigenmittel reduzierende Wirkung entfalten.

85

e) Externe Verlustdaten (Art. 94 Abs. 2 ERV)

Banken müssen in ihren institutsspezifischen Ansatz relevante externe Verlustdaten einfließen lassen. Dadurch soll die Berücksichtigung seltener aber potenziell schwerwiegender Verlustereignisse sichergestellt werden. Als Quelle der relevanten Informationen können sowohl öffentlich verfügbare als auch zwischen bestimmten Banken ausgetauschte externe Verlustdaten dienen.

86

Für diese externe Verlustdaten sind die effektive Verlusthöhe, Informationen zum Umfang der Aktivitäten im durch den Verlust betroffenen Geschäftsbereich, Informationen über die Ursachen und Umstände des Verlustes sowie Informationen zur Beurteilung der Relevanz des Verlustereignisses für die eigene Bank zu berücksichtigen.

87

Banken müssen die Verwendung externer Verlustdaten durch einen systematischen Prozess festlegen und dokumentieren. Dazu gehört insbesondere eine klare Methodik betreffend die Integration dieser Daten in den institutsspezifischen Ansatz (z.B. Skalierung, qualitative Anpassungen oder Einfluss auf die Szenarioanalyse). Die Rahmenbedingungen und die Verfahren zur Verwendung externer Verlustdaten sind regelmässig zu überprüfen, sowohl intern als auch durch die Prüfgesellschaft.

88

f) Szenarioanalyse (Art. 94 Abs. 2 ERV)

Institutsspezifische Ansätze müssen die Ergebnisse von Szenarioanalyseverfahren berücksichtigen.

89

Für Szenarioanalysen ist auf der Grundlage von Expertenmeinungen und externen Daten die Bedrohung der Bank durch potenziell schwerwiegende Verlustereignisse zu beurteilen.

90

Die für die Szenarioanalyse verwendeten Szenarien und die ihnen zugeordneten Parameter sind bei wesentlichen Veränderungen der Risikolage, mindestens aber jährlich, auf ihre Aktualität und Relevanz hin zu überprüfen und allenfalls anzupassen. Bei wesentlichen Veränderungen der Risikolage sind Anpassungen unmittelbar vorzunehmen.

g) Geschäftsumfeld und internes Kontrollsysteem (Art. 94 Abs. 2 ERV)

Als vorausschauendes Element muss eine Bank prädiktive Faktoren aus dem Umfeld ihrer Geschäftsaktivitäten und aus ihrem internen Kontrollsysteem im institutsspezifischen Ansatz berücksichtigen. Diese dienen dem Ziel, aktuellen Charakteristiken im Risikoprofil der Bank (z.B. neue Aktivitäten, neue Informatiklösungen, veränderte Prozessabläufe) oder Veränderungen in ihrem Umfeld (z.B. sicherheitspolitische Lage, veränderte Gerichtspraxis, Bedrohung durch Computerviren) spezifisch Rechnung tragen zu können. 92

Um im Rahmen eines institutsspezifischen Ansatzes verwendet werden zu dürfen, müssen für die Faktoren des Geschäftsumfelds und des internen Kontrollsysteems die folgenden Anforderungen erfüllt sein: 93

- Jeder Faktor muss gemäss Erfahrungen und der Beurteilung aus dem betroffenen Geschäftsbereich ein relevanter Risikotreiber sein. Idealerweise sollte der Faktor quantifizierbar und verifizierbar sein. 94
- Die Sensitivität der Risikoschätzungen einer Bank in Bezug auf Veränderungen der Faktoren und ihrer relativen Bedeutung muss begründet werden können und nachvollziehbar sein. Neben möglichen Veränderungen des Risikoprofils durch Verbesserungen der Kontrollumgebung muss das Konzept insbesondere auch potenzielle Erhöhungen der Risiken durch wachsende Komplexität oder durch Wachstum der Geschäftsaktivitäten erfassen. 95
- Das Konzept an sich sowie die Auswahl und Anwendung der einzelnen Faktoren, inklusive der Grundprinzipien zu Anpassungen der empirischen Schätzungen, müssen dokumentiert sein. Die Dokumentation soll auch innerhalb der Bank Gegenstand unabhängiger Überprüfung sein. 96
- Die Prozesse, deren Ergebnisse und vorgenommene Anpassungen sind in regelmässigen Zeitabständen mit den effektiven internen und externen Verlusterfahrungen zu vergleichen. 97

h) Risikoverminderung durch Versicherungen

Bei Verwendung eines institutsspezifischen Ansatzes dürfen Banken die Risiko vermindernde Wirkung von Versicherungskontrakten bei der Bestimmung ihrer Eigenmittelanforderungen für operationelle Risiken berücksichtigen. Die Anerkennung solcher Absicherungswirkungen ist jedoch auf eine Reduktion von maximal 20 % der mittels eines institutsspezifischen Ansatzes berechneten Eigenmittelanforderungen beschränkt. 98

Die Möglichkeiten zur Reduktion der Eigenmittelanforderungen ist an die Erfüllung der folgenden Bedingungen geknüpft: 99

- Der Versicherungsgeber verfügt über ein langfristiges Kreditrating der Ratingklasse 3 oder besser. Das Kreditrating muss von einer durch die FINMA anerkannten Ratingagentur stammen. 100
- Der Versicherungskontrakt muss über eine Ursprungslaufzeit von mindestens einem Jahr 101

verfügen. Sinkt seine Restlaufzeit auf unter ein Jahr, ist die Anerkennung seiner Absicherungswirkung linear von 100 % (bei mindestens 365 Tagen Restlaufzeit) auf 0 % (bei 90 Tagen Restlaufzeit) zu reduzieren. Absicherungswirkungen aus Versicherungskontrakten mit einer Restlaufzeit von 90 Tagen oder weniger werden für die Bestimmung der Eigenmittelanforderungen nicht anerkannt.

- Der Versicherungskontrakt verfügt über eine Kündigungsfrist von mindestens 90 Tagen. Die Anerkennung der Absicherungswirkung nimmt bei Kündigungsfristen von unter einem Jahr linear ab; von 100 % (bei einer Kündigungsfrist von mindestens 365 Tagen) bis zu 0 % (bei einer Kündigungsfrist von 90 Tagen). Die Sätze sind auf die allenfalls bereits durch Rz 101 reduzierten Absicherungswirkungen anzuwenden. 102
- Der Versicherungskontrakt darf keine Ausschlussklauseln oder Einschränkungen für den Fall einer regulatorischen Intervention oder einer Zahlungsunfähigkeit der betreffenden Bank beinhalten, welche die Bank, ihren allfälligen Käufer, den Sanierungsbeauftragten oder den Liquidator von Versicherungsleistungen ausschliessen könnten. Zulässig wären entsprechende Ausschlussklauseln oder Einschränkungen jedoch, falls sie sich ausschliesslich auf Ereignisse nach Eröffnung des Konkursverfahrens oder nach der Liquidation beschränken. 103
- Die Berechnung der Absicherungswirkung aus Versicherungskontrakten muss transparent sein. Sie muss konsistent sein mit der im institutsspezifischen Ansatz verwendeten Wahrscheinlichkeit und der Grösse eines potenziellen Verlustereignisses. 104
- Der Versicherungsgeber muss eine externe Partei sein und darf nicht zur gleichen Gruppe wie die Bank gehören. Sollte er dies tun, so sind die Absicherungswirkungen aus den Versicherungskontrakten nur dann anerkennungsfähig, wenn der Versicherungsgeber die Risiken seinerseits an eine unabhängige dritte Partei (z.B. eine Rückversicherungsgesellschaft) weitergibt. Für eine Anerkennung der Absicherungswirkung muss diese unabhängige dritte Partei ihrerseits sämtliche entsprechenden Anforderungen an einen Versicherungsgeber erfüllen. 105
- Das bankinterne Konzept zur Berücksichtigung von Versicherungslösungen muss sich am effektiven Risikotransfer orientieren. Es muss gut dokumentiert sein. 106
- Die Bank hat Informationen zur Verwendung von Versicherungslösungen mit dem Ziel einer Verminderung operationeller Risiken zu publizieren. 107

D. Partielle Anwendung von Ansätzen

Es ist grundsätzlich zulässig, die Anwendung eines institutsspezifischen Ansatzes auf einzelne Aktivitätsbereiche zu beschränken und die übrigen entweder durch den Basisindikator- oder den Standardansatz abzudecken. Voraussetzung dazu ist die Erfüllung der folgenden Bedingungen:

- Sämtliche operationellen Risiken einer Bank werden durch einen in diesem Rundschreiben aufgeführten Ansatz erfasst. Dabei sind die jeweiligen Anforderungen für diese An-

sätze in den entsprechenden Aktivitätsbereichen zu erfüllen.

- Zum Zeitpunkt der Anwendung eines institutsspezifischen Ansatzes hat dieser einen wesentlichen Teil der operationellen Risiken der Bank zu erfassen. 110
 - Die Bank muss über einen Zeitplan verfügen, aus dem sich der zeitliche Ablauf der Ausdehnung des institutsspezifischen Ansatzes auf all ihre materiellen rechtlichen Einheiten und Geschäftsfelder ergibt. 111
 - Es ist nicht zulässig, den Basisindikator- oder den Standardansatz in einzelnen materiellen Aktivitätsbereichen aus Gründen der Minimierung von Eigenmittelanforderungen beizubehalten. 112
- Die Abgrenzung zwischen dem institutsspezifischen Ansatz und dem Basisindikator- bzw. dem Standardansatz kann sich an Geschäftsfeldern, rechtlichen Strukturen, geographischen Abgrenzungen oder anderen intern klar definierten Abgrenzungskriterien orientieren. 113
- Abgesehen von den in Rz 108–113 genannten Fällen ist es nicht zulässig, die Eigenmittelanforderungen für operationelle Risiken in einer Bank unter Verwendung unterschiedlicher Ansätze zu bestimmen. 114

E. Anpassungen der Eigenmittelanforderungen (Art. 45 ERV)

Im Rahmen ihrer Überwachungsfunktionen betreffend zusätzliche Eigenmittel (Art. 45 ERV) kann die FINMA die Eigenmittelanforderungen für einzelne Banken individuell erhöhen. Solche individuellen Erhöhungen der Eigenmittelanforderungen drängen sich insbesondere dann auf, wenn eine ausschliesslich auf den Basisindikator- oder den Standardansatz gestützte Bestimmung der Eigenmittelanforderungen auf Grund tiefer Ertragsindikatoren GI zu unangemessen geringen Eigenmittelanforderungen führen würde. 115

F. Mindesteigenmittel und Untergrenze (*Floor*)

In Anwendung der vom Basler Ausschuss publizierten Fortführung des „*Floor-Regimes*“ gilt:⁴ Für Banken, die operationelle Risiken nach dem AMA unterlegen, dürfen auf Gesamtbankstufe die Mindesteigenmittelanforderungen, unter zusätzlicher Berücksichtigung von Abzügen von den anrechenbaren Eigenmitteln, nicht tiefer als 80 % jener Anforderungen und Abzüge betragen, welche die Bank theoretisch unter dem Mindeststandard von Basel I gehabt hätte.⁵ In Anwendung von Art. 47 ERV bestimmt die FINMA im institutsspezifischen Einzelfall, wie eine angemessene approximative Berechnung der theoretischen Basel I-Anforderungen vorgenommen werden kann. Für operationelle Risiken orientiert sie sich am Standardansatz gemäss Art. 93 ERV. 116*

⁴ Vgl. Pressemitteilung des Basler Ausschusses vom 13. Juli 2009: www.bis.org/press/p090713.htm.

⁵ Dies entspräche der Berechnung der Eigenmittelanforderungen nach der bis 31.12.2006 gültigen Bankenverordnung vom 17. Mai 1972 (AS 1995 253, AS 1998 16).

IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken

A. Proportionalitätsprinzip

Die Anforderungen dieses Kapitels gelten grundsätzlich für alle Adressaten dieses Rundschreibens. Die Anforderungen dieses Kapitels sind jedoch im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. Die Rz 119 listet die Randziffern auf, von deren Umsetzung kleine Institute gänzlich ausgenommen sind.

117*

Kleine Institute im Sinne der Rz 117 sind Banken und Effektenhändler der FINMA-Kategorien⁶ 4 und 5. Die FINMA kann im Einzelfall Erleichterungen oder Verschärfungen anordnen.

118*

B. Qualitative Grundanforderungen

Kleine Institute gemäss Rz 117 und 118 sind von der Erfüllung von Rz 129 und 132–134 ausgenommen.

119*

Die qualitativen Grundanforderungen basieren auf den „Principles for the Sound Management of Operational Risk“ des Basel Committee on Banking Supervision (Juni 2011).⁷

120*

a) Grundsatz 1: Kategorisierung und Klassifizierung von operationellen Risiken

Die operationellen Risiken sind zur Gewährleistung der Konsistenz im Rahmen der Risikoidentifikation, der Risikobeurteilung und der Zielsetzung im operativen Risikomanagement einheitlich zu kategorisieren⁹.

121*

Die einheitliche Klassifizierung der operationellen Risiken erfolgt auf Basis der Kategorisierung der operationellen Risiken gemäss Rz 121 und umfasst eine Beurteilung sowohl der inhärenten Risiken¹⁰ als auch der Residualrisiken¹¹. Typischerweise erfolgt die Beurteilung entlang den Dimensionen „Eintrittswahrscheinlichkeit“ und „Schadensausmass“. Die Klassifizierung dient insbesondere auch der Bestimmung der Risiken mit weitreichender Tragweite im Sinne von Rz 137.

122*

Aufgehoben

123*

Aufgehoben

124*

⁶ Vgl. den Anhang im FINMA-RS 11/2 „Eigenmittelpuffer und Kapitalplanung Banken“.

⁷ www.bis.org/publ/bcbs195.pdf

⁹ Diese einheitliche Kategorisierung kann in Anlehnung an Anhang 2 dieses Rundschreibens oder mittels einer internen Terminologie oder Taxonomie erfolgen.

¹⁰ Vgl. Anhang 3, Rz 59

¹¹ Vgl. Anhang 3, Rz 60.

b) Aufgehoben

Aufgehoben	125*
Aufgehoben	126*
Aufgehoben	127*

c) Grundsatz 2: Identifizierung, Begrenzung und Überwachung

Eine wirksame Risikoidentifikation, welche die Grundlage für die Begrenzung und Überwachung der operationellen Risiken bildet, berücksichtigt sowohl interne¹² als auch externe¹³ Faktoren. Hierzu gehören mindestens Risiko- und Kontrollbeurteilungen sowie Revisionsergebnisse.

In Abhängigkeit von den institutsspezifischen Geschäftsaktivitäten und deren Art, Umfang, Komplexität und Risikogehalt, ist die Berücksichtigung weiterer Instrumente und Methoden zu prüfen und sind diese gegebenenfalls anzuwenden:

- a. Erhebung und Analyse interner Verlustdaten;
- b. Erhebung und Analyse externer Ereignisse, die mit operationellen Risiken verbunden sind;
- c. Analyse der Zusammenhänge zwischen Risiken, Prozessen und Kontrollen;
- d. Risiko- und Performance-Indikatoren für die Überwachung von operationellen Risiken und Indikatoren für die Wirksamkeit des internen Kontrollsystems;
- e. Szenarioanalysen;
- f. Abschätzung des Verlustpotenzials;
- g. Vergleichende Analysen¹⁴.

Die Begrenzung und Überwachung erfolgt mittels der im Rahmenkonzept für das institutsweite Risikomanagement gemäss dem FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken“ definierten Instrumente, Strukturen, Ansätze usw. von den hierfür vorgesehenen Organisationseinheiten.

d) Grundsatz 3: Interne und externe Berichterstattung

Aufgehoben	131*
------------	------

¹² Beispielsweise Unternehmensstruktur, Art der Aktivitäten, Qualifikationen der Mitarbeitenden, organisatorische Veränderungen und Personalfluktuation einer Bank.

¹³ Beispielsweise Veränderungen des weiteren Umfelds und der Branche sowie technologische Fortschritte.

¹⁴ Bei einer vergleichenden Analyse werden die Resultate der verschiedenen Beurteilungsinstrumente verglichen, um sich ein umfassenderes Bild der operationellen Risiken der Bank zu verschaffen.

Die interne Berichterstattung über operationelle Risiken muss sowohl Finanz-, Betriebs- und Compliance-Daten, aber auch wesentliche risikorelevante externe Informationen über Ereignisse und Bedingungen umfassen. Die Berichterstattung über operationelle Risiken muss dabei mindestens folgende Punkte abdecken und deren mögliche Auswirkungen auf das Institut und das für die operationellen Risiken erforderliche Eigenkapital darstellen:	132*
a. Wesentliche Verstöße gegen die in Bezug auf die inhärenten und Residualrisiken definierte Risikotoleranz des Instituts sowie Überschreitungen von diesbezüglich festgesetzten Risikobegrenzungen;	132.1*
b. Einzelheiten zu wesentlichen internen operationellen Risikoereignissen und/oder Verlusten;	132.2*
c. Informationen zu externen Ereignissen, welche für das Institut relevant sein können, und potentiellen Risiken sowie deren mögliche Auswirkungen auf das Institut.	132.3*
Ein Institut muss über eine formelle, vom Oberleitungsorgan genehmigte Offenlegungspolitik verfügen, aus der hervorgeht, wie die Bank ihre operationellen Risiken offenlegt und welche Kontrollprozesse bezüglich der Offenlegung anzuwenden sind.	133*
Von den Instituten extern offen zu legende Informationen müssen es den Anspruchsgruppen erlauben, sich ein Urteil über den Ansatz zum Management von operationellen Risiken zu bilden. Hierzu gehört u.a. das Konzept für das Management operationeller Risiken. Dieses muss den Anspruchsgruppen eine Beurteilung der Wirksamkeit der Identifikation, Begrenzung und Überwachung der operationellen Risiken ermöglichen.	134*
e) Grundsatz 4: Technologieinfrastruktur¹⁵	
Die Geschäftsleitung hat ein IT-Risikomanagement-Konzept in Übereinstimmung mit der IT-Strategie und der definierten Risikotoleranz sowie unter Berücksichtigung von für das jeweilige Institut relevanten Aspekten gemäss international anerkannten Standards zu implementieren.	135*
Die Geschäftsleitung stellt dabei sicher, dass das IT-Risikomanagement-Konzept die folgenden minimalen Aspekte beinhaltet:	135.1*
a. Aktuelle Übersicht über die wesentlichsten Bestandteile der Netzwerkinfrastruktur und ein Inventar aller kritischen Applikationen und der damit verbundenen IT-Infrastruktur sowie Schnittstellen mit Dritten,	135.2*
b. Eindeutige Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf die kritischen Applikationen sowie damit verbundener IT-Infrastruktur und kritischen und/oder sensiblen Daten und Prozesse,	135.3*

¹⁵ Technologieinfrastruktur bezeichnet den physischen und logischen (elektronischen) Aufbau von IT- und Kommunikationssystemen, die einzelnen Hard- und Softwarekomponenten, die Daten und die Betriebsumgebung.

c.	Systematischer Prozess im Hinblick auf die Identifikation und Beurteilung von IT-Risiken im Rahmen der Sorgfalsprüfung (Due Diligence) insbesondere bei Akquisitionen bzw. Auslagerungen im IT-Bereich sowie bei der Überwachung von Dienstleistungsvereinbarungen,	135.4*
d.	Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Verantwortung zur Reduktion von IT-Risiken sowie Einhaltung und Stärkung der IT-Informationssicherheit.	135.5*
Die Geschäftsleitung hat zudem ein Risikomanagement-Konzept für den Umgang mit Cyber-Risiken¹⁷ zu implementieren. Dieses Konzept hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch geeignete Prozesse sowie eine eindeutige Festlegung von Aufgaben, Rollen und Verantwortlichkeiten zu gewährleisten:		
a.	Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken ¹⁹ , insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme,	135.7*
b.	Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensiblen Daten und IT-Systeme,	135.8*
c.	Zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken auf Basis eines Prozesses zur systematischen Überwachung der Technologieinfrastruktur,	135.9*
d.	Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyber-Attacken in Abstimmung mit dem BCM, und	135.10*
e.	Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen.	135.11*
Die Geschäftsleitung lässt zum Schutz der kritischen und/oder sensiblen Daten und IT-Systemen vor Cyber-Attacken regelmässig Verwundbarkeitsanalysen²⁰ und <i>Penetration Testing</i>²¹ durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen durchgeführt werden.		

¹⁷ Operationelle Risiken in Bezug auf mögliche Verluste durch Cyber-Attacken.

¹⁹ Sind Angriffe aus dem Internet und vergleichbaren Netzen, auf die Integrität, die Verfügbarkeit und die Vertraulichkeit der Technologieinfrastruktur, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme.

²⁰ Analyse zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken.

²¹ Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der Technologieinfrastruktur, um unberechtigten Zugang zu dieser Technologieinfrastruktur zu erhalten.

f) Grundsatz 5: Kontinuität bei Geschäftsunterbrechung	136
Die Geschäftsleitung hat über Pläne zur Fortführung der Geschäfte des Instituts zu verfügen, welche die Kontinuität der Tätigkeiten und die Schadensbegrenzung im Falle einer schwerwiegenden Geschäftsunterbrechung gewährleisten. ²²	136
g) Grundsatz 6: Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken	136.1*
Systemrelevante Banken treffen im Rahmen ihrer Notfallplanung die für die unterbruchsfreie Weiterführung von systemrelevanten Funktionen nötigen Massnahmen (Art. 9 Abs. 2 Bst. d BankG i.V.m. Art. 60 ff. BankV). Sie identifizieren die zur Fortführung der systemrelevanten Funktionen im Fall der Abwicklung, Sanierung oder Restrukturierung notwendigen Dienstleistungen („kritische Dienstleistungen“) und ergreifen die für deren Weiterführung nötigen Massnahmen. Dabei berücksichtigen sie die von internationalen Standardsettern erlassenen Vorgaben in diesem Zusammenhang.	136.1*
h) Grundsatz 7: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft	136.2*
Wenn Institute oder ihre Gruppengesellschaften grenzüberschreitend Finanzdienstleistungen erbringen oder Finanzprodukte vertreiben, sind auch die aus einer Anwendung ausländischer Rechtsvorschriften (Steuer-, Straf-, Geldwäschereirecht usw.) resultierenden Risiken angemessen zu erfassen, begrenzen und kontrollieren. Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Institute ausländisches Aufsichtsrecht einhalten.	136.2*
Die Institute unterziehen ihr grenzüberschreitendes Finanzdienstleistungsgeschäft sowie den grenzüberschreitenden Vertrieb von Finanzprodukten einer vertieften Analyse der rechtlichen Rahmenbedingungen und der damit verbundenen Risiken. Gestützt auf diese Analyse treffen die Institute die erforderlichen strategischen und organisatorischen Massnahmen zur Risikoeliminierung -minimierung und passen diese laufend geänderten Bedingungen an. Insbesondere verfügen sie über das notwendige länderspezifische Fachwissen, definieren sie spezifische Dienstleistungsmodelle für die bedienten Länder, schulen die Mitarbeiter und stellen durch entsprechende organisatorische Massnahmen, Weisungen, Vergütungs- und Sanktionsmodelle die Einhaltung der Vorgaben sicher.	136.3*
Auch die durch externe Vermögensverwalter, Vermittler und andere Dienstleister generierten Risiken sind zu berücksichtigen. Entsprechend ist bei der Auswahl und Instruktion dieser Partner sorgfältig vorzugehen.	136.4*
Von diesem Grundsatz werden auch Konstellationen erfasst, in denen eine im Ausland ansässige Tochtergesellschaft, Zweigniederlassung oder dergleichen eines Schweizer Finanzinstituts Kunden grenzüberschreitend bedient.	136.5*

²² Vgl. die im FINMA-Rundschreiben 2008/10 „Selbstregulierung als Mindeststandard“ als Mindeststandard anerkannten Ziffern der SBVg-Empfehlungen für das *Business Continuity Management* (BCM).

C. Risikospezifische qualitative Anforderungen

Die Steuerung und Kontrolle spezifischer operationeller Risiken mit weitreichender Tragweite hat umfassender und intensiver zu erfolgen als dies in den qualitativen Grundanforderungen vorgegeben ist. Die Geschäftsleitung hat hierfür ergänzende risikospezifische Massnahmen oder eine Verschärfung bestehender Massnahmen situativ zu bestimmen und umzusetzen.

137*

Falls die FINMA es als notwendig erachtet, kann sie für spezifische Themen weitergehende Konkretisierungen an das Management von operationellen Risiken definieren. Dies geschieht zurückhaltend und unter Anwendung des Proportionalitätsprinzips. Weitergehende qualitative Anforderungen werden thematisch sortiert im Anhang zum Rundschreiben veröffentlicht.

138*

V. Prüfung und Beurteilung durch die Prüfgesellschaften

Die Prüfgesellschaften prüfen die Einhaltung dieses Rundschreibens nach Massgabe des FINMA-RS 13/3 „Prüfwesen“ und halten das Ergebnis ihrer Prüfungshandlungen im Prüfbericht fest.

139*

Anhang 1



Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

I. Übersicht

1

1. Ebene	2. Ebene	Aktivitäten
Unternehmens-finanzierung/-beratung	Unternehmensfinanzie- rung/-beratung	Fusionen und Übernahmen, Emissions- und Platzierungsgeschäfte, Privatisierungen, Verbriefungen, Research, Kredite (öffentliche Haushalte, <i>High-Yield</i>), Beteiligungen, Syndizierungen, Börsengänge (<i>Initial Public Offerings</i>), Privatplatzierungen im Sekundärhandel
	Öffentliche Haushalte	
	Handelsfinanzierungen	
	Beratungsdienstleis- tungen	
Handel	Kundenhandel	Anleihen, Aktien, Devisengeschäfte, Rohstoffgeschäfte, Kredite, Derivate, <i>Funding</i> , Eigenhandel, Wertpapierleihe und Repos, <i>Brokerage</i> (für Nicht-Retail-Investoren), <i>Prime Brokerage</i>
	<i>Market Making</i>	
	Eigenhandel	
	<i>Treasury</i>	
Privatkundengeschäft	Retail Banking	Anlage- und Kreditgeschäft, Serviceleistungen, Treuhandgeschäfte und Anlageberatung
	Private Banking	Anlage- und Kreditgeschäft, Serviceleistungen, Treuhandgeschäfte, Anlageberatung und andere Private-Banking-Dienstleistungen
	Karten- Dienstleistungen	Karten für Firmen und Privatpersonen
Firmenkundengeschäft	Firmenkundengeschäft	Projektfinanzierung, Immobilienfinanzierung, Exportfinanzierung, Handelsfinanzierung, <i>Factoring</i> , Leasing, Kreditgewährungen, Garantien und Bürgschaften, Wechselgeschäft
Zahlungsverkehr/Wertschriftenabwicklung ²³	Externe Kunden	Zahlungsverkehr, Clearing und Wertpapierabwicklung für Drittparteien
Depot- und Treuhand- geschäfte	Custody	Treuhandverwahrung, Depotgeschäft, <i>Custody</i> , Wertpapierleihe für Kunden; ähnliche Dienstleistungen für Firmen
	Treuhandgeschäft	Emissions- und Zahlstellenfunktionen
	Unternehmens- stiftungen	
Institutionelle Vermö- gensverwaltung	Freie Vermögensver- waltung	Im Pool, segmentiert, Retail-bezogen, institu- tionell, geschlossen, offen, <i>Private Equity</i>

²³ Verluste aus dem Bereich Zahlungsverkehr und Wertpapierabwicklung, die eigene Aktivitäten eines Institutes betreffen, sind jeweils dem entsprechenden Geschäftsfeld zuzuordnen.

Anhang 1



Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

	Gebundene Vermögensverwaltung	Im Pool, segmentiert, Retail-bezogen, individuell, privat, institutionell, geschlossen, offen
Wertpapierprovisionsgeschäft	Ausführung von Wertschriftenaufträgen	Ausführung, inkl. sämtlicher damit verbundenen Dienstleistungen

II. Grundsätze für die Allokation

1. Sämtliche Aktivitäten einer Bank müssen vollständig einem der acht Geschäftsfelder (1. Ebene in Tabelle 2) zugeordnet werden. Die Zuordnung darf nicht zu Überschneidungen führen. 2
2. Auch jene Tätigkeiten, die nicht direkt mit dem eigentlichen Geschäft einer Bank zusammenhängen, sondern unterstützenden Charakter haben, sind einem Geschäftsfeld zuzuordnen. Falls die Unterstützung ein Geschäftsfeld betrifft, erfolgt auch die Zuordnung zu diesem Geschäftsfeld. Sind mehrere Geschäftsfelder durch eine unterstützende Aktivität betroffen, hat die Zuordnung gestützt auf objektive Kriterien zu erfolgen. 3
3. Kann eine Aktivität nicht auf Grund objektiver Kriterien in ein bestimmtes Geschäftsfeld kategorisiert werden, so ist sie innerhalb der relevanten Geschäftsfelder jenem mit dem höchsten β -Faktor zuzuordnen. Dies gilt auch für die Aktivitäten mit Unterstützungscharakter. 4
4. Banken dürfen für die Allokation ihres Ertragsindikators GI interne Verrechnungsmethoden anwenden. In jedem Fall muss jedoch die Summe der Ertragsindikatoren aus den acht Geschäftsfeldern dem Ertragsindikator für die gesamte Bank – wie er im Basisindikatoransatz verwendet wird – entsprechen. 5
5. Die Kategorisierung von Aktivitäten in die verschiedenen Geschäftsfelder für die Bestimmung der Eigenmittelanforderungen für operationelle Risiken muss grundsätzlich mit den für Kredit- und Marktrisiken verwendeten Abgrenzungskriterien kompatibel sein. Allfällige Abweichungen von diesem Prinzip sind klar zu begründen und müssen dokumentiert sein. 6
6. Der gesamte Kategorisierungsprozess muss klar dokumentiert sein. Insbesondere haben die schriftlichen Definitionen der Geschäftsfelder ausreichend klar und detailliert genug sein, um auch von nicht mit der Bank vertrauten Personen nachvollzogen werden zu können. Wo Ausnahmen von den Grundsätzen der Kategorisierung möglich sind, müssen auch diese klar begründet und dokumentiert sein. 7
7. Die Bank muss über Verfahren verfügen, die ihr die Kategorisierung neuer Aktivitäten oder Produkte ermöglichen. 8
8. Die Geschäftsleitung ist für die Grundsätze der Kategorisierung verantwortlich. Diese sind durch das Organ für die Oberleitung, Aufsicht und Kontrolle der Bank zu genehmigen. 9
9. Die Verfahren der Kategorisierung sind regelmässig durch die Prüfgesellschaft zu überprüfen. 10

Anhang 2



Übersicht zur Kategorisierung von Ereignistypen

Verlustereigniskategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
Interner Betrug	Verluste auf Grund von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum, Umgehung von Gesetzen, Vorschriften oder internen Bestimmungen (unter Beteiligung mindestens einer internen Partei)	Unautorisierte Aktivität	Nicht rapportierte Transaktionen (vorsätzlich) Unautorisierte Transaktionen (mit finanziellem Schaden) Falscherfassung von Positionen (vorsätzlich)
		Diebstahl und Betrug	Betrug, Kreditbetrug, wertlose Einlagen Diebstahl, Erpressung, Veruntreuung, Raub Veruntreuung von Vermögenswerten Böswillige Vernichtung von Vermögenswerten Fälschungen Scheckbetrug Schmuggel Unbefugter Zugriff auf fremde Konten Steuerdelikte Bestechung Insidergeschäfte (nicht auf Rechnung des Arbeitgebers)
Externer Betrug	Verluste auf Grund von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum oder der Umgehung von Gesetzen bzw. Vorschriften (ohne Beteiligung einer internen Partei)	Diebstahl und Betrug	Diebstahl, Raub Fälschungen Scheckbetrug
		Informatiksicherheit	Schäden durch Hacker-Aktivitäten Unbefugter Zugriff auf Informationen (mit finanziellem Schaden)

Anhang 2



Übersicht zur Kategorisierung von Ereignistypen

Verlustereigniskategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
Arbeitsplatz	Verluste auf Grund von Widerhandlungen gegen arbeitsrechtliche, sicherheits- oder gesundheitsbezogene Vorschriften oder Vereinbarungen; inkl. aller Zahlungen im Zusammenhang mit solchen Widerhandlungen	Mitarbeiter	Kompensations- und Abfindungszahlungen, Verluste im Zusammenhang mit Streiks usw.
		Sicherheit am Arbeitsplatz	Allgemeine Haftpflicht Verstoss gegen sicherheits- oder gesundheitsbezogene Bestimmungen Entschädigungs- oder Schadenersatzzahlungen an Mitarbeiter
		Diskriminierung	Schadenersatzzahlungen auf Grund von Diskriminierungsklagen
Kunden, Produkte und Geschäftspraktiken	Verluste auf Grund unbeabsichtigter oder fahrlässiger Nichterfüllung von Verpflichtungen gegenüber Kunden sowie Verluste auf Grund der Art oder Struktur bestimmter Produkte	Angemessenheit, Offenlegung und Treuhandpflichten	Verstoss gegen Treuhandpflichten, Verletzung von Richtlinien Probleme bezüglich Angemessenheit und Offenlegung (Know-your-Customer-Regeln usw.) Verletzung von Informationspflichten gegenüber Kunden Verletzung des Bankkundengeheimnisses bzw. von Datenschutzbestimmungen Aggressive Verkaufspraktiken Inadäquate Generierung von Kommissions- und Courtagenzahlungen Missbrauch vertraulicher Informationen Haftung des Kreditgebers

Anhang 2



Übersicht zur Kategorisierung von Ereignistypen

Verlustereigniskategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
		Unzulässige Geschäfts- oder Marktpraktiken	Verstoss gegen kartellrechtliche Bestimmungen Unlautere Marktplatzpraktiken Marktmanipulationen Insidergeschäfte (auf Rechnung des Arbeitgebers) Geschäftstätigkeiten ohne entsprechende Bewilligung Geldwäscherei
		Probleme mit Produkten	Produktprobleme (Befugnismängel usw.) Modellfehler
		Kundenselektion, Geschäftsvergabe und Kreditexposition	Nicht mit internen Richtlinien kompatibles Vorgehen bei Kundenprüfungen Überschreitung von Limiten
		Beratungstätigkeiten	Streitigkeiten in Bezug auf Resultate von Beratungstätigkeiten
Sachschaden	Verluste auf Grund von Schäden an physischen Vermögenswerten infolge Naturkatastrophen oder anderer Ereignisse	Katastrophen oder andere Ereignisse	Naturkatastrophen Terrorismus Vandalismus
Geschäftsunterbrüche und Systemausfälle	Verluste auf Grund von Störungen der Geschäftstätigkeit oder Problemen mit technischen Systemen	Technische Systeme	Hardware Software Telekommunikation Stromausfälle usw.

Anhang 2



Übersicht zur Kategorisierung von Ereignistypen

Verlustereigniskategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
Abwicklung, Vertrieb und Prozessmanagement	Verluste auf Grund von Fehlern bei der Geschäftsabwicklung oder beim Prozessmanagement; Verluste aus Beziehungen mit Geschäftspartnern, Lieferanten usw.	Erfassung, Abwicklung und Betreuung von Transaktionen	Kommunikationsfehler Fehler bei der Datenerfassung oder im Datenunterhalt Terminüberschreitung Nichterfüllung einer Aufgabe Fehler bei Modell- oder Systemanwendung Buchhaltungsfehler bzw. Zuordnung zur falschen Einheit Fehlerhafte bzw. nichterfolgte Lieferung Fehlerhafte Bewirtschaftung von Absicherungsinstrumenten Fehler im Umgang mit Referenzdaten Fehler bei übrigen Aufgaben
		Überwachung und Meldungen	Nichterfüllung von Meldepflichten Inadäquate Berichte an Externe (mit Verlustfolge)
		Kundenaufnahme und Kundendokumentation	Nichteinhaltung entsprechender interner und externer Vorgaben
		Kontoführung für Kunden	Gewährung eines nichtlegitimierten Kontozugriffs Unkorrekte Kontoführung mit Verlustfolge Verlust oder Beschädigung von Kundenvermögenswerten durch fahrlässige Handlungen

Anhang 2



Übersicht zur Kategorisierung von Ereignistypen

Verlustereigniskategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
		Geschäftspartner	Fehlerhafte Leistung von Geschäftspartnern (Nichtkunden) Verschiedene Streitigkeiten mit Geschäftspartnern (Nichtkunden)
		Lieferanten und Anbieter	Outsourcing Streitigkeiten mit Lieferanten und Anbietern

Anhang 3*



Umgang mit elektronischen Kundendaten

In diesem Anhang werden die Grundsätze und die dazugehörigen Ausführungen für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen („Privatkunden“²⁴), deren Geschäftsbeziehungen in oder von der Schweiz aus betreut oder geführt werden („Kundendaten“), formuliert. Die Grundsätze sind hauptsächlich auf das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von Kundendaten durch Verwendung elektronischer Systeme zugeschnitten. Sie gehen nur am Rande auf Sicherheitsüberlegungen für physische Daten sowie auf Fragen der Integrität und Verfügbarkeit von Daten ein. Die einschlägigen rechtlichen Bestimmungen finden sich nicht nur im Aufsichtsrecht²⁵, sondern auch im Datenschutzrecht²⁶ und Zivilrecht.

1*

Kleine Banken²⁷ sind von der Erfüllung folgender Randziffern ausgenommen:

2*

- Rz 15, 17–19 sowie 22 des Grundsatzes 3;
- Alle Randziffern der Grundsätze 4–6;
- Rz 41 des Grundsatzes 7.

I. Grundsätze für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten

A. Grundsatz 1: Governance

Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten werden systematisch identifiziert, begrenzt und überwacht. Dazu überwacht das Oberleitungsorgan die Geschäftsleitung zur Sicherstellung einer wirksamen Implementierung von Massnahmen zur Gewährleistung der Vertraulichkeit von Kundendaten. Die Geschäftsleitung beauftragt eine unabhängige Einheit als Kontrollfunktion, die Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zu schaffen und aufrechtzuerhalten.

3*

a) Unabhängigkeit und Verantwortung

Die für die Schaffung und Aufrechterhaltung der Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zuständige Einheit muss unabhängig von jenen Einheiten sein, welche für die Verarbeitung der Daten zuständig sind.

4*

Für alle beteiligten Funktionen und Standorte müssen die Verantwortlichkeiten geregelt sein und klare Eskalationsstrukturen geschaffen werden. Insbesondere die Festlegung der Verantwortlichkeiten und ihre Zuteilung an Front-Office-, IT- und Kontrollfunktionen sind von der Geschäftsleitung zu definieren und vom Oberleitungsorgan zu genehmigen. Die Geschäftsleitung infor-

5*

²⁴ Unter „Privatkunden“ werden auch solche Geschäftsbeziehungen verstanden, bei denen die natürliche Person mittels einer juristischen Person (z.B. als wirtschaftlich Berechtigter einer Sitzgesellschaft, Domizilgesellschaft, Stiftung) oder Trust eine Geschäftsbeziehung mit der Bank eingeht.

²⁵ Insbesondere Art. 3 und 47 BankG sowie Art. 12 BankV; Art. 10 und 43 BEHG sowie Art. 19 f. BEHV.

²⁶ Insbesondere Art. 7 DSG sowie Art. 8 ff. VDSG (vgl. dazu auch die Leitfäden des EDÖB; abrufbar unter www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de).

²⁷ Vgl. Rz 118

Anhang 3*



Umgang mit elektronischen Kundendaten

miert das Oberleitungsorgan regelmässig über die Wirksamkeit der eingeführten Kontrollen.

b) Vorgaben, Prozesse und Systeme

Es wird vorausgesetzt, dass ein formales und umfassendes Rahmenkonzept von Aktivitäten, Prozessen und Systemen zur Datenvertraulichkeit besteht, dessen Struktur der Grösse und Komplexität der Bank Rechnung trägt. Dieses Rahmenkonzept muss in allen Funktionsbereichen und Einheiten, die auf Kundendaten zugreifen oder diese bearbeiten, konsistent umgesetzt werden.

Die Massnahmen und die Periodizität deren Durchführung sind aufgrund der von der Bank festgelegten Risikotoleranz schriftlich, nachvollziehbar und verbindlich festzulegen.

Die Implementierung und Einhaltung des Rahmenkonzepts zur Vertraulichkeit von Kundendaten ist durch das Oberleitungsorgan zu überwachen und muss durch regelmässige Kontrollen der für Datensicherheit und -vertraulichkeit zuständigen Einheit sichergestellt werden.

B. Grundsatz 2: Kundenidentifikationsdaten (*Client Identifying Data, CID*)

Grundlegende Anforderung für ein angemessenes Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten ist die Kategorisierung der Kundendaten, die eine Bank verarbeitet. Dies erfordert die unternehmensspezifische Festlegung von Kundenidentifikationsdaten (CID) und deren Klassifizierung bzgl. ihrer Vertraulichkeits- und Schutzstufe. Zudem muss die Zuordnung der Datenverantwortung (*Data Owners*) geregelt sein.

a) Kundendatenkategorien und CID-Definition

Eine klare und transparente Liste der Kundendatenkategorien, einschliesslich der unternehmensspezifischen Festlegung von CID, muss in der Bank vorliegen und formell dokumentiert werden. Die Kategorisierung und Definition von Kundendaten hat sämtliche direkten Kundenidentifikationsdaten (z.B. Vorname, zweiter Name, Nachname), indirekten Kundenidentifikationsdaten (z.B. Passnummer) und potenziell indirekten Kundenidentifikationsdaten (z.B. Kombinationen aus Geburtsdatum, Beruf, Staatsangehörigkeit usw.) zu umfassen.

Jede Bank muss über eine Kategorisierung und unternehmensspezifische Festlegung von CID verfügen, die ihrem spezifischen Kundenstamm angemessen ist.

b) CID-Klassifizierung und Vertraulichkeitsstufen

CID müssen nach formalen Klassifizierungskriterien in Vertraulichkeitsstufen zugeordnet werden. Die Kundendatenklassifizierung hat zum Schutz der Vertraulichkeit klare Anforderungen für den Zugriff und entsprechende technische Massnahmen zu enthalten (z.B. Anonymisierung, Verschlüsselung oder Pseudonymisierung) und grundsätzlich zwischen verschiedenen Vertraulichkeits- und Schutzstufen zu unterscheiden.

c) CID-Verantwortung

Es müssen Kriterien für die Zuordnung der Datenverantwortung festgelegt werden, die gleich-

6*

7*

8*

9*

10*

11*

12*

13*

Anhang 3*



Umgang mit elektronischen Kundendaten

ermassen für alle Einheiten gelten, die auf CID zugreifen oder diese verarbeiten. Die für CID verantwortlichen Einheiten (*Data Owners*) müssen die Überwachung des gesamten Lebenszyklus der Kundendaten abdecken, einschliesslich der Genehmigung der Zugriffsrechte sowie des Löschens und Entsorgens von allen Backup- und operationellen Systemen.

Die für CID verantwortlichen Einheiten (*Data Owners*) sind für die Implementierung der Datenklassifizierungsrichtlinien sowie die Rechtfertigung und Dokumentierung von Ausnahmen zuständig.

14*

C. Grundsatz 3: Datenspeicherort und -zugriff

Die Bank muss wissen, wo CID gespeichert werden, von welchen Anwendungen und IT-Systemen CID verarbeitet werden und wo elektronisch auf sie zugegriffen werden kann. Mittels angemessenen Kontrollen ist sicherzustellen, dass die Daten nach Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz bearbeitet werden. Für physische Bereiche (z.B. Serverräume) oder Netzwerkzonen, in denen grosse Mengen an CID gespeichert oder zugänglich gemacht werden, sind spezielle Kontrollen erforderlich. Der Datenzugriff muss klar geregelt werden und darf nur auf einer strikten *Need to know*-Basis erfolgen.

15*

a) Datenspeicherort und -zugriff allgemein

Ein Inventar der Applikationen und der damit verbundenen Infrastruktur, die CID enthalten oder verarbeiten, muss verfügbar sein und laufend aktualisiert werden. Die Aktualisierung des Inventars hat insbesondere bei strukturellen Änderungen (z.B. neue Standorte oder Erneuerung der technischen Infrastruktur) zeitnah zu erfolgen. Änderungen von geringer Tragweite sind regelmässig nachzuführen.

16*

Es wird vorausgesetzt, dass die Granularität des Inventars der Bank erlaubt zu ermitteln:

17*

- wo CID gespeichert sind, durch welche Anwendungen und IT-Systeme CID verarbeitet werden und wo elektronisch auf CID zugegriffen werden kann (Endbenutzeranwendungen);
- von welchen nationalen und internationalen Standorten und Rechtseinheiten aus auf Daten zugegriffen werden kann (einschliesslich ausgelagerter Dienstleistungen und externer Firmen).

18*

19*

b) Datenspeicherort und -zugriff im Ausland

Falls CID ausserhalb der Schweiz gespeichert werden oder vom Ausland aus auf sie zugegriffen wird, sind die damit verbundenen erhöhten Risiken in Bezug auf den Kundendatenschutz angemessen zu begrenzen.²⁸ CID müssen angemessen geschützt (z.B. anonymisiert, verschlüsselt oder pseudonymisiert) werden.

20*

²⁸ Zudem sind die einschlägigen Bestimmungen des Datenschutzrechts einzuhalten, wie Art. 6 DSG.

Anhang 3*



Umgang mit elektronischen Kundendaten

c) Need to know-Grundsatz

Personen dürfen nur auf diejenigen Informationen oder Funktionalitäten Zugriff haben, die für die Wahrnehmung ihrer Aufgaben erforderlich sind. 21*

d) Zugriffsberechtigung

Die Bank hat über ein rollen- und funktionsspezifisches Autorisierungssystem zu verfügen, welches die Zugriffsberechtigungen von Mitarbeitenden und Dritten auf CID eindeutig regelt. Um sicherzustellen, dass nur aktuell autorisierte Personen auf CID Zugriff haben, sind Berechtigungen regelmässig zu bestätigen. 22*

D. Grundsatz 4: Sicherheitsstandards für die Infrastruktur und die Technologie

Die zum Schutz der CID-Vertraulichkeit verwendeten Sicherheitsstandards für die Infrastruktur und Technologie müssen in Bezug auf die Komplexität der Bank sowie ihrer Risikoexposition angemessen sein und den Schutz von CID auf dem Endgerät (am Endpoint), von übertragenen und gespeicherten CID sicherstellen. Da die Informationstechnologien schnellen Änderungen unterliegen, ist die Entwicklung von Datensicherheitslösungen aufmerksam zu verfolgen. Lücken zwischen dem bestehenden internen Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten und der Marktpraxis sind regelmässig zu beurteilen. 23*

a) Sicherheitsstandards

Die Sicherheitsstandards müssen in Bezug auf die Grösse der Bank und den Grad der Komplexität seiner IT-Architektur angemessen sein. 24*

b) Sicherheitsstandards und Marktpraxis

Die Sicherheitsstandards bilden einen festen Bestandteil des Rahmenkonzepts zur Sicherstellung der Vertraulichkeit von Kundendaten. Es wird erwartet, dass sie regelmässig mit der Marktpraxis verglichen werden, um potenzielle Sicherheitslücken zu ermitteln. Auch externe Inputs in Form von unabhängigen Überprüfungen und Prüfberichte müssen berücksichtigt werden. 25*

c) Sicherheit bei Übertragung von CID und bei gespeicherten CID auf dem Endgerät (Endpoint)

Um die Vertraulichkeit von CID sicherzustellen, hat die Bank Schutzmassnahmen (z.B. Verschlüsselung) abzuwägen und diese soweit erforderlich auf den folgenden Ebenen umsetzen: 26*

a. Sicherheit von CID auf dem Endgerät bzw. am Endpoint (z.B. PCs, Notebooks, portable Datenspeicher und Mobilgeräte); 27*

b. Sicherheit bei Übertragung von CID (z.B. innerhalb eines Netzwerks oder zwischen verschiedenen Standorten); 28*

c. Sicherheit von gespeicherten CID (z.B. auf Servern, in Datenbanken oder auf Backup- 29*

Anhang 3*



Umgang mit elektronischen Kundendaten

Medien).

E. Grundsatz 5: Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben

Gut ausgebildete und verantwortungsbewusste Mitarbeitende sind für die Umsetzung erfolgreicher unternehmensweiter Massnahmen zum Schutz der Vertraulichkeit von Kundendaten zentral. Mitarbeitende, die auf CID zugreifen können, sind sorgfältig auszuwählen, zu schulen und zu überwachen. Dies gilt auch für Dritte, die im Auftrag der Bank auf CID zugreifen können. Erhöhte Sicherheitsanforderungen müssen für (hoch-)privilegierte IT-Benutzer (bspw. Systemadministratoren) und Anwender mit funktionalem Zugriff auf Massen-CID („Schlüsselmitarbeitenden“) gelten. Ihnen ist besondere Aufmerksamkeit zu schenken.

30*

a) Sorgfältige Auswahl der Mitarbeitenden

Mitarbeitende, die auf CID zugreifen können, sind sorgfältig auszuwählen. Insbesondere ist vor der Aufnahme der Tätigkeit zu überprüfen, ob der potentielle Mitarbeitende die Anforderungen für einen angemessenen Umgang mit CID erfüllt. Die Bank hat ferner vertraglich zu regeln wie die Auswahl von Mitarbeitenden durch Dritte, als auch die Bestimmung von Mitarbeitenden von Drittunternehmen, welche im Auftrag der Bank auf CID zugreifen können erfolgt, damit alle Mitarbeitenden einen vergleichbaren, sorgfältigen Auswahlprozess durchlaufen.

31*

b) Gezielte Schulungen der Mitarbeitenden

Interne und externe Mitarbeitende müssen im Rahmen gezielter Schulungen in Bezug auf die Kundendatensicherheit sensibilisiert werden.

32*

c) Sicherheitsanforderungen

Die Bank muss über klare Sicherheitsanforderungen für Mitarbeitende, die auf CID zugreifen, verfügen. Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind. Erhöhte Sicherheitsanforderungen müssen für (hoch-)privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff²⁹ auf Massen-CID („Schlüsselmitarbeitenden“) gelten.

33*

d) Liste von Schlüsselmitarbeitenden

Als Ergänzung zu den allgemeinen Anforderungen in Bezug auf Zugriffsberechtigungen für Mitarbeitende und Dritte (siehe Rz 22) wird von der Bank die Führung und laufende Aktualisierung einer Liste mit den Namen aller internen und externen (hoch-) privilegierten IT-Benutzer und Anwender (Schlüsselmitarbeitenden) erwartet, die Zugriff auf Massen-CID³⁰ haben und/oder deren Verantwortlichkeiten hinsichtlich der Kontrolle und Überwachung der Vertraulichkeit von Kundendaten übertragen wurden.

34*

²⁹ Bei erweiterten Zugriffsrechten wie z.B. die Abfrage und Extraktion/Migration von Massen-CID.

³⁰ Einzelabfragen mit eingegrenzten Zugriffsrechten (z.B. von Schaltermitarbeitern) fallen nicht unter den Begriff des Zugriffs auf Massen-CID.

Anhang 3*



Umgang mit elektronischen Kundendaten

Vorkehrungen, wie z.B. das Führen von Log-Dateien, sind einzuführen, um die Identifizierung von Benutzern, die auf Massen-CID zugreifen, zu ermöglichen. 35*

F. Grundsatz 6: Risikoidentifizierung und -kontrolle in Bezug auf die CID-Vertraulichkeit

Die für die Datensicherheit und -vertraulichkeit zuständige Einheit identifiziert und bewertet die inhärenten Risiken und die Residualrisiken betreffend die Vertraulichkeit von CID mithilfe eines strukturierten Prozesses. Dieser Prozess muss die Risikoszenarien³¹ in Bezug auf die CID-Vertraulichkeit umfassen, die für die Bank und die Definition der entsprechenden Schlüsselkontrollen relevant sind. Der Katalog der Schlüsselkontrollen in Bezug auf die Datenvertraulichkeit zur Gewährleistung des CID-Schutzes muss laufend auf Adäquanz geprüft und gegebenenfalls angepasst werden.

a) Risikobeurteilungsprozess

Die Beurteilung des mit der Vertraulichkeit von CID verbundenen inhärenten Risikos und Residualrisikos muss auf Basis eines strukturierten Prozesses und unter Einbezug der Geschäfts-, IT- und Kontrollfunktionen erfolgen. 37*

b) Risikoszenarien und Schlüsselkontrollen³²

Die Definition von Risikoszenarien und entsprechenden Schlüsselkontrollen in Bezug auf die Vertraulichkeit von CID muss der Risikoexposition sowie der Komplexität der Bank angemessen sein und regelmässig überarbeitet werden. 38*

G. Grundsatz 7: Risikominderung in Bezug auf die CID-Vertraulichkeit

Identifizierte Risiken müssen überwacht und angemessen minimiert werden. Dies gilt namentlich in Verbindung mit Datenbearbeitungsaktivitäten, bei denen grosse Mengen von CID verändert oder migriert werden müssen.³³ Bei strukturellen Veränderungen (z.B. bedeutende Reorganisationen) muss sich die Bank frühzeitig und vertieft mit Sicherheitsmassnahmen der Vertraulichkeit von CID befassen.

a) Produktionsumfeld, Datenbearbeitung in Verbindung mit Massen-CID

Die Datenbearbeitung, die im Produktionsumfeld mit nicht anonymisierten, nicht verschlüsselten und nicht pseudonymisierten Massen-CID durchgeführt wird, muss geeigneten Verfahren unter-

³¹ Auf der Grundlage einer Analyse schwerwiegender Vorfälle in Bezug auf die Datensicherheit, die in der eigenen Bank oder bei der Konkurrenz eingetreten sind, oder einer Beschreibung rein hypothetischer schwerwiegender Vorfälle.

³² Marktpрактиken zu Sicherheitsszenarien und damit verbundenen Schlüsselkontrollen sind umfassend durch die Schweizerische Bankiervereinigung unter dem Titel „Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association“ behandelt (verabschiedet im Oktober 2012).

³³ Dazu kommt es in der Regel bei der Weiterentwicklung, Veränderung oder Migration von Systemen infolge von Technologie-Upgrades oder organisatorischen Strukturierungen.

Anhang 3*



Umgang mit elektronischen Kundendaten

liegen (z.B. Vier-Augen-Prinzip oder Log-Dateien), einschliesslich der Benachrichtigung der für die Datensicherheit und -vertraulichkeit zuständigen Einheit.

b) Tests für die Entwicklung, Veränderungen und Migration von Systemen

Während der Entwicklung, Veränderung und Migration von Systemen müssen die CID angemessen vor dem Zugriff und der Nutzung durch Unberechtigte geschützt werden. 41*

Wendet ein Institut bei der Entwicklung, Veränderung und Migration von Systemen (bspw. bei der Generierung von Testdaten oder bei der Zwischenspeicherung von Daten während der Datenmigration) keine Methoden zur Anonymisierung, Pseudonymisierung oder Verschlüsselung an (Arbeiten „in Klartext“), so wendet es bei diesen Tätigkeiten die Vorgaben gemäss Rz 40 an. 41.1*

H. Grundsatz 8: Vorfälle im Zusammenhang mit der CID-Vertraulichkeit, interne und externe Kommunikation

Von den Banken wird erwartet, dass sie vordefinierte Prozesse einführen, um rasch auf Vorfälle in Verbindung mit der Vertraulichkeit zu reagieren, einschliesslich einer klaren Strategie zur Kommunikation schwerwiegender Vorfälle. Zudem müssen Ausnahmen, Vorfälle, Kontroll- und Prüfergebnisse überwacht, analysiert und in geeigneter Form dem obersten Management gemeldet werden. Dies muss zur laufenden Verfeinerung der Massnahmen zur Sicherstellung der Vertraulichkeit von CID beitragen. 42*

a) Identifikation von Vorfällen in Bezug auf die Vertraulichkeit und Reaktion

Es ist ein klar definierter Prozess für die Identifikation von Vorfällen in Bezug auf die Vertraulichkeit sowie die Reaktion darauf zu formalisieren und dieser allen innerhalb des Instituts involvierten Stellen zu kommunizieren. 43*

b) Meldung

Es wird erwartet, dass das Risiko der Verletzung der Vertraulichkeit von CID und diesbezügliche Compliance-Meldungen in den internen Berichterstattungen angemessen abgebildet sind oder alternativ sichergestellt ist, dass eine systematische Erfassung und Eskalierung an geeignete Stellen erfolgt, falls dies die Geheimhaltung solcher Vorkommnisse erfordert. 44*

c) Laufende Verfeinerung des Rahmens zur Sicherstellung der Vertraulichkeit von CID

Das Rahmenkonzept zur Sicherstellung der Vertraulichkeit von CID (Rz 6, 7 und 8) und die Sicherheitsstandards (Rz 24) sind regelmässig zu kontrollieren. Vorfälle, Ausnahmen, Kontroll- und Prüfergebnisse müssen zur laufenden Verfeinerung dieses Rahmenkonzeptes beitragen. 45*

d) Externe Kommunikation

Die Bank muss über eine klare Kommunikationsstrategie verfügen, wenn schwerwiegende Vorfälle in Bezug auf die Vertraulichkeit von CID auftreten. Darin sind insbesondere die Form und der Zeitpunkt der Kommunikation an die FINMA, Strafverfolgungsbehörden, die betroffenen

Anhang 3*



Umgang mit elektronischen Kundendaten

Kunden und die Medien zu regeln.

I. Grundsatz 9: Outsourcing-Dienstleistungen und Grossaufträge in Verbindung mit CID

Bei der Auswahl der Anbieter von Outsourcing-Dienstleistungen, welche CID bearbeiten, muss die CID-Vertraulichkeit ein ausschlaggebendes Kriterium sowie integraler Bestandteil der zu grunde liegenden Sorgfaltsprüfung (Due Diligence) sein. Gemäss dem FINMA-RS 08/7 „Outsourcing Banken“ trägt die Bank über den gesamten Lebenszyklus der ausgelagerten Dienstleistungen weiterhin die endgültige Verantwortung für die CID. Die folgenden Anforderungen gelten zwingend für alle Arten von Aktivitäten, die den Zugriff auf Massen-CID beinhalten, worunter sowohl Grossaufträge (z.B. Drittanbieter von IT-Services, Support für die Installation und den Unterhalt extern entwickelter IT-Plattformen, Hosting von Anwendungen) als auch Nicht-IT-Dienstleistungen (z.B. Outsourcing von Kundenveranstaltungen usw.) fallen.

47*

a) Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID

Die Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID muss Teil des Prozesses für die Auswahl von Outsourcing-Dienstleistern und Anbietern von Grossaufträgen sein. Es müssen klare Kriterien für die Beurteilung der Sicherheits- und Vertraulichkeitsstandards solcher Dritter definiert werden. Die Prüfung in Bezug auf die CID-Sicherheits- und -Vertraulichkeitsstandards muss vor der Vertragsvereinbarung erfolgen und regelmässig wiederholt werden.

48*

b) Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID und Dienstleistungsvereinbarungen

Dritte müssen über die internen Sicherheits- und Vertraulichkeitsstandards der Bank sowie deren allfällige Erweiterungen informiert werden und diese als Mindestanforderung erfüllen.

49*

c) Allgemeine Verantwortung

Die Bank muss für jede ausgelagerte Aktivität, die Zugriff auf CID beinhaltet, mindestens einen internen Mitarbeitenden bestimmen, der dafür verantwortlich ist, dass die Sicherheits- und Vertraulichkeitsstandards in Bezug auf die Vertraulichkeit von CID eingehalten werden.

50*

d) Ausgestaltung der Kontrollen und Wirksamkeitstests

Die Bank muss wissen und verstehen, welche Schlüsselkontrollen der Outsourcing-Dienstleister in Verbindung mit der Vertraulichkeit von CID durchzuführen hat. Die Einhaltung interner Anforderungen sowie die Wirksamkeit der Schlüsselkontrollen sind dabei zu prüfen und zu beurteilen.

51*

II. Glossar

Kundenidentifikationsdaten (Client Identifying Data, CID): Kundendaten, die Personendaten nach Art. 3 Bst. a DSG darstellen und es ermöglichen, die betroffenen Kunden zu identifizieren.

52*

Massen-CID: Menge von CID, welche im Vergleich zur Gesamtzahl der Konten/Gesamtgrösse

53*

Anhang 3*

Umgang mit elektronischen Kundendaten



des Privatkundenportfolios bedeutend ist.

Grossaufträge: Alle durch Dritte erbrachten Dienstleistungen, die Zugriff auf Massen-CID erfordern oder potenziell zum Zugriff auf Massen-CID führen (z.B. bei der Implementierung von Zugriffsrechtsprofilen durch Mitarbeitende eines Dritten). Ein CID-Risiko kann beispielsweise auftreten bei der Installation von Anwendungen oder der Implementierung von lokalen Einstellungen (z.B. Zugriffsrechten), der Datenspeicherung oder dem laufenden Systemunterhalt (z.B. Drittanbieter von IT-Services, extern entwickelte IT-Plattformen). Dies umfasst auch interne Prüfarbeiten und externe Prüfungen. Gewöhnlich sind solche Grossaufträge langfristiger Natur. 54*

Mitarbeitende Dritter: Alle Mitarbeitenden, die für Beauftragte der Bank arbeiten (z.B. Auftragnehmer, Berater, externe Prüfer, externe Unterstützung usw.), die Zugriff auf CID haben und nicht interne Mitarbeitende sind. 55*

Schlüsselmitarbeitende: Alle internen und externen im IT-Bereich sowie in weiteren Unternehmensbereichen tätigen Mitarbeitenden, die aufgrund ihres Tätigkeitsprofils und ihrer Aufgaben (hoch-)privilegierten Zugriff auf CID im grossen Umfang haben (z.B. Datenbankadministratoren, Mitglieder des obersten Managements). 56*

Schwerwiegender Vorfall in Bezug auf die Vertraulichkeit von Kundendaten / Leck von Kundendaten: Ein Vorfall in Bezug auf die Vertraulichkeit von Kundendaten, der ein bedeutendes Leck von CID impliziert (im Vergleich zur Gesamtzahl der Konten/Gesamtgrösse des Kundenportfolios). 57*

Schlüsselkontrolle: Eine Kontrolle, die, falls sachgerecht definiert, implementiert und durchgeführt, das Risiko der Verletzung der Vertraulichkeit von CID massgeblich senkt. 58*

Inhärentes Risiko: Risiko vor Kontroll- oder Minderungsmassnahmen. 59*

Residualrisiko: Risiko nach Berücksichtigung von Kontroll- oder Minderungsmassnahmen. 60*

Reversible Datenbearbeitungstechniken: 61*

- Pseudonymisierte Daten (Pseudonymisierung): Unter Pseudonymisierung versteht man den Vorgang der Trennung der identifizierenden (z.B. Name, Foto, E-Mail Adresse, Telefonnummer) von anderen Daten (z.B. Kontostand, Kreditwürdigkeit). Das Bindeglied zwischen den beiden Datenbereichen bilden sogenannte Pseudonyme und eine Zuordnungsregel (Konkordanztabelle). Beispielsweise können Pseudonyme durch einen Zufallszahlengenerator erzeugt und mittels einer Konkordanztabelle den identifizierenden Personendaten bei Bedarf zugeordnet werden. 62*

- Verschlüsselte Daten: In der Praxis wird die Pseudonymisierung auch mittels Verschlüsselungsverfahren umgesetzt. Das Pseudonym wird in diesem Fall durch Verschlüsselung von identifizierenden Personendaten mit einem kryptographischen Schlüssel erzeugt. Die Reidentifikation erfolgt aufgrund der Entschlüsselung mit Hilfe des geheimen Schlüssels. 63*

Anhang 3*



Umgang mit elektronischen Kundendaten

Irreversible Datenbearbeitungstechniken:

64*

- Anonymisierte Daten: Bei der Anonymisierung von Personendaten werden sämtliche Elemente, die eine Identifizierung einer Person ermöglichen, unwiederbringlich entfernt oder verändert (z.B. durch Löschung oder Aggregierung), so dass die Daten nicht mehr mit einer bestimmten oder bestimmmbaren Person verknüpft werden können. Solche Daten sind/enthalten gemäss Definition keine CID mehr und fallen nicht unter das DSG³⁴.

65*

³⁴ Vgl. EDÖB, Anhang zu den Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem, 5.

Verzeichnis der Änderungen



Das Rundschreiben wird wie folgt geändert:

Diese Änderungen wurden am 1.6.2012 beschlossen und treten am 1.1.2013 in Kraft.

Geänderte Rz 84

Zudem wurden die Verweise auf die Eigenmittelverordnung (ERV; SR 952.03) an die am 1.1.2013 in Kraft tretende Fassung angepasst.

Diese Änderungen wurden am 29.8.2013 beschlossen und treten am 1.1.2014 in Kraft.

Neu eingefügte Rz 116

Diese Änderungen wurden am 29.8.2013 beschlossen und treten am 1.1.2015 in Kraft.

Neu eingefügte Rz 2.1, 117–139

Geänderte Rz 1, 29, 50, 53, 71, 79

Aufgehobene Rz 20–22, 28, 30–44, 64

Übrige Änderungen Neuer Haupttitel vor Rz 3 und Neugliederung der Titel
Titeländerung vor Rz 50

Diese Änderungen wurden am 27.3.2014 beschlossen und treten am 1.1.2015 in Kraft.

Geänderte Rz 1, 9, 10, 11, 12, 13, 14

Diese Änderungen wurden am 22.9.2016 beschlossen und treten am 1.7.2017 in Kraft.

Neu eingefügte Rz 132.1–132.3, 135.1–135.12, 136.1–136.5

Geänderte Rz 2, 53, 117, 118, 119, 121, 122, 128, 129, 130, 132, 133, 134, 135,
136, 137

Aufgehobene Rz 2.1, 123, 124, 125, 126, 127, 131

Übrige Änderungen Kap. IV.B: Neunummerierung der Grundsätze

Die Anhänge des Rundschreibens wurden wie folgt geändert:

Diese Änderungen wurden am 29.8.2013 beschlossen und treten am 1.1.2015 in Kraft.

Die Nummerierung der Anhänge wird angepasst: Anhang 2 "Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV" wird neu zum Anhang 1 und Anhang 3 "Übersicht zur Klassifikation von Ereignistypen" wird neu zum Anhang 2.

Neu Anhang 3

Aufgehoben Anhänge 1 und 4

Verzeichnis der Änderungen



Diese Änderungen wurden am 22.9.2016 beschlossen und treten am 1.7.2017 in Kraft.

Neu	Anhang 3: Rz 41.1
Geändert	Anhang 1: Rz 9 Anhang 2: Titel des Anhangs Anhang 3: Rz 2, 3, 5, 6, 7, 8, 16, 17, 30, 33, 34, 56

Rundschreiben 2018/3 Outsourcing – Banken und Versicherer

Auslagerungen bei Banken und Versicherungsunternehmen

Referenz: FINMA-RS 18/3 „Outsourcing – Banken und Versicherer“
 Erlass: 21. September 2017
 Inkraftsetzung: 1. April 2018
 Konkordanz: vormals FINMA-RS 08/7 „Outsourcing Banken“ vom 20. November 2008
 Rechtliche Grundlagen: FINMAG Art. 7 Abs. 1 Bst. b
 BankG Art. 3 Abs. 2 Bst. a
 BEHG Art. 10 Abs. 2 Bst. a
 BEHV Art. 19
 VAG Art. 4 Abs. 2 Bst. j, 5 Abs. 2, 14 Abs. 3, 47 Abs. 2

Adressaten									
Banken		BankG		VAG		BEHG		FintrAG	
Banken	Finanzgruppen und -kongl. Andere Intermediaire	Versicherer	Vers.-Gruppen und -Kongl.	Vermittler	Effektenhändler	Handelsplätze	Zentrale Gegenparteien	Zentralenverwahrer	Transaktionsregister
X	X	X	X	X	X	Handelsplätze	Zentrale Gegenparteien	Zentralenverwahrer	Zahlungssysteme
									Teilnehmer
									Fondsteilungen
									SICAV
									Kmfd für KKA
									SICAF
									Degabanken
									Vermögensverwalter KKA
									Vertreter/-träger
									Vertreter ausl. KKA
									Andere Intermediaire
									SRO
									DUFI
									SRO/Beauftragte
									Prüfgesellschaften
									Andere
									Ratingagenturen

Inhaltsverzeichnis



I. Zweck	Rz	1
II. Begriffe	Rz	2–4
III. Geltungsbereich	Rz	5–6
IV. Zulässigkeit	Rz	7–13
A. Gemeinsame Bestimmungen	Rz	7–9
B. Versicherungsunternehmen	Rz	10–13
V. Anforderungen an auslagernde Unternehmen	Rz	14–35
A. Inventarisierung der ausgelagerten Funktionen	Rz	14–15
B. Auswahl, Instruktion und Kontrolle des Dienstleisters	Rz	16–21
C. Konzern- / gruppeninterne Auslagerungen	Rz	22
D. Verantwortung	Rz	23
E. Sicherheit	Rz	24–25
F. Prüfung und Aufsicht	Rz	26–29
G. Auslagerungen ins Ausland	Rz	30–31
H. Vertrag	Rz	32–35
VI. Auflagen und Ausnahmen	Rz	36
VII. Übergangsbestimmungen	Rz	37–38

I. Zweck

Das vorliegende Rundschreiben legt die aufsichtsrechtlichen Anforderungen an Outsourcing-Lösungen von Banken, Effektenhändlern und Versicherungsunternehmen dar. Für diese enthält es Anforderungen an eine angemessene Organisation und bezweckt deren Risikobegrenzung.

1

II. Begriffe

Als Unternehmen gelten Institute (Banken, Effektenhändler und Versicherungsunternehmen) im Geltungsbereich dieses Rundschreibens.

2

Ein Outsourcing (Auslagerung) im Sinne des Rundschreibens liegt vor, wenn ein Unternehmen einen Dienstleister beauftragt, selbständig und dauernd eine für die Geschäftstätigkeit des Unternehmens wesentliche Funktion ganz oder teilweise zu erfüllen.

3

Wesentlich sind jene Funktionen, von denen die Einhaltung der Ziele und Vorschriften der Finanzmarktaufsichtsgesetzgebung signifikant abhängt.

4

III. Geltungsbereich

Dieses Rundschreiben gilt für:

- Banken und Effektenhändler mit Sitz in der Schweiz sowie schweizerische Zweigniederlassungen ausländischer Banken und Effektenhändler;
- Versicherungsunternehmen mit Sitz in der Schweiz und Zweigniederlassungen von ausländischen Versicherungsunternehmen, welche die Bewilligung zum Geschäftsbetrieb nach Art. 3 und 6 VAG (Erstbewilligung) oder die Bewilligung für einzelne Elemente des Geschäftsplans nach Art. 4 i.V.m. Art. 5 VAG (Änderungsbewilligung) bedürfen.

5

6

IV. Zulässigkeit

A. Gemeinsame Bestimmungen

Vorbehältlich der nachfolgenden Ausnahmen (Rz 8–13) ist die Auslagerung aller wesentlichen Funktionen zulässig.

7

Nicht auslagerbar sind die Oberleitung, Aufsicht und Kontrolle durch das Oberleitungsorgan, zentrale Führungsaufgaben der Geschäftsleitung sowie Funktionen, die das Fällen von strategischen Entscheiden umfassen. Dies gilt ebenso für Entscheide über die Aufnahme und den Abbruch von Geschäftsbeziehungen.

8

Die Unternehmen der Aufsichtskategorien 1 bis 3 verfügen über eine eigenständige Risikokontrolle und Compliance-Funktion als unabhängige Kontrollinstanzen. Bei Unternehmen der Aufsichtskategorien 4 und 5 genügt es, wenn eine für diese Funktionen verantwortliche Person in der Geschäftsleitung bestimmt ist. Operative Risikomanagement- und Compliance-Aufgaben sind bei allen Aufsichtskategorien auslagerbar.

9

B. Versicherungsunternehmen

Das Outsourcing von wesentlichen Funktionen und die beschränkt zulässige Auslagerung von Kontrollfunktionen sind nach Art. 4 Abs. 2 Bst. j i.V.m. Art. 5 Abs. 2 VAG geschäftsplanrelevant und damit genehmigungspflichtig. 10

Für Versicherungscaptives ist die Auslagerung von Führungs- und Kontrollfunktionen in einem weiteren Umfang zulässig als bei den übrigen Versicherungsunternehmen. Zulässig sind:

- Das Outsourcing des Managements von Direkt- und Rückversicherungscaptives mit Sitz in der Schweiz (inkl. zentraler Führungsaufgaben der Geschäftsführung) auf entsprechend spezialisierte Captive-Management-Gesellschaften; 12
- Das Outsourcing des Managements von Zweigniederlassungen ausländischer Direktversicherungscaptives innerhalb des Konzerns oder auf entsprechend spezialisierte Captive-Management-Gesellschaften. Die aufsichtsrechtliche Funktion des Generalbevollmächtigten (Art. 17 und 18 AVO) darf dadurch nicht eingeschränkt werden. 13

V. Anforderungen an auslagernde Unternehmen

A. Inventarisierung der ausgelagerten Funktionen

Über die ausgelagerten Funktionen ist ein aktuell zu haltendes Inventar zu führen. Dieses enthält eine Umschreibung der ausgelagerten Funktion, nennt Erbringer (inkl. Unterakordanten) und Empfänger sowie die unternehmensintern verantwortliche Stelle (vgl. Rz 20). 14

Die Versicherungsunternehmen führen dieses Inventar im Rahmen des Geschäftsplanformulars J. 15

B. Auswahl, Instruktion und Kontrolle des Dienstleisters

Entsprechend den mit der Auslagerung verfolgten Zielen sind die Anforderungen an die Leistungserbringung vor Vertragsschluss festzulegen und zu dokumentieren. Dies beinhaltet eine Risikoanalyse, welche die wesentlichen ökonomischen und operativen Überlegungen und die damit verbundenen Risiken und Chancen einschliesst. 16

Die Auswahl des Dienstleisters hat unter Berücksichtigung und Prüfung seiner professionellen Fähigkeiten sowie finanziellen und personellen Ressourcen zu erfolgen. Werden mehrere Funktionen an den gleichen Dienstleister ausgelagert, so ist dem Konzentrationsrisiko Rechnung zu tragen. 17

Ferner sind beim Entscheid über das Outsourcing und bei der Auswahl des Dienstleisters die Möglichkeiten und Folgen eines Wechsels zu berücksichtigen. Der Dienstleister hat Gewähr für eine dauerhafte Leistungserbringung zu bieten. Die geordnete Rückführung der ausgelagerten Funktion muss sichergestellt sein. 18

Die Zuständigkeiten des Unternehmens und des Dienstleisters sind vertraglich festzulegen und abzugrenzen, insbesondere bezüglich Schnittstellen und Verantwortlichkeiten. 19

Die ausgelagerte Funktion ist in das interne Kontrollsystrem des Unternehmens zu integrieren. Die mit der Auslagerung verbundenen wesentlichen Risiken sind systematisch zu 20

identifizieren, zu überwachen, zu quantifizieren und zu steuern. Unternehmensintern ist eine verantwortliche Stelle zu definieren, die für die Überwachung und Kontrolle des Dienstleisters zuständig ist. Dessen Leistungen sind fortlaufend zu überwachen und zu beurteilen, so dass allfällige nötige Massnahmen zeitnah ergrieffen werden können.

Das Unternehmen hat sich die dazu nötigen Weisungs- und Kontrollrechte vom Dienstleister vertraglich einräumen zu lassen.

21

C. Konzern- / gruppeninterne Auslagerungen

Bei den Anforderungen gemäss den Rz 16–21 sowie 32–35 kann die Verbundenheit im Konzern/in der Gruppe berücksichtigt werden, sofern die mit der Auslagerung typischerweise vorhandenen Risiken nachweislich nicht bestehen oder gewisse Anforderungen nicht relevant oder anders geregelt sind.

22

D. Verantwortung

Das Unternehmen trägt gegenüber der FINMA weiterhin die selbe Verantwortung, wie wenn es die ausgelagerte Funktion selber erbringen würde. Es hat die ordnungsgemässe Geschäftsführung jederzeit zu gewährleisten.

23

E. Sicherheit

Bei sicherheitsrelevanten Auslagerungen (namentlich im Bereich IT) legen das Unternehmen und der Dienstleister vertraglich Sicherheitsanforderungen fest. Deren Einhaltungen sind vom Unternehmen zu überwachen.

24

Das Unternehmen und der Dienstleister erarbeiten ein Sicherheitsdispositiv, das die Weiterführung der ausgelagerten Funktion in Notfällen erlaubt. Bei Errichtung und Anwendung des Sicherheitsdispositivs gilt für das Unternehmen derselbe Sorgfaltsmassstab, wie wenn es die ausgelagerte Funktion selber erbringen würde.

25

F. Prüfung und Aufsicht

Das Unternehmen und dessen Prüfgesellschaft sowie die FINMA müssen in der Lage sein, die Einhaltung der aufsichtsrechtlichen Bestimmungen beim Dienstleister zu prüfen. Zu ihren Gunsten ist vertraglich ein jederzeitiges, voluminöses und ungehindertes Einsichts- und Prüfrecht in Bezug auf die ausgelagerte Funktion einzuräumen.

26

Prüftätigkeiten können an die Revisionsstelle des Dienstleisters delegiert werden, sofern diese über die notwendigen fachlichen Kompetenzen verfügt. Erfolgt eine solche Delegation, kann die Prüfgesellschaft des Unternehmens auf die Prüfungsergebnisse der Revisionsstelle des Dienstleisters abstellen.

27

Die Auslagerung einer Funktion darf die Aufsicht durch die FINMA nicht erschweren, insbesondere bei einer Auslagerung ins Ausland.

28

Untersteht der Dienstleister nicht der Aufsicht der FINMA, hat er sich gegenüber dem Unternehmen vertraglich zu verpflichten, der FINMA sämtliche Auskünfte und Unterlagen bezogen auf den ausgelagerten Geschäftsbereich zur Verfügung zu stellen, die sie für die Aufsichtstätigkeit benötigt. Falls Prüftätigkeiten an die Revisionsstelle des Dienstleisters delegiert werden, ist ihr Bericht der FINMA, der internen Revisionsstelle und der Prüfgesellschaft des auslagernden Unternehmens auf Anfrage zur Verfügung zu stellen.

G. Auslagerungen ins Ausland

Auslagerungen ins Ausland sind zulässig, sofern das Unternehmen ausdrücklich zusichern kann, dass es selber, seine Prüfgesellschaft sowie die FINMA ihre Einsichts- und Prüfrechte wahrnehmen und durchsetzen können. 30

Die Sanierbarkeit bzw. Abwickelbarkeit des Unternehmens in der Schweiz muss gewährleistet sein. Der Zugriff auf die dafür notwendigen Informationen muss jederzeit in der Schweiz möglich sein. 31

H. Vertrag

Die Auslagerung muss auf einem schriftlichen Vertrag beruhen. Neben der Bezeichnung der Parteien und einer Beschreibung der Funktion enthält dieser im Minimum folgenden Inhalt (Rz 33–34): 32

Das Unternehmen hat den Bezug von Unterakkordanten, die wesentliche Funktionen erbringen, von seiner vorgängigen Genehmigung abhängig zu machen. Werden solche Unterakkordanten beigezogen, sind ihnen die Pflichten und Zusicherungen des Dienstleisters, die zur Erfüllung dieses Rundschreibens erforderlich sind, zu überbinden. 33

Es sind vertragliche Vorkehrungen zur Umsetzung der Anforderungen gemäss diesem Rundschreiben und insbesondere den Rz 21, 24, 26, 29, 30 und 31 zu treffen. 34

Das Unternehmen hat die internen Bewilligungsverfahren für Outsourcing-Projekte sowie die Zuständigkeiten für die entsprechenden Vertragsabschlüsse festzulegen. 35

VI. Auflagen und Ausnahmen

Die FINMA kann einem Unternehmen in begründeten Fällen Auflagen machen oder dieses von der Einhaltung des Rundschreibens ganz oder teilweise befreien. 36

VII. Übergangsbestimmungen

Das Rundschreiben findet unmittelbar Anwendung auf Outsourcingverhältnisse von Banken und Effektenhändlern, die nach dessen Inkrafttreten abgeschlossen oder geändert werden. Outsourcingverhältnisse von Banken und Effektenhändlern, die bei Inkrafttreten des Rundschreibens bereits bestehen, sind innerhalb einer Übergangsfrist von fünf Jahren ab Inkrafttreten so anzupassen, dass die Anforderungen des Rundschreibens eingehalten sind. 37

Für Versicherungsunternehmen gilt das Rundschreiben für Erstbewilligungen ab dessen Inkrafttreten. Für Änderungsgenehmigungen gilt das Rundschreiben ab dem Zeitpunkt, in dem eine Geschäftsplanänderung der FINMA zur Genehmigung unterbreitet bzw. mitgeteilt wird. 38

C Kundendaten im Konkursverfahren (DSB ZH)

Kundendaten im Konkursverfahren

Das Konkursamt darf im Rahmen seiner Aufgabenerfüllung Kundendateien verwerten. Je nach der Qualifikation des ursprünglichen Kundenverhältnisses sind unterschiedliche Formen der Verwertung zu beachten.

1 Grundlagen

Ein öffentliches Organ darf Personendaten bearbeiten, soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist (§ 8 Abs. 1 Gesetz über die Information und den Datenschutz, IDG, [LS 170.4](#)). Eine Bekanntgabe von Personendaten setzt eine Ermächtigung durch eine rechtliche Bestimmung oder die Einwilligung der betroffenen Person voraus (§ 16 Abs. 1 IDG). Vor der Bekanntgabe hat jeweils eine Interessenabwägung zu erfolgen. Die Bekanntgabe kann erfolgen, wenn ihr keine überwiegenden öffentlichen oder privaten Interessen im Wege stehen (§ 23 IDG).

Zu den Aufgaben des Konkursamtes gehört die Verwertung von Aktiven aus der Konkursmasse (Art. 252 ff. Bundesgesetz über Schuldbetreibung und Konkurs, SchKG, [SR 281.1](#)). Dazu kann auch die konkursamtliche Verwertung von Kundendateien gehören. Die Bearbeitung und Bekanntgabe von Kundendaten ergibt sich in diesen Fällen aus der gesetzlichen Aufgabe der Verwertung der Konkursmasse.

2 Interessenabwägung

Im Rahmen der Interessenabwägung ist zu berücksichtigen, ob das ursprüngliche Vertragsverhältnis zwischen dem konkursiten Unternehmen und den Kundinnen und Kunden von einem besonderen Vertrauensverhältnis geprägt war. Je nachdem ist eine Datenbekanntgabe einzuschränken.

Bei einem unqualifizierten Vertragsverhältnis wie beispielsweise zwischen einem Versandhaus und seiner Kundschaft ist eine Bekanntgabe der Kundendaten (Namen und Adressen) auch ohne Zustimmung der Kundschaft durch die Aufgabenerfüllung des Konkursamtes möglich.

Demgegenüber ist bei einem qualifizierten Vertragsverhältnis wie beispielsweise zwischen einer Ärztin oder einem Arzt und seiner Patientin oder Patienten grundsätzlich die Zustimmung der betroffenen Personen notwendig. Zwischen dem konkursiten Unternehmen und seiner Kundschaft bestand ein von einem besonderen Vertrauen abhängiges Vertragsverhältnis. Die betroffene Person muss demnach nicht damit rechnen, dass jemand anders, zu dem sie kein Vertrauen hat oder kein Vertrauen haben muss, ihre Daten erfährt. Deshalb ist ihre Zustimmung zur Datenbekanntgabe erforderlich.

Bei der Form der Zustimmung ist weiter zu differenzieren, welche Daten bekannt zu geben sind. Bei wenig heiklen Daten genügt eine Anzeige mit einer angemessenen Widerspruchsfrist. Dies ist beispielsweise bei der Bekanntgabe der Bankbeziehung bei der Übernahme einer Bank im Rahmen einer Fusion der Fall. Bei heiklen Daten ist eine ausdrückliche vorläufige Zustimmung erforderlich. Dies gilt beispielsweise für die Bekanntgabe von Gesundheitsdaten und in sämtlichen weiteren Fällen, in denen besondere Geheimhaltungspflichten betroffen sind (Patientengeheimnis, Anwaltsgeheimnis, Amtsgeheimnis).