Cloud Verträge – Regelungsbedarf und Vorgehensweise

Wolfgang Straub

Cloudbasierte Services sind vielgestaltig und reichen von Gratisservices im Internet bis zu eigentlichen IT Outsourcinglösungen. Ebenso vielfältig sind die vertraglichen Regelungen, welche von per Mausclick zu bestätigenden Allgemeinen Nutzungsbedingungen bis zu massgeschneiderten Vertragswerken gehen. Vorliegend wird ein Überblick über die rechtlichen Problemstellungen von Cloud Verträgen gegeben. Als Orientierungshilfe für komplexe Vorhaben wird zudem eine Vorgehensmethodik skizziert, wie der in die Cloud auszulagernden Bereich festgelegt, der Provider ausgewählt und die Vertragsinhalte konkretisiert werden können.

Les services basés sur des clouds sont très variés et s'étendent des services gratuits aux véritables solutions d'outsourcing informatique. On retrouve cette même variété dans les réglementations contractuelles, qui vont des conditions générales d'utilisation à confirmer d'un clic de souris aux contrats complexes, taillés sur mesure. Cet article donne une vue d'ensemble des problématiques juridiques des contrats relatifs aux clouds. Afin de faciliter l'orientation dans le cas de projet complexes, l'auteur esquisse en outre une marche à suivre pour la définition du domaine à externaliser vers le cloud, le choix du prestataire et la détermination concrète des contenus du contrat.

Inhaltsübersicht

1. Einleitung

«Cloud» ist kein juristischer Begriff. – An ihn knüpfen keine direkten rechtlichen Folgen an. Vielmehr werden darunter sehr unterschiedliche Erscheinungsformen von computergestützten Services verstanden, welche über ein Netzwerk zur Verfügung gestellt werden.[1] Im vorliegenden Zusammenhang sind vor allem drei Dimensionen relevant:[2]

– *Die Serviceebene:* Es können verschiedene jeweils aufeinander aufbauende Ebenen von Services unterschieden werden: *Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (Saas), Business Process as a Service (BPaaS)*.[3] Die Services der einzelnen Ebenen werden oft durch unterschiedliche Subunternehmer erbracht. Systemintegratoren treten mitunter auch als Generalunternehmer auf. Sie bieten zusätzlich zu Dienstleistungen, welche auf Cloud Computing basieren (nachfolgend als Cloud Services bezeichnet), teilweise auch noch weitere Leistungen an.
– *Der Grad der Exklusivität der Services:* Handelt es sich um für einen einzigen Kunden dediziert[4] betrie-

Wolfgang Straub, Dr. iur., LL.M., ist Rechtsanwalt in Bern.
Der vorliegende Aufsatz ist aus der Diskussion mit zahlreichen Kolleginnen und Kollegen heraus entstanden. Für wertvolle Anregungen und Hinweise danke ich namentlich Caroline Gloor-Scheidegger, Adrian Hässig, Karin Koç, Christian Laux, Christian Leupi, Daniel Markwalder, Peter Neuenschwander, Stephan Rothenbühler, Renate Scherrer-Jost, Jürg Schneider, Christoph Stalder, Peter Trachsel, Fridolin Walther, Maria Winkler und Esther Zysset.

1 Siehe dazu auch Informatiksteuerungsorgan des Bundes, Kommentar zur Cloud-Computing-Strategie der Behörden, online verfügbar unter *www.isb.admin.ch/cloud-strategie*?.

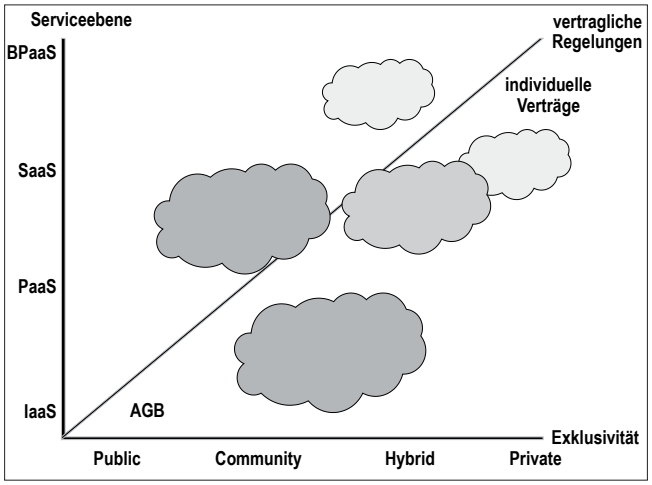
2 Weitere Unterteilungen können z.B. nach dem Vergütungsmodell vorgenommen werden. Dabei gibt es zahlreiche Mischformen zwischen rein nutzungsabhängigen und festen Vergütungen.

3 Die Abgrenzung zwischen den einzelnen Serviceebenen verläuft teilweise fliessend. Bei *Infrastructure as a Service* wird dem Kunden Speicherplatz und eventuell zusätzlich Rechenkapazität auf Hardware des Providers zur Verfügung gestellt. Der Begriff *Platform as a Service* wird teils in einem engeren Sinn nur als Zurverfügungstellen von Plattformen für die Entwicklung von (Web-) Anwendungen verstanden. Nach dem hier zugrunde gelegten, weiteren Verständnis umfasst *Platform as a Service* auch das Zurverfügungstellen von Betriebssystemen und *Middleware* (z.B. Datenbanksoftware). Bei *Software as a Service* werden dem Kunden darüber hinaus auch Anwendungsprogramme (Applikationen) zur Verfügung gestellt.

4 Der Begriff der «dedizierten» Infrastruktur wird in der Praxis nicht immer einheitlich verwendet. Es sollte vertraglich präzise definiert werden, ob es sich um eigens für einen bestimmten Kunden betriebene Hardware handelt (und welche Hardwarekomponenten umfasst sind), oder ob für die einzelnen Kunden lediglich virtuelle Maschinen aufgesetzt werden.

bene *Private Clouds* oder um *Public Clouds,* bei welchen sich viele Kunden dieselbe Infrastruktur teilen?[5]

– *Die Struktur*[6] *der vertraglichen Regelungen:* Diese reichen von Allgemeinen Geschäftsbedingungen für Gratisservices bis zu komplexen, individuell ausgehandelten Vertragswerken.[7]



Grafik 1
Schematische Übersicht über verschiedene Cloud-Typen: Serviceebene, Exklusivität der Services und Individualisierungsgrad der vertraglichen Regelungen können je als Dimensionen verstanden werden. Je höher die Serviceebene und die Exklusivität, umso individueller sind in der Regel aber auch die vertraglichen Regelungen.

Sowohl beim IT Outsourcing als auch bei Cloud Services handelt es sich um Dauerdienstleistungsverträge mit Innominatcharakter.[8] *Software as a Service* entspricht rechtlich einem *Application Service Providing*.[9] Cloud Service Verträge können alle Fragestellungen mit sich bringen, welche von Outsourcingverträgen her bereits bekannt sind (z.B. Service Levels, Sicherheitsaspekte, Haftungsfragen).[10] Die von der Lehre zum IT Outsourcing entwickelten Grundsätze[11] sind weitestgehend auch auf Cloud Service Verträge anwendbar.[12] Was ist aber gegenüber einem «traditionellen» *Outsourcing* überhaupt neu oder anders?

---

5 Der Begriff der *Private Cloud* wird in der Praxis nicht einheitlich verwendet. Er kann sowohl virtualisierte Infrastrukturen innerhalb eines Unternehmens als auch bei externen Providern für einen Kunden dediziert gehostete Infrastrukturen umfassen. Zwischenformen von Private Clouds und Public Clouds bilden *Community Clouds,* in welchen die Mitglieder einer Gruppe oder einer Organisation gemeinsame Infrastruktur teilen sowie *Hybrid Clouds,* bei denen einzelne Leistungskomponenten eines Gesamtservices in Private Clouds, andere in Public Clouds erbracht werden. *Virtual Private Clouds* stellen eine besondere Ausprägung von Public Clouds dar. Dem Kunden wird dabei eine abgekapselte IT-Infrastruktur zur Verfügung gestellt und via Virtual Private Network mit seinem Netzwerk verbunden.

6 Teilweise wird in Bezug auf die vertragliche Beziehung unterschieden zwischen *Open Clouds,* die vom Provider zugunsten eines offenen Benutzerkreises aufgesetzt werden und nach dem Akzeptieren vorformulierter Vertragsbedingungen per Mausclick von jedermann genutzt werden können, und *Exclusive Clouds,* welche entsprechend den in einem individuellen Vertrag ausgehandelten Bedingungen für den Kunden dediziert aufgesetzt werden. Allerdings sind auch hier Zwischenformen durch individuelle Anpassungen standardisierter Angebote möglich. Die Struktur der vertraglichen Regelungen kann auch unterschiedlich sein, je nachdem ob ein direkter Zugang zu den Services möglich ist (z.B. via Webbrowser) oder ob spezielle Clientsoftware dazu eingesetzt wird, welche zusätzlich lizenziert werden muss. Der Begriff der Open Cloud ist indessen mehrdeutig und wird auch für Cloud Services verwendet, welche auf offenen Standards oder auf Open Source Software basieren.

7 Gemäss einer Studie aus den Jahr 2011 wurden nur rund die Hälfte der Cloud Service Verträge von Unternehmenskunden individuell verhandelt. Siehe dazu auch Kuan W. Hon/Christopher Millard/Ian Walden, Negotiating Cloud Contracts: looking at clouds from both sides now, Stanford Technology Law Review Vol. 16, Nr. 1/2012, 79–129, 84, online verfügbar unter *http://stlr.stanford.edu/pdf/cloudcontracts.pdf.*

8 Siehe zur rechtlichen Qualifikation von IT-Dienstleistungsverträgen mit Langzeitcharakter Wolfgang Straub, Informatikrecht – Einführung in Softwareschutz, Projektverträge und Haftung, Bern/Zürich 2004, 201 ff.

9 Siehe zu den Erscheinungsformen und zur Rechtsnatur solcher Verträge Christian Imhof, Der ASP-Vertrag, Zürich 2008, zugl. Diss. Fribourg 2008, Rz. 32 ff., 99 ff. und 156 ff.; Michel Jaccard, Les contrats de fourniture de services d'application, in: Raphaël Bagnoud/Laure Dallèves (Hrsg.), Internet 2005, Lausanne 2006, 149–180, 154 ff. und 162 ff.; Florian S. Jörg, Application Service Providing-Vertrag, in: Florian S. Jörg/Oliver Arter (Hrsg.), Internet-Recht und IT-Verträge, Bern 2005, 285–326, 290 ff.; Mathis Berger, ASP: ein neues Geschäftsmodell als Herausforderung für das Recht? sic 2002, 667–676, 667 ff.; Lukas Morscher, Software-Überlassungsverträge, Teil I: Vertragsschluss, Rechtseinräumung, Typisierung, Anknüpfung, in: Hans Rudolf Trüeb (Hrsg.), Softwareverträge: Referate der Tagung der Stiftung für juristische Weiterbildung Zürich vom 11. November 2003, Zürich 2004, 61–88, 79; Nicolas Passadelis, Application Service Providing-Vertrag, in: Peter Münch/Peter Böhringer/Sabina Kasper/Franz Probst (Hrsg.), Schweizer Vertragshandbuch, Musterverträge für die Praxis, 2. A. Basel 2010; 1817 ff.; Pierre-Alain Killias, Contrats relatifs aux sites Internet et les contrats de type ASP, in: Nathalie Tissot (Hrsg.), Quelques facettes du droit de l'internet, Band 5, Neuchâtel 2004, 23–48, 43 f.

10 Gemäss der Untersuchung von Hon/Millard/Walden (FN 7), 81, wird beim Abschluss von Cloud Service Verträgen am meisten über Haftungsfragen, Service Level Agreements, Datenschutz und Informationssicherheit, Auflösungsrechte, Leistungsänderungen sowie Immaterialgüterrechte verhandelt.

11 Siehe zur Rechtsnatur von IT Outsourcingverträgen András Gurovits, IT-Outsourcing Verträge in der Vertragspraxis, in: Florian S. Jörg/Oliver Arter (Hrsg.), Internet-Recht und IT-Verträge, Bern 2005, 261–285; Bernhard Heusler/Roland Mathys, IT-Vertragsrecht: Praxisorientierte Vertragsgestaltung in der Informationstechnologie, Zürich 2004, 17 ff.; Gianni Fröhlich-Bleuler, Softwareverträge, System-, Software-Lizenz und Software-Pflegevertrag, 2. A., Bern 2014, Rz. 2454; Ursula Sury, Informatikrecht, Bern 2013, 59 f.; Straub (FN 8), Informatikrecht, 223 ff.

12 Siehe zur vertragsrechtlichen Einordnung von Cloud Service Verträgen Carmen de la Cruz, Cloud Computing – alter Wein in neuen Schläuchen? jusletter IT vom 15.5.2013, Rz. 12 ff.; Andreas

– Cloud Computing basiert stets auf *IT-Leistungen*. Im Rahmen eines Cloud Service Vertrages können zwar auch Geschäftsprozesse ausgelagert werden, welche lediglich auf IT-Services aufbauen. Outsourcing kann sich hingegen auch auf Geschäftsprozesse beziehen, welche gar keinen IT-Bezug haben.[13]
– Cloud Services sind innerhalb bestimmter Bandbreiten entsprechend dem Bedarf des Auftraggebers einfach und rasch, oft sogar vollautomatisch *skalierbar* (z.B. dynamische Erhöhung oder Verringerung der zur Verfügung gestellten Speicherkapazitäten).
– Typischerweise kommen für Cloud *Services nutzungsabhängige Vergütungsmodelle («pay as you go»)* zum Einsatz.
– Für Public Cloud-Lösungen typisch ist die *fehlende Lokalisierbarkeit* der Datenspeicherung, da Daten – soweit nicht vertraglich anders geregelt – oft dynamisch über verschiedene Rechenzentren verteilt werden.[14] Dies bringt insbesondere datenschutzrechtliche Fragen mit sich.
– Bei *Software as a Service* werden meistens Daten des Auftraggebers auf Plattformen des Providers gespeichert. Dadurch entsteht ein erhöhtes *Abhängigkeitspotenzial* vom Provider.

Bei der rechtlichen *Prüfung, Redaktion und Verhandlung von Cloud Service Verträgen* ist insbesondere folgenden Bereichen erhöhte Aufmerksamkeit zu widmen:

– *Rechte an Daten:* Datenschutz, Immaterialgüterrechte, Herausgabe von Daten im Insolvenzfall etc.
– *Compliance* mit rechtlichen Vorschriften: Geheimhaltungs- und Datenschutzvorschriften[15], Beweis-[16] und Archivierungsvorschriften[17], sektorenspezifische Vorgaben[18] etc.
– *Klärung der Verantwortlichkeitssphären* zwischen Auftraggeber[19] und Provider sowie Drittleistungserbringern (z.B. Zugangsprovider, Subunternehmer, Softwarelieferanten). Um negative Kompetenzkonflikte zu vermeiden, hat der Auftraggeber ein Interesse daran, dass der Provider die Gesamtverantwortung für die Services im Sinn eines Generalunternehmers übernimmt *(End-to-End-Services)*.
– *Wahrung der eigenen Handlungsfähigkeit* für den Fall, dass der Cloud Provider die Leistungen einstellt oder nicht zu angemessenen Konditionen weiter erbringen will.
– *Kostenkontrolle*[20].

Nachfolgend wird im Sinn einer *systematischen Vorgehensweise*[21] skizziert, welche Fragen vor der Inanspruchnahme von Cloud Services geklärt werden sollten. Zudem wird auf einige typische Rechtsfragen eingegangen, welche Verträge über cloudbasierte Leistungen (nachfolgend als Cloud Service Verträge bezeichnet) mit sich bringen können.[22] Die hier vorgeschlagene Vorgehensweise ist vor allem auf private Unternehmen und Organisationen zugeschnitten. Für Gemeinwesen stellen sich neben der Beachtung des Legalitätsprinzips insbesondere auch Fragen der staatlichen Souveränität.[23]

2. Vorgehensweise

Die Qualität von Cloud Service Verträgen zeigt sich vor allem daran, inwieweit diese der Zielsetzung des konkre-

---

C. Baumgartner, Cloud Computing – Vertragsgestaltung als Teil des Risikomanagements, in: Daniel Lengauer/Giordano Rezzonico (Hrsg.), Chancen und Risiken rechtlicher Neuerungen 2011/2012, Zürich 2012, 104–112, 107; Andreas C. Baumgartner, Cloud computing – La rédaction du contrat en tant qu'élément de la gestion des risques, in: Daniel Lengauer/Giordano Rezzonico (Hrsg.), Perspectives et risques de nouveautés juridiques 2011/2012, Zürich 2012, 104–112, 110; Fröhlich-Bleuler (FN 11), Rz. 2444;.

13 Siehe zur Abgrenzung zwischen Cloud Computing und IT Outsourcing auch Fabian Schuster/Wolfgang Reichl, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen? Computer und Recht 2010, 38–43, 38 ff.

14 Siehe dazu auch Thomas Söbbing, Cloud Computing, die Zukunftsvisionen von Amazon, Google und Microsoft rechtlich betrachtet, jusletter vom 10.8.2009.

15 Siehe dazu im Einzelnen Abschnitt 3–6.

16 Siehe zur Bedeutung von Unterstützungsleistungen bei E-Discovery Verfahren Hon/Millard/Walden (FN 7), 116.

17 Siehe zu den Archivierungsvorschriften Abschnitt 3.

18 Das *Rundschreiben der FINMA* Outsourcing Banken 2008/7 sowie Anhang 3 des Rundschreibens der FINMA Operationelle Risiken Banken 2008/21 gelten grundsätzlich nur für die Finanzbranche. Die darin erwähnten Grundsätze könnten aber als «best practice» auch für andere Branchen herangezogen werden – insbesondere wenn es um die Bestimmung der erforderlichen Sorgfalt im Umgang mit Kundendaten geht.

19 Vorliegend werden die Bezüger von Cloud Services unabhängig von der rechtlichen Qualifikation des Vertragsverhältnisses jeweils als «Auftraggeber» bezeichnet, die Leistungserbringer als «Provider».

20 Siehe dazu Abschnitt. 8.

21 Siehe zur Vorgehensweise bei der Erarbeitung von Verträgen generell Rainer Schumacher, Vertragsgestaltung, Systemtechnik für die Praxis, Zürich/Basel/Genf 2004, 64 ff.; Wolfgang Straub, Legal Engineering – eine neue Disziplin? Jusletter vom 24.5.2004,.

22 Siehe dazu auch David Schwaninger/Stephanie S. Lattmann, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, jusletter vom 11.3.2013; Rauno Hoffmann, Cloud Computing, ST 2012, 465–469.

23 Siehe dazu auch *www.isb.admin.ch/themen/architektur/00183/01368/01372/index.html?lang=de*.

ten Vorhabens und der Eigenart der jeweiligen Services[24] Rechnung tragen.[25] Der Ausarbeitung individueller Verträge sollte daher eine Analyse der *Interessenlage* beider Parteien und der wirtschaftlichen, technischen und rechtlichen *Chancen* und *Risiken* vorangehen.[26] Das ist nicht zwingend mit einem grossen Aufwand verbunden. Oft bringt es bereits etwas, im Rahmen eines Brainstormings festzuhalten, wofür man die Cloud nutzen möchte und was dabei alles schiefgehen könnte.

In einem ersten Schritt sollten der *in der Cloud zu betreibende Leistungsbereich* definiert und die rechtlichen Rahmenbedingungen ermittelt werden.[27] Es ist insbesondere zu bestimmen, welche Daten in der Cloud gespeichert und verarbeitet werden sollen und zu welchem Zweck die Bearbeitung erfolgt:

- Handelt es sich um *Personendaten,* gar um besonders schützenswerte Personendaten oder Persönlichkeitsprofile?[28] Könnten Personendaten allenfalls vollständig anonymisiert[29] oder pseudonymisiert werden? Sind die Daten als intern, vertraulich oder geheim klassifiziert?
- *Welche Vorschriften sind auf diese Daten anwendbar:* schweizerische und/oder ausländische Datenschutzvorschriften, spezialgesetzliche Geheimhaltungsvorschriften?
- Bestehen *besondere regulatorische Vorgaben* an die Auslagerung der Datenverarbeitung (z.B. für Versicherungs- und Bankdaten oder Daten der öffentlichen Hand)?
- Sind die erforderlichen *immaterialgüterrechtlichen Befugnisse* zur Nutzung von geschützten Inhalten[30], Software etc. vorhanden?[31]
- Unterliegen die Daten besonderen *Nachweis- und Archivierungsvorschriften* (z.B. Geschäftsbücherverordnung, Sozialversicherungsrecht, Mehrwertsteuerrecht)?

In einem zweiten Schritt sind die *Kriterien für die Auswahl*[32] *und die Zusammenarbeit* mit dem Cloud Provider festzulegen.[33]

In einem dritten Schritt ist anhand des konkreten Projekts zu prüfen, ob der Provider – und allfällige Subunternehmer des Providers – über die fachlichen, technischen und personellen *Ressourcen* verfügen und wie die *rechtlichen Anforderungen* eingehalten werden können.

---

24 Siehe zu den typischen Chancen und Risiken der einzelnen Service Layers den Eurocloud Leitfaden Risk & Compliance, online verfügbar unter *www.eurocloudswiss.ch/index.php/publikationen/leitfaden,* 12 ff.; Bundeskanzleramt Österreich (Hrsg.), Österreichisches Informationssicherheitshandbuch – Cloud Strategie, online verfügbar unter *https://www.sicherheitshandbuch.gv.at/downloads/Cloud.pdf,* 8 ff.; Ralf Blaha, in: Ralf Blaha (Hrsg.), Rechtsfragen des Cloud Computing; Vertragsrecht – Datenschutz – Risiken und Haftung, Wien 2011, 92 ff.

25 Siehe dazu auch Andreas C. Baumgartner, Cloud Computing – Vertragsgestaltung (FN 12), 105 ff.; Baumgartner, Cloud computing – La rédaction du contrat (FN 12), 107 ff.

26 Siehe dazu auch FINMA Rundschreiben 2008/7 Outsourcing Banken, Rz. 19 f. und Rz. 22; Urs Egli, Outsourcing und IT-Governance, jusletter IT vom 6.6.2012, Rz. 24 ff.

27 Die hier empfohlene Vorgehensweise ist an die Anforderungen des konkreten Vorhabens anzupassen. Siehe zu den Planungsschritten bei Projekten der öffentlichen Hand Eurocloud Leitfaden Cloud Computing – Öffentliche Auftragsvergabe, online verfügbar unter *www.eurocloudswiss.ch/index.php/publikationen/leitfaden,* Kap. 8; Wolfgang Straub, Beschaffung komplexer Leistungen zwischen Vertragsfreiheit und Beschaffungsrecht, AJP/PJA 2005, 1330–1340, 1330 ff.

28 Siehe dazu auch Philippe Meier, Protection des données: Fondements, principes généraux et droit privé, Bern 2011, Rz. 793, welcher je nach Missbrauchspotential vier Klassen der Schutzwürdigkeit von Personendaten unterscheidet.

29 Siehe zur Anonymisierung von Personendaten Abschnitt 3.

30 Siehe zur Nutzung von urheberrechtlich geschützten Inhalten im Rahmen des Cloud Computing Nicole Beranek Zanon/Carmen de la Cruz Böhringer, Urheberrechtliche Beurteilung von IaaS- (und XaaS)-Cloud-Diensten für die betriebliche Nutzung gemäss Art. 19 URG, sic 2013, 663–680.

31 Der Provider muss über die nötigen Immaterialgüter- oder Lizenzrechte verfügen, um dem Auftraggeber die Nutzung von Software etc. im Rahmen der Cloud Services zu ermöglichen. Wenn der Kunde eigene Software auf Plattformen des Providers betreiben will, muss er selbst sicherstellen, dass er über entsprechende Nutzungsrechte verfügt. Siehe dazu Wolfgang Straub, Softwareschutz – Urheberrecht, Patentrecht, Open Source, Zürich/St. Gallen 2011, Rz. 218 ff.; de la Cruz (FN 12), Rz. 36 ff.; Baumgartner, Cloud Computing – Vertragsgestaltung (FN 12), 110; Hon/Millard/Walden (FN 7), S. 125 f. Siehe zur Nutzung von Open Source Software Henriette Picot, Dealing with Open Source Software Licenses in Outsourcing Transactions, Computer und Recht international 2010, 9–12.

32 Als Auswahlkriterien kommen insbesondere auch Zertifizierungen des Providers und seiner Subunternehmer sowie das Vorhandensein von Datenschutzverantwortlichen im Sinn von Art. 11a Abs. 5 lit. e DSG in Betracht. Siehe auch Eurocloud Leitfaden Risk & Compliance (FN 24), 23 und 28. Derzeit gibt es keine datenschutzrechtlichen Zertifizierungen von Cloud Services gemäss Art. 11 DSG bzw. Art. 5 VDSZ. Siehe dazu auch *http://www.edoeb.admin.ch/datenschutz/00756/00757/index.html?lang=d;* Caroline Gloor Scheidegger/Karin Koç, Datenschutzzertifizierung: Stand der Dinge, Digma 2/2010, 74 f. Siehe zur datenschutzrechtlichen Bedeutung von sonstigen Zertifizierungen Meier (FN 28), Rz. 1238; David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz sowie weiteren ausgewählten Bestimmungen, Zürich 2008, N. 127 zu Art. 10a DSG.

33 Siehe FINMA Rundschreiben 2008/7 Outsourcing Banken, Rz. 22, sowie Rundschreiben der FINMA Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 47 f.

Dazu kann auch ein spezifisches Due Diligence Verfahren durchgeführt werden, in welchem z.B. die Services getestet, die Informationssicherheit der Systeme des Providers und die Portierbarkeit von Applikationen und Datenformaten geprüft werden.[34] Auch wenn die Analyse ergibt, dass die rechtlichen Rahmenbedingungen eingehalten werden, bestehen unter Umständen Restrisiken, welche transparent ausgewiesen werden sollten. Nur so kann ein bewusster und nachvollziehbarer Entscheid darüber gefällt werden, ob das betreffende Risiko akzeptiert wird.[35]

Anschliessend sind die Zuständigkeiten, Schnittstellen und Verantwortlichkeiten[36] zwischen den Parteien zu klären und vertraglich zu regeln.[37] Ich habe meine eigene *Checkliste* zum vertraglichen Regelungsbedarf in Cloud Verträgen veröffentlicht.[38] Solche Checklisten können zwar Denkanstösse geben, eine individuelle Prüfung der zu regelnden Themen aber nie ersetzen.

Während der Vertragsvollzugsphase ist der Cloud Provider durch den Auftraggeber zu *instruieren* (z.B. über Vorschriften bei der Datenbearbeitung) und zu *überwachen*[39] (z.B. durch Audits[40] oder Datenschutzberichte[41]). Dies setzt auch auf Seiten des Auftraggebers entsprechende Ressourcen voraus. Der ausgelagerte Bereich ist gegebenenfalls auch in das interne Kontrollsystem des Auftraggebers zu integrieren.[42] Im Fall von schwerwiegenden Verstössen gegen gesetzliche oder vertragliche Bestimmungen muss die Datenverarbeitung in der Cloud unter Umständen beendet werden.[43]

---

34 Im Rahmen einer vorvertraglichen Due Diligence können z.B. Security Audits oder Penetration Tests durchgeführt werden, mit denen die Resistenz eines Testsystems des Providers gegenüber Hackerangriffen geprüft wird. Siehe dazu auch Hon/Millard/Walden (FN 7), 112 f. und 121. Es können aber auch die finanziellen und personellen Ressourcen des Providers geprüft werden.

35 Siehe dazu auch Wolfgang Straub, Verantwortung für Informationstechnologie – Gewährleistung, Haftung und Verantwortlichkeitsansprüche, Zürich/St. Gallen 2008, Rz. 578 und Rz. 583.

36 Siehe in Bezug auf Banken auch FINMA Rundschreiben Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 5 f. Gemäss dem FINMA Rundschreiben 2008/7 Outsourcing Banken müssen auch Haftungsfragen im Vertrag adressiert werden. In Bezug auf die Haftung kann grundsätzlich auch bloss auf die Vorschriften des Obligationenrechts verwiesen werden. Allerdings werden Cloud Service Verträge vom Vertragstypensystem des OR nicht spezifisch normiert – nach dem hier vertretenen Verständnis handelt es sich um einen in der Praxis herausgebildeten Typ von Dauerdienstleistungsverträgen. Ein Abstellen auf das dispositive Gesetzesrecht lässt – jedenfalls solange es an entsprechender höchstrichterlicher Rechtsprechung fehlt – einige für Gewährleistung und Haftung relevanten Fragen offen (z.B. die anwendbaren Verjährungsfristen). Diese sollten vertraglich geklärt werden. Siehe dazu Straub, Verantwortung für Informationstechnologie (FN 35), Rz. 326 ff.; sowie in Bezug auf Verletzungen des Datenschutzrechts Philippe Fuchs, Cloud Computing – eine datenschutzrechtliche Betrachtung, jusletter IT vom 6.6.2012, Rz. 32 f. Siehe zudem den Überblick über typische Haftungsbestimmungen in internationalen Cloud Service Verträgen bei Hon/Millard/Walden (FN 7), 92 f. und 102 f.

37 Im FINMA Rundschreiben 2008/7 Outsourcing Banken, Rz. 23 und 25, werden folgende Mindestinhalte für Outsourcingverträge genannt: Abgrenzung der Zuständigkeiten von Auftraggeber und Provider, Schnittstellen, Verantwortlichkeiten und Haftungsfragen, Einsichts-, Weisungs- und Kontrollrechte.

38 Wolfgang Straub, Cloud Computing – Checkliste zum vertraglichen Regelungsbedarf, jusletter vom 14.7.2014. Weitere Checklisten finden sich auch in den Eurocloud Leitfäden zum Cloud Computing, online verfügbar unter *www.eurocloudswiss.ch/index.php/publikationen/leitfaden*. Siehe insbesondere den detaillierten Fragekatalog zur Informationssicherheit im Leitfaden Risk & Compliance, Kap. 6, S. 28 ff. Eine Checkliste für Audits findet sich bei Ben Halpert (Hrsg.), Auditing Cloud Computing: A Security and Privacy Guide, Hoboken NJ 2011, 175 ff. Siehe zudem die Checkliste des Branchenverbandes Swiss ICT zu Outsourcingverträgen, online verfügbar unter *www.modellvertraege.ch,* die Checkliste Outsourcing Contracts Control Review des Switzerland Chapters der Information Systems Audit and Control Association, online verfügbar unter *http://www.isaca.ch* sowie die Checkliste des Datenschutzbeauftragten des Kantons Zürich, online verfügbar unter *http://stadt.winterthur.ch/fileadmin/user_upload/Portal/Dateien/Datenaufsicht/Checklisten_f%C3%BCr_Outsourcing-Vertr%C3%A4ge.pdf*. Diese sind allerdings nicht spezifisch auf Cloud Service Verträge zugeschnitten.

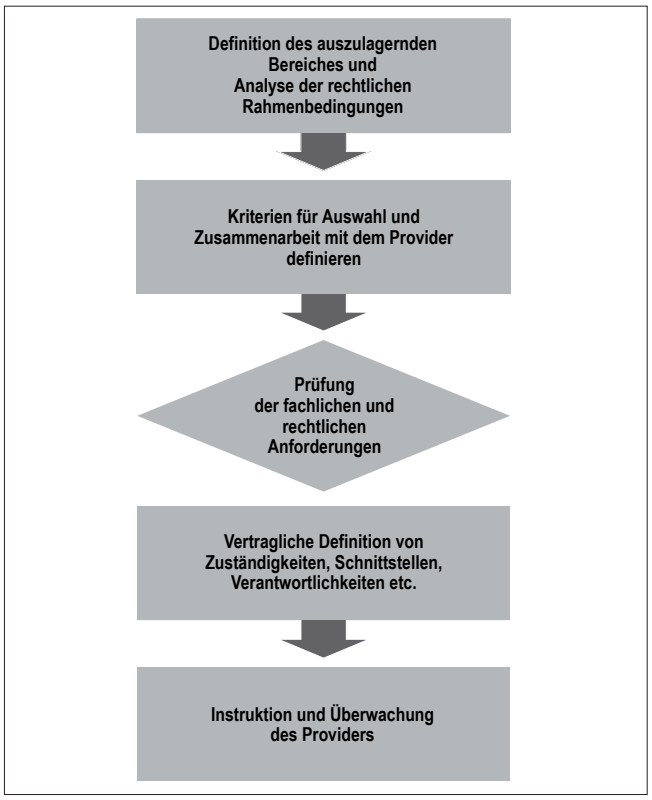
39 Siehe dazu auch Astrid Epiney/Tobias Fasnacht, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht: Grundlagen und öffentliches Recht, Bern 2011, 588 f., Rz. 43 f.

40 Grosse Cloud Provider sind oft im Bereich der Informationssicherheit zertifiziert (z.B. entsprechend ISO 27 001). Provider weigern sich mit Verweis auf die Sicherheit aber häufig, die entsprechenden Auditberichte gegenüber ihren Kunden offen zu legen. In Cloud Service Verträgen sollte daher definiert werden, welche Teile dieser Berichte offen gelegt werden müssen (insbesondere diejenigen, welche den Auftraggeber betreffen).

41 Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 40 zu Art. 6 DSG und N. 123 zu Art. 10a DSG, wonach im Falle sensibler Daten jährliche interne oder externe Audits oder Datenschutzberichte erforderlich sind. In wenig heiklen Bereichen könne es hingegen genügen, die Aktivitäten des Providers in der Öffentlichkeit zu verfolgen, bei Hinweisen auf Datenschutzverletzungen eine Stellungnahme zu verlangen und gegebenenfalls den Vertrag zu beenden.

42 Siehe in Bezug auf Banken FINMA Rundschreiben 2008/7 Outsourcing Banken, Rz. 24, sowie Rundschreiben der FINMA Operationelle Risiken Banken 2008/21, Anhang 3.

43 Siehe dazu Art. 2 Abs. 3 des Mustervertrages des Europarats sowie Fuchs (FN 36), Rz. 14 f.

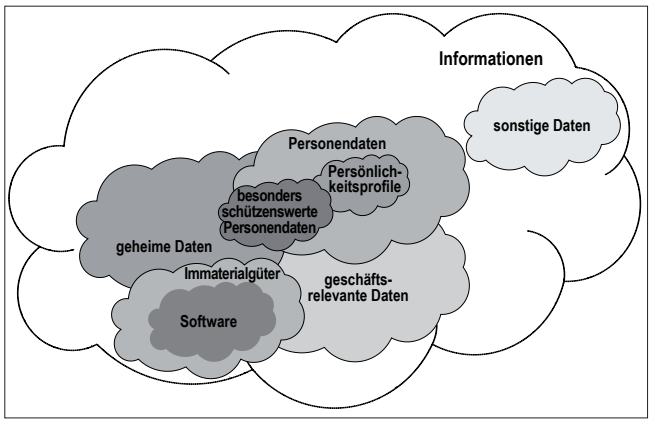


Grafik 2
Schematische Darstellung der Vorgehensweise

3. Generelle Anforderungen an den Schutz von Daten

Daten werden zunächst einmal auf physischen *Speichermedien* gespeichert. Diese stehen meistens im Eigentum des Cloud Providers oder eines Dritten (z.B. eines Leasinggebers oder eines Subunternehmers). Im Rahmen einer *Private Cloud* kann der Auftraggeber zwar auch eigene Server[44] durch einen Provider betreiben lassen und sich so die Eigentümerstellung an Datenträgern sichern – die Vorteile der kostengünstigen Skalierbarkeit ergeben sich allerdings nur, wenn die entsprechende Infrastruktur durch den Provider zur Verfügung gestellt wird. In der Regel besteht auch kein immaterialgüterrechtlicher Anspruch auf Herausgabe von Daten.[45] Um sich Rechte an eigenen Daten zu sichern, sind somit die vertraglichen Regelungen und die organisatorischen und technischen Abläufe entscheidend.

Im Hinblick auf die rechtlichen Anforderungen an den Umgang mit Daten ist zwischen *geschäftsrelevanten Daten, Personendaten, geheimen Daten*[46] und *sonstigen Daten* zu unterscheiden, wobei sich die Kategorien auch überschneiden können.[47]



Grafik 3
Schematische Darstellung unterschiedlicher Informationsarten

In Bezug auf *geschäftsrelevante Daten* bestehen Sorgfaltspflichten von Arbeitnehmern und Geschäftsleitungsmitgliedern, Buchführungs- und Aufbewahrungspflichten. Geschäftsrelevante Daten und Dokumente müssen insbesondere so aufbewahrt werden, dass sich feststellen lässt, ob sie nachträglich verändert wurden. Das bedeutet, dass für solche Daten – unabhängig davon, ob sie auf eigenen Servern des Unternehmens oder bei einem Cloud Provider gespeichert sind – zusätzliche Massnahmen getroffen werden müssen. Geschäftsrelevante Daten können insbesondere mit einer digitalen Signatur und einem

---

[44] Eine entsprechende Eigentümerstellung setzt voraus, dass für einen bestimmten Kunden nicht nur virtuelle Server auf Hardware des Providers aufgesetzt werden. Siehe dazu auch FN 4.

[45] Ein Herausgabeanspruch an Daten könnte sich in Ausnahmefällen aus dem in Art. 15 URG vorgesehenen Schutz vor Zerstörung urheberrechtlich geschützter Werke ergeben. Wenn der Provider wesentliche Investitionen für Strukturierung der Daten getragen hat, könnte er – falls EU-Recht anwendbar ist – allenfalls seinerseits Rechte entsprechend der Datenbank-Richtlinie 96/9 EG geltend machen.

[46] Geheime Daten in einem weiteren Sinn umfassen einerseits Daten, welche einer spezialgesetzlichen Geheimhaltungspflicht unterstehen (z.B. Bankkundendaten, medizinische Daten, unter ein Amtsgeheimnis fallende Daten), andererseits Daten, an welchen ein sonstiges Geheimhaltungsinteresse besteht (z.B. Rezepturen, Bezugsquellen, Preiskalkulationen). Letztere sind rechtlich durch Art. 4 lit. c und Art. 6 UWG sowie Art. 273 StGB gegenüber einem Ausspionieren geschützt. Gemeinwesen klassifizieren in der Regel interne, vertrauliche und geheime Daten, für die je unterschiedliche Sicherheitsanforderungen gelten.

[47] Im Rahmen von Cloud Services entstehen oft auch Metadaten (z.B. Daten zur Beschreibung und Indexierung von Files) und Randdaten (z.B. Daten über das Verhalten der Benutzer, Logsfiles, Auditberichte etc.). Diese können ihrerseits Datenschutz- oder Geheimhaltungsvorschriften unterstehen.

elektronischen Zeitstempel versehen werden.[48] Die Abläufe und Verfahren müssen aber schriftlich festgelegt und dokumentiert werden. Zudem sind die entsprechenden Hilfsinformationen aufzubewahren (z.B. Protokolle und Logfiles). Aufgrund der technischen Entwicklung müssen heute als unveränderbar geltende Daten im Lauf der Aufbewahrungsdauer eventuell auf eine höherwertige Verschlüsselung migriert werden. Bei einer Speicherung geschäftsrelevanter Daten in der Cloud ist die Dokumentation der Datenverarbeitungsprozesse von besonderer Bedeutung.[49] Neben den handelsrechtlichen Aufbewahrungsvorschriften sind gegebenenfalls auch steuer- und sozialversicherungsrechtliche Vorgaben zu beachten.[50] Da die Daten bis zum Ablauf der Verjährungsfristen jederzeit in beweissicherer Form lesbar sein müssen, sollte in Cloud Service Verträgen ein entsprechendes Prüfungsrecht verankert und periodisch ausgeübt werden.

Sofern es sich um Geschäftsgeheimnisse, medizinische Daten, Bankdaten, Klientendaten von Anwälten[51] etc. handelt, bestehen überdies zivil- und strafrechtlich sanktionierte *Geheimhaltungspflichten.*[52] Es ist kontrovers, inwieweit solche Daten ohne individuelle Zustimmung der Betroffenen ausgelagert werden dürfen.[53] Jedenfalls sollte der Provider als Gehilfe den entsprechenden Geheimhaltungsvorschriften und dem Weisungsrecht des Auftraggebers unterstellt werden[54]. Der Zugriff muss auf jene Personen beschränkt werden, welche die Daten zu ihrer Aufgabenerfüllung effektiv benötigen.[55] Zudem sollten die geheim zu haltenden Informationen so von sonstigen

---

48 Siehe Art. 9 Abs. 1 lit. b GeBüV.

49 In Bezug auf die Aufbewahrungsplichten muss auf die Spezialliteratur verwiesen werden. Siehe dazu Jaques Beglinger/Daniel Burgwinkel/Beat Lehmann/Peter K. Neuenschwander/Bruno Wildhaber, Records Management, Leitfaden zur Compliance bei der Aufbewahrung von elektronischen Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern, Vorlagen, 2. A. Zürich 2008; Benjamin Chapuis, Conservation des documents – enjeux juridiques, ST 2011, 590–594; Patrick Kos, Rechtliche Anforderungen an die elektronische Schriftgutverwaltung in der Privatwirtschaft und Zertifizierungen nach ISO 15489-1 und ISO/IEC 27001, Zürich/St. Gallen 2011, zugl. Diss. St. Gallen 2011; Peter K. Neuenschwander, Elektronische Buchführung und Aufbewahrung, in: Walter Fellmann/ Thomas Poledna (Hrsg.), Aktuelle Anwaltspraxis 2001, Bern 2002, 122 f.; Peter K. Neuenschwander/Jeanette Heiniger, Checkliste elektronische Archivierung – rechtliche Rahmenbedingungen, online verfügbar unter *www.rwi.uzh.ch/oe/zik/archiv/ChecklisteElektronische Archivierung.pdf;* Wolfgang Straub, Aufbewahrung und Archivierung in der Anwaltskanzlei, AJP/PJA 2010, 547–56; Ursula Sury (FN 11), 107 ff.; Rolf H. Weber, Elektronische Aufbewahrung und Archivierung, recht 2004, 67–77; Rolf H. Weber/Annette Willi, IT-Sicherheit und Recht, Zürich 2006, 208–224; Maria Winkler, Neue Buchführungs- und Rechnungslegungsvorschriften: darf die Geschäftskorrespondenz nun vernichtet werden? TREX 2013, 88 f.; Jürg Schneider, Informationssicherheit in der IT und persönliche Haftung der Verwaltungsräte, ZSR Beiheft 48, 2008, 3 ff.

50 Siehe zu den mehrwertsteuerrechtlichen Anforderungen an die Auslagerung der Datenverarbeitung insbesondere Art. 3, 7 und 9 f. der Verordnung des EFD über elektronische Daten und Informationen (ElDI-V, SR 641.201.511). Die Übermittlung und Archivierung der Daten muss mittels einer fortgeschrittenen elektronischen Signatur im Sinn des Bundesgesetzes über die elektronische Signatur (ZertES, SR 943.03) erfolgen. Bei einer Archivierung elektronischer Rechnungsbelege auf Servern im Ausland muss ein Zugriff von der Schweiz aus jederzeit möglich sein. Für die Bearbeitung mehrwertsteuerrelevanter Daten bleibt gegenüber der Eidgenössischen Steuerverwaltung immer der Auftraggeber verantwortlich. Der Cloud Provider untersteht jedoch einer Auskunftspflicht. Siehe zu den steuerrechtlichen Aspekten von Cloud Service Verträgen auch Eurocloud Leitfaden Cloud Computing – steuerliche Aspekte in der DACH-Region, online verfügbar unter *www.eurocloudswiss.ch/index.php/publikationen/leitfaden.*

51 Siehe zur Nutzung von cloudbasierten Services in Anwaltskanzleien Sébastien Fanti, Cloud Computing: opportunités et risques pour les avocats, Revue de l'avocat 2013 S. 74–77; Adrian Rufener, Arbeiten in der Cloud, Anwaltsrevue 2013, 295 f.

52 Siehe die Übersicht über die einschlägigen Geheimhaltungsbestimmungen bei Epiney/Fasnacht (FN 39), 590 f., Rz. 46. In strafrechtlicher Hinsicht ist eine Weitergabe an Hilfspersonen dann zulässig, wenn diese ebenfalls dem Berufsgeheimnis unterstehen. Siehe dazu auch Schwaninger/Lattmann (FN 22), Rz. 29 ff. Für die Auslagerung von Bankkundendaten gelten teilweise spezifische Regeln. Siehe dazu FINMA Rundschreiben 2008/7 Outsourcing Banken, Rz. 37 ff. sowie Rundschreiben der FINMA Operationelle Risiken Banken 2008/21, Anhang 3.

53 Das Vorliegen einer vertraglichen oder gesetzlichen Geheimhaltungspflicht macht eine Auslagerung der Datenverarbeitung nicht *per se* unzulässig. Siehe dazu auch Meier (FN 28), Rz. 1224 und 1229 ff. Vielmehr ist durch Auslegung der entsprechenden Bestimmungen zu prüfen, inwieweit ihrerseits zur Geheimhaltung verpflichtete Dritte in eine Datenbearbeitung einbezogen werden dürfen. Siehe dazu Rosenthal/Jöhri (FN 32), 104 ff. zu Art. 10a DSG. Nach Epiney/Fasnacht (FN 39), 592, Rz. 50, ist gegenüber einer Auslagerung der Bearbeitung von unter ein Berufsgeheimnis fallenden Daten ins Ausland generell Zurückhaltung angebracht. Tatsächlich untersteht der Provider bei einer Datenverarbeitung im Ausland nicht dem schweizerischen Berufsgeheimnis. Zudem greift auch der Schutz von Art. 271 und 273 StGB nicht. Schwaninger/Lattmann (FN 22), Rz. 31 f., gehen daher davon aus, dass in solchen Fällen grundsätzlich eine Einwilligung der betroffenen Personen zur Auslagerung der Datenbearbeitung notwendig ist. Nach der hier vertretenen Auffassung sollte eine Auslagerung jedenfalls dann möglich sein, wenn die betroffenen Personen mit einer Auslagerung generell rechnen müssen und eine Einhaltung der Schutzanforderungen auf anderem Weg sichergestellt werden kann (insbesondere technische Massnahmen und vertragliche Garantien).

54 Siehe dazu auch die entsprechenden Formulierungsvorschläge bei Rosenthal/Jöhri (FN 32), N. 71 ff. zu Art. 10a DSG.

55 Dass nur diejenigen Personen Zugriff zu den Daten erhalten dürfen, welche diese zur Auftragserfüllung effektiv benötigen, ergibt sich bereits aus dem Verhältnismässigkeitsprinzip. Siehe dazu auch Meier (FN 28), Rz. 1234.

Daten abgekapselt werden, dass die Zugriffsmöglichkeiten vom Auftraggeber kontrolliert werden können.[56]

Eine umfassende Darstellung der *datenschutzrechtlichen Anforderungen* an die Auslagerung von Daten würde den Rahmen des vorliegenden Beitrages sprengen. Ergänzend muss daher auf die Spezialliteratur verwiesen werden.[57] Es besteht auch die Möglichkeit, konkrete Sachverhalte dem EDÖB vorab zur Beratung zu unterbreiten.[58] Die Verantwortung bleibt aber letztlich stets beim Inhaber der Datensammlung.

Personendaten[59] müssen durch *angemessene technische und organisatorische Massnahmen* gegen unerlaubte Bearbeitungen geschützt werden.[60] Diese sollten in der Regel in einem Sicherheitskonzept definiert werden.[61] Es sollen insbesondere unbefugte oder zufällige Vernichtung, technische Fehler und unbefugtes Zugreifen, Kopieren und Ändern verhindert werden.[62] Bei der Beurteilung, welche Massnahmen angemessen sind, muss im Sinn einer Abwägung der Interessen aller Beteiligten[63] dem Zweck, der Art und dem Umfang der Datenbearbeitung, den möglichen Risiken für die betroffenen Personen und dem Stand der Technik Rechnung getragen werden. Die technischen und organisatorischen Anforderungen können somit nur bezogen auf den Einzelfall beurteilt werden.[64] Für den Fall von Sicherheitslecks sollten vertragliche Informationspflichten vorgesehen werden.[65] Zudem muss periodisch überprüft werden, ob die Sicherheitsmassnahmen noch angemessen sind.[66] Sowohl für den Inhaber der Datensammlung als auch für den Provider[67] ist die Beurteilung, welche Massnahmen erforderlich sind, deshalb heikel, weil eine Bearbeitung von Personendaten, welche den entsprechenden Anforderungen nicht genügt, als Persönlichkeitsverletzung gilt.[68]

Zumindest bei der Nutzung von *Software as a Service* erfolgt die technische Datenverarbeitung durch den Provider[69]. Die *Auftragsdatenverarbeitung durch Dritte*[70] ist

---

56 Siehe dazu auch Eurocloud Leitfaden Risk & Compliance (FN 24), 18.

57 Siehe dazu Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Erläuterungen zu Cloud Computing vom 20.2.2012, online verfügbar unter *www.edoeb.admin.ch;* Rolf H. Weber/Dominic N. Staiger, Legal Challenges of Trans-border Data Flow in the Cloud, jusletter IT vom 15.5.2013, mit weiteren Hinweisen; Fuchs (FN 36); Schwaninger/Lattmann (FN 22), Rz. 5 ff.; Hoffmann (FN 22), 466 ff. Siehe zum europäischen Datenschutzrecht Kirstin Brennscheidt, Cloud Computing und Datenschutz, Baden-Baden 2013, zugl. Diss. Bochum 2013, 47 ff.; Florian Jotzo, Der Schutz personenbezogener Daten in der Cloud, Baden-Baden 2103, zugl. Diss. Kiel 2013, 146 ff.; Andreas Zellhofer/Helmut Liebel, in: Ralf Blaha (Hrsg.), Rechtsfragen des Cloud Computing, Vertragsrecht – Datenschutz – Risiken und Haftung, Wien 2011, 65 ff.

58 Art. 28 DSG. Siehe dazu auch Schwaninger/Lattmann (FN 22), Rz. 70.

59 Zu den Personendaten gehören auch die Logindaten der Systeme. In ein Sicherheitskonzept sind gegebenenfalls aber auch nicht personenbezogene Daten einzubeziehen (z.B. Pläne, Rezepturen, Konzepte).

60 Siehe dazu auch Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, *http://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=de*.

61 Siehe dazu Epiney (FN 39), S. 557 f., Rz. 57; Kurt Pauli, in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Basler Kommentar zum Datenschutzgesetz, 2. A., Basel 2006, N. 6 zu Art. 7 Datenschutzgesetz; zurückhaltend Rosenthal/Jöhri (FN 32), N. 4 zu Art. 7 DSG. Siehe in Bezug auf Banken FINMA Rundschreiben Operationelle Risiken Banken 2008/21, Anhang 3.

62 Art. 7 DSG in Verbindung mit Art. 8 VDSG. Siehe dazu im Einzelnen Rosenthal/Jöhri (FN 32), N. 18 ff. zu Art. 7 DSG; Pauli (FN 61), N. 2 und 11 ff. zu Art. 7 DSG.

63 Siehe zur Interessenabwägung auch Rosenthal/Jöhri (FN 32), N. 3 zu Art. 7 DSG; Epiney/Fasnacht (FN 39), S. 582, Rz. 34.

64 Bei der Bestimmung der im konkreten Fall erforderlichen Sicherheitsmassnahmen ist insbesondere das Verhältnismässigkeitsprinzip zu beachten. Siehe dazu Epiney (FN 39), S. 555, Rz. 53. Ein Überblick über gängige Sicherheitsstandards findet sich bei Meier (FN 28), Rz. 802; Rosenthal/Jöhri (FN 32), N. 15 ff. zu Art. 7 DSG; Pauli (FN 61), N. 9 ff. zu Art. 7 DSG.

65 Aus dem Grundsatz der Datenbearbeitung nach Treu und Glauben kann sich unter Umständen auch eine Informationspflicht des Inhabers der Datensammlung gegenüber den Betroffenen über Sicherheitspannen ergeben. Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 16 zu Art. 4 DSG. Vertraglich sollte aber auf jeden Fall eine sofortige und umfassende Informationspflicht über sicherheitsrelevante Incidents und Datenschutzverletzungen vorgesehen werden. Banken müssen zudem über eine Kommunikationsstrategie für schwerwiegende Sicherheitslecks verfügen und gegebenenfalls die FINMA orientieren. Siehe dazu FINMA Rundschreiben Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 42 ff.

66 Siehe dazu auch Meier (FN 28), Rz. 795; Rosenthal/Jöhri (FN 32), N. 5 zu Art. 7 DSG; Epiney (FN 39), S. 556, Rz. 54, die davon ausgehen, dass das Sicherheitsniveau jährlich sowie bei wichtigen Änderungen (insbesondere der IT-Infrastruktur) überprüft werden muss.

67 Unabhängig von den vertraglichen Regelungen zur Datensicherheit trifft auch den Provider eine datenschutzrechtliche Pflicht, für einen angemessenen Schutz zu sorgen. Entsprechende Ansprüche können von den Geschädigten gestützt auf Art. 7 Abs. 1 DSG in Verbindung mit Art. 12 und Art. 15 DSG direkt gegenüber dem Provider geltend gemacht werden. Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 6 und 10 zu Art. 7 DSG; Epiney (FN 39), S. 556, Rz. 55.

68 Art. 12 Abs. 2 lit. a DSG. Siehe dazu Rosenthal/Jöhri (FN 32), N. 10 zu Art. 7 DSG mit weiteren Hinweisen; Meier (FN 28), Rz. 796; Pauli (FN 61), N. 2 und 18 f. zu Art. 7 DSG.

69 Sofern der Provider die Datenverarbeitung seinerseits an einen Subunternehmer auslagert, haben sowohl der Auftraggeber als auch der Provider in Bezug auf den Subunternehmer die Anforderungen von Art. 10a und Art. 6 DSG zu beachten. Der Auftraggeber hat sicherzustellen, dass eine wirksame Kontrollkette vorhanden ist. Siehe dazu Rosenthal/Jöhri (FN 32), N. 14 zu Art. 6 DSG und N. 77 zu Art. 10a DSG; Schwaninger/Lattmann (FN 22), Rz. 13; Fuchs

datenschutzrechtlich grundsätzlich zulässig, sofern keine gesetzlichen oder vertraglichen Geheimhaltungspflichten die Auslagerung verbieten.[71] Wenn der Auftraggeber selbst nicht über die entsprechenden Kompetenzen verfügt, kann die Datensicherheit eine Auslagerung der Datenbearbeitung an externe Spezialisten unter Umständen sogar erforderlich machen. Der Provider darf die Daten aber nur im gleichen Umfang verarbeiten, wie dies auch der Auftraggeber tun dürfte. Insbesondere darf er sie nicht für eigene oder fremde Zwecke nutzen (z.B. durch Versand personalisierter Werbung an die betreffenden Personen oder durch Vermischung mit anderen Kundendaten). Der Auftraggeber muss zudem sicherstellen, dass der Provider die Datensicherheit gewährleistet.[72]

Durch *Anonymisierung* werden Personendaten grundsätzlich zu «Nichtpersonendaten».[73] Eine wirksame Anonymisierung liegt aber nur dann vor, wenn auch aus dem Kontext heraus keine Rückschlüsse auf die betreffenden Personen mehr möglich sind. Zu diesem Kontext können auch die im Internet verfügbaren Informationen zählen. Wenn anhand eines Datensatzes z.B. aufgrund von im Internet frei verfügbaren Informationen auf die betreffende Person rückgeschlossen werden kann, liegen somit Personendaten im Sinn des Datenschutzrechts vor, auch wenn ihr Name im Datensatz nicht enthalten ist. Wird z.B. in einem Datensatz statt eines Firmennamens eine nicht aussagekräftige Referenznummer verwendet, aber die Sitzadresse mitgespeichert, so können ein Blick ins Telefonbuch oder die Eingabe der Adresse in einer Suchmaschine bereits Rückschlüsse auf die Identität ermöglichen. Ursprünglich wirksam anonymisierte Daten können im Lauf der Zeit wieder zu Personendaten werden, wenn Informationen verfügbar werden, welche entsprechende Querbezüge erschliessen.

Ähnlich verhält es sich mit der *Verschlüsselung* der Daten: Heute als unüberwindbar geltende kryptologische Verfahren können im Lauf der Zeit ihre Wirksamkeit verlieren. Es ist anhand der Umstände des Einzelfalls zu entscheiden, welche Verschlüsselungsmethoden erforderlich sind. Beispielsweise dürften an die Verschlüsselung von Kundendaten einer Bank höhere Anforderungen gestellt werden als an jene einer Schreinerei. Eine Verschlüsselung der Daten[74] ist in der Regel allerdings nur sinnvoll, wenn die Cloud bloss zur Datenspeicherung genutzt wird, da die heute gängigen Applikationen Daten nur im Klartext weiterverarbeiten können. Sofern die Daten mit Applikationen des Cloud Providers bearbeitet werden sollen, sind Entschlüsselungsvorgänge notwendig. Dazu muss er auf die entsprechenden Schlüssel zugreifen können.[75]

4. Bearbeitung von Daten im Ausland

Heikel ist die *Auslagerung von Personendaten ins Ausland*.[76] Das schweizerische Datenschutzrecht[77] erlaubt

(FN 36) Rz. 14; Epiney/Fasnacht (FN 39), S. 587, Rz. 40 f. Siehe in diesem Zusammenhang auch den Vorschlag der Arbeitsgruppe der EU zu Artikel 29 der Richtlinie 95/46/EG vom 21.3.2014 für Musterklauseln zur Auslagerung der Datenverarbeitung von Auftragsdatenverarbeitern in der EU an Subunternehmer ausserhalb der EU, *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf*.

70 Der Begriff der Auftragsdatenverarbeitung ist im Datenschutzrecht weiter gefasst als jener des Outsourcings im FINMA Rundschreiben 2008/7 Outsourcing Banken. Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 23 zu Art. 10a DSG.

71 Der Hinweis auf sonstige gesetzliche oder vertragliche Geheimhaltungspflichten in Art. 10a Abs. 1 lit. b DSG ist allerdings nur deklaratorischer Natur. Ob eine Auslagerung zulässig ist, muss durch Auslegung der betreffenden Bestimmungen ermittelt werden. Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 101 zu Art. 10a DSG; Epiney/Fasnacht (FN 39), S. 584, Rz. 36.

72 Siehe dazu Rosenthal/Jöhri (FN 32), N. 82 zu Art. 10a DSG.

73 Siehe dazu auch Meier (FN 28), Rz. 1285. Auch IP-Adressen können den Charakter von Personendaten haben. Siehe dazu BGE 136 II 508 E. 3: Eine Person gilt dann als bestimmt, wenn sich aus der Information selbst ergibt, dass es sich genau um diese Person handelt. Bestimmbar ist die Person, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.

74 Von der Verschlüsselung der Datenspeicherung ist die Verschlüsselung der Datenübermittlung zu unterscheiden. Eine solche ist generell sinnvoll, wenn vertrauliche Daten via öffentliche Netze ausgetauscht werden.

75 Eine Bekanntgabe des Schlüssels an den Provider kann insbesondere dann problematisch sein, wenn dieser im Ausland domiziliert ist und ausländische Behörden den Schlüssel herausverlangen könnten. Siehe dazu Rosenthal/Jöhri (FN 32), N. 8 zu Art. 6 DSG sowie weiter hinten Abschnitt 5.

76 Siehe dazu Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG; Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Die Datenübermittlung ins Ausland kurz erklärt zuhanden von Bundesbehörden und Privatwirtschaft, beide online verfügbar unter *www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de;* Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Datenübermittlung ins Ausland im Rahmen eines «Out-

die Verschiebung bzw. Bearbeiten von Personendaten[78] grundsätzlich nur, wenn im betreffenden Land ein angemessener Schutz gewährleistet ist.

Datenschutzrechtlich relevant sind nicht nur die Orte, an welchen eine effektive Datenbearbeitung stattfindet, sondern auch alle anderen *Orte, von welchen aus eine Zugriffs- oder Bearbeitungsmöglichkeit* besteht.[79] Wenn Personendaten zwar in einem Rechenzentrum in der Schweiz gehostet werden, Zugriffe (z.B. durch Systemadministratoren)[80] auch aus Ländern ohne gleichwertige Datenschutzgesetzgebung möglich sind, so ist das schweizerische Datenschutzrecht bereits tangiert.[81] Dieses Problem könnte allenfalls dadurch gelöst werden, dass der Zugriff aus solchen Ländern heraus vertraglich verboten oder an die Einhaltung von Bedingungen gebunden wird. Organisatorisch/technische Massnahmen zur Sicherung des Datenschutzes sind aber in der Regel vertraglichen Vereinbarungen vorzuziehen bzw. sollten diese ergänzen.[82]

Innerhalb der EU besteht grundsätzlich ein angemessener Schutz für Daten von natürlichen Personen.[83] Für Daten von juristischen Personen sehen allerdings nur wenige Mitgliedstaaten einen entsprechenden Schutz vor. Wenn im Rahmen eines Cloud Service Vertrages Daten juristischer Personen in Länder ohne entsprechenden Schutz übermittelt werden, sollte der Auftraggeber nach der hier vertretenen Auffassung vertraglich ein angemessenes Datenschutzniveau sicherstellen.[84]

Falls im Zielland[85] keine als angemessen[86] anerkannte Datenschutzgesetzgebung[87] besteht[88], sind *zusätzliche*

---

sourcing», *www.edoeb.admin.ch/datenschutz/00626/00753/00969/index.html?lang=de;* Weber/Staiger (FN 57), Rz. 25 ff.; Fröhlich-Bleuler (FN 11), Rz. 2852 ff.; Sylvain Métille, Confier ses données à une société étrangère n'est pas sans risque, medialex 2/2013, 63 f.

77 Siehe in Bezug auf Banken auch FINMA Rundschreiben Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 19 f.

78 Konstellationen, in welchen die Betroffenen ihre Daten selbst via Webserver erfassen, gelten jedenfalls dann nicht als Datenexport im Sinn von Art. 6 DSG, wenn diese davon ausgehen müssen, dass sich der betreffende Server auch in einem Land ohne gleichwertige Datenschutzgesetzgebung befinden kann. Siehe dazu Rosenthal/Jöhri (FN 32), N. 20 zu Art. 6 DSG.

79 Wann liegt überhaupt eine Datenbearbeitung im Ausland vor? Diesbezüglich ist zu differenzieren: Im Hinblick auf das Datenschutzrecht sind der Standort der Server und die Zugriffsmöglichkeiten relevant. Siehe dazu auch Fuchs (FN 36), Rz. 18; Schwaninger/Lattmann (FN 22), Rz. 18; Brennscheidt (FN 57), 74 f. Herausgabepflichten gegenüber ausländischen Behörden können zudem auch am Sitz des Leistungserbringers oder seiner Konzerngesellschaften oder an einer Geschäftstätigkeit im betreffenden Land anknüpfen (siehe dazu Abschnitt 5). Eine Verlagerung der Datenverarbeitung ins Ausland (z.B. im Rahmen von *Infrastructure as a Service* oder *Platform as a Service)* kann zudem lizenzrechtlich relevant sein, wenn die Nutzung der verwendeten Software auf bestimmte Länder beschränkt wurde. Sie kann allenfalls auch gegen Exportrestriktionen verstossen (z.B. Export von Verschlüsselungstechnologie). Siehe dazu auch Hon/Millard/Walden (FN 7), 102 f.

80 Der Zugriff auf Personendaten wird oft durch Passwörter etc. geschützt. Auch in solchen Konstellationen kann allerdings die Gefahr bestehen, dass die entsprechenden Zugangscodes dem Provider durch Mitarbeitende des Auftraggebers (z.B. im Rahmen von Supportanfragen) bekannt gegeben werden und dass dadurch eine datenschutzrelevante Bekanntgabe der Daten ins Ausland erfolgt. Siehe dazu auch Hon/Millard/Walden (FN 7), 106.

81 Siehe zur Datenschutz-Kollisionsrecht in der EU auch Brennscheidt (FN 57), 181 ff.; Hon/Millard/Walden (FN 7), 102.

82 Siehe dazu Meier (FN 28), Rz. 1269. Rosenthal/Jöhri (FN 32), N. 9 zu Art. 6 DSG, gehen davon aus, dass Daten trotz einer technischen Zugriffsmöglichkeit nicht als bekanntgegeben gelten, wenn der betreffenden Person ein Zugriff vertraglich oder gestützt auf eine Weisung untersagt wurde. Eine vertragliche Regelung ist allerdings nur dann ausreichend, wenn davon ausgegangen werden kann, dass sie vom Provider auch respektiert wird – die Übertragung der Datenbearbeitung an einen nicht vertrauenswürdigen Provider kann selbst bereits einen Verstoss gegen Art. 7 Abs. 1 DSG und Art. 4 Abs. 2 DSG darstellen. Eine vollständige Überwachung vertraglicher Zugriffsverbote dürfte sehr schwierig sein. Die Einhaltung sollte periodisch stichprobenweise überprüft werden (z.B. Definition der zu protokollierenden Logdaten für alle Zugriffe und stichprobenweise Überprüfung der Logfiles). Die Stichproben sollten risikobasiert konzipiert werden und auch vom Umfang her dem Verhältnismässigkeitsprinzip genügen. Siehe in diesem Zusammenhang auch Rosenthal/Jöhri (FN 32), N. 35, 54, 67 und 85 zu Art. 10a DSG; Weber/Staiger (FN 57), Rz. 101. Zweifel an der Wirksamkeit vertraglicher Zugriffsverbote können sich aber auch durch Zugriffsrechte ausländischer Behörden ergeben. Eine Bekanntgabe ins Ausland ist dann unzulässig, wenn dadurch die Persönlichkeit der betreffenden Personen schwerwiegend gefährdet wird. Ob sich aus der Tatsache, dass ausländische Behörden auf die betreffenden Daten zugreifen könnten, tatsächlich eine solche Gefährdung ergibt, muss anhand der Umstände des Einzelfalls geprüft werden. Siehe dazu auch Epiney/Fasnacht (FN 39), S. 568 f., Rz. 13 f.

83 Siehe dazu Rosenthal/Jöhri (FN 32), N. 32 zu Art. 6 DSG. Umgekehrt hat auch die EU den Datenschutz in der Schweiz grundsätzlich als angemessen anerkannt, was für Fälle des Re-Imports von Daten in die Schweiz relevant sein kann. Siehe die Entscheidung der Kommission vom 26.6.2000 gemäss der Richtlinie 95/46/EG über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz.

84 Rosenthal/Jöhri (FN 32), N. 33 ff. zu Art. 6 DSG gehen pragmatisch davon aus, dass Daten juristischer Personen auch in Länder ohne entsprechende Schutzbestimmungen exportiert werden können, sofern sich nicht aus den Umständen des Einzelfalls eine schwerwiegende Gefährdung der Persönlichkeit ergibt und dass eine solche bei juristischen Personen kaum je vorliegt. Epiney/Fasnacht (FN 39), S. 567, Rz. 11; Fröhlich-Bleuler (FN 11), Rz. 2856; betrachten eine Bekanntgabe der Daten juristischer Personen in ein Land, das diese nicht datenschutzrechtlich schützt, hingegen nur als zulässig, wenn die Voraussetzungen von Art. 6 Abs. 2 DSG erfüllt sind.

85 Im Fall eines Weiterexports der Daten in Drittstaaten müssen die Anforderungen von Art. 6 DSG stets erfüllt werden. Siehe dazu Rosenthal/Jöhri (FN 32), N. 14 ff. zu Art. 6 DSG. Dies ist insbesondere bei der dynamischen Verteilung von Daten über mehrere Rechenzentren zu beachten.

Garantien (z.B. vertragliche[89] Absicherungen) oder eine Einwilligung[90] der betroffenen Personen erforderlich.[91]

Wie die *vertraglichen Garantien* im Einzelnen auszugestalten sind, hängt von den Umständen des konkreten Falles ab. Es sind aber insbesondere folgende Elemente zu regeln:

- *Identität* des Datenübermittlers und des Datenempfängers
- *Kategorien*[92] der zu übermittelnden Personendaten
- *Zwecke* der Übermittlung
- *Zugriffsberechtigungen*
- *Aufbewahrungsdauer.*

Die vertraglichen Regelungen müssen die *Beachtung der datenschutzrechtlichen Grundsätze* gewährleisten, es den betroffenen Personen ermöglichen, ihre Rechte wahrzunehmen (insbesondere Auskunfts-, Berichtigungs- und Klagerechte) sowie einen Kontrollmechanismus vorsehen. Im Falle von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen sind erhöhte Sicherheitsanforderungen zu erfüllen.[93]

Zur vertraglichen Absicherung werden in der Praxis meist die vom EDÖB anerkannten *Modellklauseln* verwendet. Vom EDÖB sind folgende Musterverträge oder Standardvertragsklauseln (Art. 6 Abs. 3 VDSG) empfohlen:

- *Mustervertrag des EDÖB*[94]
- *Standardvertragsklauseln der Europäischen Union*[95]

---

86 Per 1.1.2008 wurde das schweizerische DSG an das Zusatzprotokoll des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ST Nr. 108) bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung angepasst. Die Anforderung der «Gleichwertigkeit» des Datenschutzes im Importland wurde durch diejenige der «Angemessenheit» ersetzt. Nach der herrschenden Lehre hat sich dabei am erforderlichen Datenschutzniveau aber materiell nichts geändert. Die Angemessenheit des Schutzes in der Gesetzgebung des Empfängerstaates gilt grundsätzlich als gewährleistet, wenn sie den Anforderungen des Übereinkommens STE 108 entspricht. Darüber hinaus ist aber auch zu berücksichtigen, wie entsprechende Gesetzgebung in der Praxis umgesetzt wird. Siehe dazu EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland (FN 76), 2 ff.; Meier (FN 28), Rz. 1287; Rosenthal/Jöhri (FN 32), N. 31 und 35 zu Art. 6 DSG; Epiney/Fasnacht (FN 39), S. 567 f., Rz. 12.

87 Das für den konkreten Fall angemessene Schutzniveau muss sich nicht alleine aus der Datenschutzgesetzgebung des betreffenden Landes ergeben. Es kann auch auf sektoriellen Rechtserlassen beruhen (z.B. Schutz medizinischer Daten). Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 28 zu Art. 6 DSG. Bei ihrer Auslegung müssen aber auch die Wertungen des Datenschutzrechts mitberücksichtigt werden. Siehe dazu Epiney/Fasnacht (FN 39), S. 561, Rz. 5 und S. 566, Rz. 11.

88 Eine Liste derjenigen Staaten, die aus Sicht des EDÖB einen angemessenen Schutz für Daten natürlicher Personen bieten, ist online verfügbar unter *http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de.* Es handelt sich um Staaten, welche Vertragspartei des Übereinkommens STE 108 und des Zusatzprotokolls sind oder nach Ansicht des EDÖB anderweitig einen angemessenen Datenschutz gewährleisten. Die Liste wird laufend aktualisiert und ist nicht abschliessend. Privatpersonen oder Bundesorgane, welche Daten in einen unter «angemessener Schutz» aufgeführten Staat übermitteln, können sich darauf berufen, gutgläubig zu handeln. Wissen sie aber, z.B. aufgrund von Erfahrungen in der Praxis, dass in einem solchen Empfängerstaat Datenschutzvorschriften – generell oder im betreffenden Bereich – nicht beachtet werden, so sind sie nicht mehr gutgläubig. Siehe dazu auch Meier (FN 28), Rz. 1304. Die Bekanntgabe darf in einem solchen Fall nur unter den Bedingungen von Art. 6 Abs. 2 DSG erfolgen.

89 Eine Absicherung ist allenfalls auch durch *Protective Orders* ausländischer Gerichte oder durch technische Massnahmen möglich. Siehe dazu Rosenthal/Jöhri (FN 32), N. 50 f. zu Art. 6 DSG.

90 Art. 6 Abs. 2 lit. b DSG. Die Einwilligung muss sich auf einen Einzelfall, d.h. eine konkrete Situation, beschränken und nach vorgängiger angemessener Information erfolgen (siehe auch Art. 4 Abs. 5 DSG). Sie kann auch durch eine Zustimmung zu allgemeinen Geschäftsbedingungen erfolgen, sofern diese den Datenexport genügend präzise beschreiben. Die betroffene Person muss sich insbesondere bewusst sein, dass die Daten in ein Land ohne gleichwertigen Datenschutz übermittelt werden können. Die Einwilligung rechtfertigt die Datenübermittlung nur insoweit, als die von der einwilligenden Person berechtigterweise erwarteten technischen und organisatorischen Schutzmassnahmen tatsächlich getroffen werden. Von der Einwilligung kann auch eine Gesamtheit von Übermittlungen erfasst werden, wenn die Voraussetzungen (insbesondere Zweck und Empfänger) gleich bleiben. Für zukünftige Datenbearbeitungen und Datenübermittlungen kann die Einwilligung jederzeit zurückgezogen werden. Falls die Bekanntgabe besonders schützenswerte Personendaten betrifft, muss die Einwilligung ausdrücklich erfolgen. Siehe dazu Rosenthal/Jöhri (FN 32), N. 53 ff. zu Art. 6 und N. 109 ff. zu Art. 10a DSG; Epiney/Fasnacht (FN 39), S. 572 f., Rz. 19 f.; Meier (FN 28), Rz. 1350. Da die Anforderungen an Einwilligungen relativ hoch sind und sie für sämtliche Betroffenen vorliegen müssen, dürfte dieser Weg für die Auslagerung grösserer Datenbeständen kaum gangbar sein.

91 Art. 6 Abs. 2 DSG enthält eine Reihe weiterer Konstellationen, in welchen die grenzüberschreitende Bekanntgabe von Personendaten ins Ausland trotz Fehlens eines angemessenen Schutzes zulässig sein kann. Da diese für Cloud Service Verträge meist nicht von praktischer Relevanz sind, wird vorliegend jedoch nicht näher darauf eingegangen.

92 Siehe in Bezug auf die Kategorisierung von Kundendaten bei Banken auch FINMA Rundschreiben Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 9 f.

93 Siehe dazu auch Epiney/Fasnacht (FN 39), S. 570., Rz. 17 und S. 588, Rz. 42.

94 Swiss Transborder Data Flow Agreement for outsourcing of data processing, online verfügbar *http://www.edoeb.admin.ch/datenschutz/00626/00743/00858/00859/index.html*.

95 Siehe den Beschluss der Kommission vom 5.2.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46EG, publiziert in ABl. L 39/5 vom 12.2.2010, online verfügbar unter *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:01:DE:HTML*. Hinweise auf weitere Modellklauseln der EU finden sich bei Meier (FN 28), Rz. 1318.

– *Mustervertrag des Europarats* für die Sicherstellung eines angemessenen Datenschutzes im Rahmen des grenzüberschreitenden Datenverkehrs[96].

Die Modellklauseln weisen allerdings eine sehr *unterschiedliche Regelungsdichte* auf.[97] In diesem Zusammenhang ist zu beachten, dass die Anerkennung der Modellklauseln durch den EDÖB grundsätzlich keine rechtlich bindende Wirkung hat.[98] Sie ist aber zweifellos ein wichtiges Indiz für die Angemessenheit des Schutzes.[99]

Ob bestimmte vertragliche Formulierungen tatsächlich einen angemessenen Schutz gewährleisten (z.B. Schutz der Daten von juristischen Personen), wäre von einem allfällig angerufenen Gericht im Einzelfall zu prüfen.[100] Dabei wäre insbesondere das *Verhältnismässigkeitsprinzip* zu beachten.[101]

Zwischen der Schweiz und den USA besteht eine Vereinbarung über den Datenschutz, das sog. *Safe Harbour Framework.*[102] Gemäss diesem können sich amerikanische Unternehmen zu einem bestimmten Schutzniveau für den Umgang mit Personendaten verpflichten. Sofern der betreffende Provider dem Safe Harbor Framework beigetreten und auf der entsprechenden Liste des U.S. Department of Commerce[103] verzeichnet ist, wird der Datenschutz vom EDÖB grundsätzlich[104] als angemessen anerkannt.[105] Vor einer Auslagerung von Daten an Safe Harbour zertifizierte Unternehmen muss ein schriftlicher Vertrag über die Datenverarbeitung abgeschlossen werden, der insbesondere auch eine Aufrechterhaltung der Zertifizierung vorsieht.

Vor einer Datenübermittlung ins Ausland sind zusammenfassend insbesondere folgende Punkte sicherzustellen:

– Der Datenexporteur muss prüfen, ob der Auslagerung *gesetzliche oder vertragliche Pflichten* entgegenstehen.[106]
– Die *Zweckbindung und die Verhältnismässigkeit* der Datenbearbeitung müssen gewährleistet sein.[107]
– Es sind alle erforderlichen technischen und organisatorischen Massnahmen zu treffen, um die *Integrität, Vertraulichkeit und Verfügbarkeit* der Daten zu sichern.[108] Der Datenexporteur hat auch alle notwendigen Massnahmen zu treffen, damit unrichtige oder unvollständige Daten berichtigt oder vernichtet werden.[109]
– Es ist abzuklären, ob der *Schutz im Zielland angemessen* ist.[110] Wenn dies nicht der Fall ist, so ist gegebenenfalls vertraglich, technisch und organisatorisch ein angemessenes Schutzniveau sicherzustellen.
– Falls kein angemessenes Datenschutzniveau im Zielland besteht und ein Datenexport gestützt auf vertragliche Garantien erfolgt, muss der *EDÖB* vor der Übermittlung der Daten über den Vertragsinhalt *informiert* werden. Der Datenexporteur hat dem EDÖB die mit dem Provider vereinbarten Datenschutzregeln offen-

---

96 Siehe *http://www.edoeb.admin.ch//datenschutz/00626/00753/index.html*. Der Europarat hat auch Erläuterungen zum Mustervertrag publiziert. Siehe zudem auch Agentur der Europäischen Union für Grundrechte/Europarat (Hrsg.), Handbuch des europäischen Datenschutzrechts, 2. A., Luxemburg 2014, online verfügbar unter *http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_de.pdf,* 153 ff.

97 So sieht z.B. der Mustervertrag des Europarats keine explizite Bestimmung zum Audit vor. Hingegen beinhalten die Standardvertragsklauseln der EU gegenüber dem Mustervertrag des EDÖB (z.B. im Bereich der Haftung gegenüber den betroffenen Personen) weiter gehende Bestimmungen.

98 Siehe dazu auch Meier (FN 28), Rz. 1330.

99 Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 30 zu Art. 6 DSG, die von einer widerlegbaren Vermutung der Angemessenheit des Schutzes ausgehen.

100 Die betroffenen Personen können eine pflichtwidrige Bekanntgabe ihrer Daten ins Ausland gerichtlich anfechten. Siehe Art. 15 Abs. 1 DSG.

101 Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 79 ff. zu Art. 10a DSG.

102 Briefwechsel vom 1./9.12.2008 zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Schaffung eines Datenschutzrahmenwerkes zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika (SR 0235.233.6).

103 Die Liste der von der International Trade Administration (ITA) zertifizierten Unternehmen ist online verfügbar unter *https://safeharbor.export.gov/swisslist.aspx*. Die Zertifizierung beruht auf einer Selbstdeklaration. Siehe dazu im Einzelnen Rosenthal/Jöhri (FN 32), N. 49 zu Art. 6 DSG; Julia Bhend, Safe Harbor: Globaler Datenumschlagplatz? digma 2011, 122 ff.; Jürg Schneider, Personendaten-Transfer in die USA, digma 2009, 126 f.; Eidgenössischer Öffentlichkeits- und Datenschutzbeauftragter, Gilt das mit den USA abgeschlossene Safe Harbor Framework auch für Personendaten von juristischen Personen? online verfügbar unter *http://www.edoeb.admin.ch/datenschutz/00763/01054/01056/index.html?lang=de*. Vor der Übermittlung von Personendaten an ein US-Unternehmen sollten die Liste konsultiert und allenfalls ergänzende Datenschutzklauseln vereinbart werden.

104 Siehe zu den Limitierungen des Safe Harbour Systems allerdings auch Meier (FN 28), Rz. 1336; Weber/Staiger (FN 57), Rz. 47 und 101.

105 In Nachgang zu den von Edward Snowden publik gemachten Abhörpraktiken der NSA gab es verschiedene parlamentarische Anfragen betreffend das Safe Harbor Framework. Siehe dazu *www.parlament.ch/d/suche/Seiten/resultate.aspx?collection=CV&gvk_gtyp_key=1,2,3,4,5,6,7,8,9,10,12,13,14,18,19&query=Safe%20Harbor&sort=GN&way=desc*.

106 Art. 4 Abs. 1 DSG.

107 Art. 4 Abs. 2 und Abs. 3 DSG.

108 Art. 7 DSG.

109 Art. 5 DSG.

110 Art. 6 Abs. 1 DSG.

zulegen.[111] Eine Verletzung der Informationspflicht hat strafrechtliche Konsequenzen.[112]

– Für die Bearbeitung von Personendaten durch einen Provider oder dessen Subunternehmer im Ausland kann allenfalls *zusätzlich auch ausländisches Datenschutzrecht* zur Anwendung kommen. Es ist vorab zu klären, welche Pflichten sich für die Beteiligten daraus ergeben (z.B. Registrierungspflichten).

Der Inhaber einer Datensammlung *haftet* für Nachteile, die aus einer Verletzung seiner Sorgfaltspflichten entstehen. Er hat insbesondere nachzuweisen, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.[113]

Der Auftraggeber hat ein Interesse daran, mit dem Provider die Anwendbarkeit schweizerischen Rechts und einen *Gerichtsstand* in der Schweiz zu vereinbaren: Einerseits vereinfacht dies die Durchsetzbarkeit von Ansprüchen gegenüber dem Provider. Andererseits sind schweizerische Gerichte am besten mit den vom Auftraggeber einzuhaltenden regulatorischen Vorgaben des schweizerischen Rechts vertraut.

5. Zugriff durch Behörden

Eine weitere Gefahr für die Daten des Auftraggebers[114] liegt in den Zugriffsrechten inländischer[115] und ausländischer Behörden[116] gegenüber dem Cloud Provider.[117] Von besonderer praktischer Relevanz ist die Möglichkeit der *USA,* unter dem US Patriot Act, dem Foreign Intelligence Surveillance Act sowie dem 50 US Code 1881a auf Daten von nicht-amerikanischen Bürgern ausserhalb der Vereinigten Staaten Zugriff zu nehmen, wenn diese bei Gesellschaften gelagert sind, welche in den USA domiziliert oder börsenkotiert sind oder zu einem Konzern gehören, der auch US-Gesellschaften umfasst oder eine dauerhafte Tätigkeit in den Vereinigten Staaten ausüben.[118]

---

111 Falls kein Mustervertrag verwendet wurde oder dieser in wesentlichen Punkten abgeändert wurde, kann der EDÖB die vertraglichen Regelungen im Einzelnen prüfen. Er ist über die Kategorien der betroffenen Daten, den Zweck der Bearbeitung und die Datenempfänger zu informieren. Der EDÖB hat die Prüfung des Vertrages bzw. der sonstigen Garantien innert 30 Tagen vorzunehmen (Art 6 Abs. 5 VDSG). Gewährleisten diese keinen angemessenen Datenschutz, so kann er mit dem Inhaber der Datensammlung Kontakt aufnehmen und – falls erforderlich – eine Empfehlung gemäss Art. 29 DSG erlassen. Erfolgt innert der Frist keine Reaktion, so kann der Inhaber der Datensammlung davon ausgehen, dass der EDÖB keine Einwände gegen die vorgelegten Regelungen hat. Werden die Datenschutzregeln nachträglich geändert oder wird der Umfang der Datenbearbeitung darüber hinaus erweitert, so ist eine erneute Mitteilung an den EDÖB erforderlich. Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 95 zu Art. 6 DSG; Epiney/Fasnacht (FN 39), S. 580, Rz. 31; Urs Maurer-Lambrou/Andrea Steiner in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Basler Kommentar zum Datenschutzgesetz, Basel 2006, 2. A.,, N. 37 zu Art. 6 DSG. In diesem Zusammenhang ist allerdings zu beachten, dass das Prüfungsergebnis des EDÖB in Bezug auf allfällige Gerichtsverfahren keine bindende Wirkung hat.

112 Art. 34 Abs. 2 lit. a DSG. Siehe zu den Voraussetzungen der Strafbarkeit im Einzelnen Rosenthal/Jöhri (FN 32), N. 98 ff. zu Art. 6 DSG. Nicht strafbar ist eine fahrlässige Begehung, wenn der Inhaber der Datensammlung z.B. bloss vergisst, seiner Informationspflicht nachzukommen.

113 Die zu Art. 55 OR entwickelten Sorgfaltspflichten sind im Datenschutzrecht analog anwendbar. Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 48 ff., 55, 63 ff., 69 und 88 ff. zu Art. 10a DSG und Meier (FN 28), Rz. 1218 ff., die zu Recht darauf hinweisen, dass faktisch keine vollständige Kontrolle der Datenhaltung und Datenbearbeitung durch den Auftraggeber möglich ist. Epiney/Fasnacht (FN 39), S. 594, Rz. 53 f., gehen indessen von einer «Erfolgspflicht» aus, wonach die Datenverarbeitung auch dann widerrechtlich ist, wenn der Auftraggeber alle erforderlichen Massnahmen getroffen hat, der Auftragnehmer aber dennoch gegen gesetzliche Vorgaben verstösst. Nach der hier vertretenen Auffassung ist zwischen der Widerrechtlichkeit der Datenverarbeitung selbst und der Schadenersatzpflicht zu unterscheiden: Eine gegen das DSG verstossende Datenbearbeitung bleibt selbst widerrechtlich, auch wenn der Auftraggeber bezüglich Auswahl, Instruktion und Überwachung des Providers alle mögliche Sorgfalt aufgewendet hat. In Bezug auf eine Haftung gemäss Art. 55 OR ist jedoch der Exzeptionsbeweis möglich.

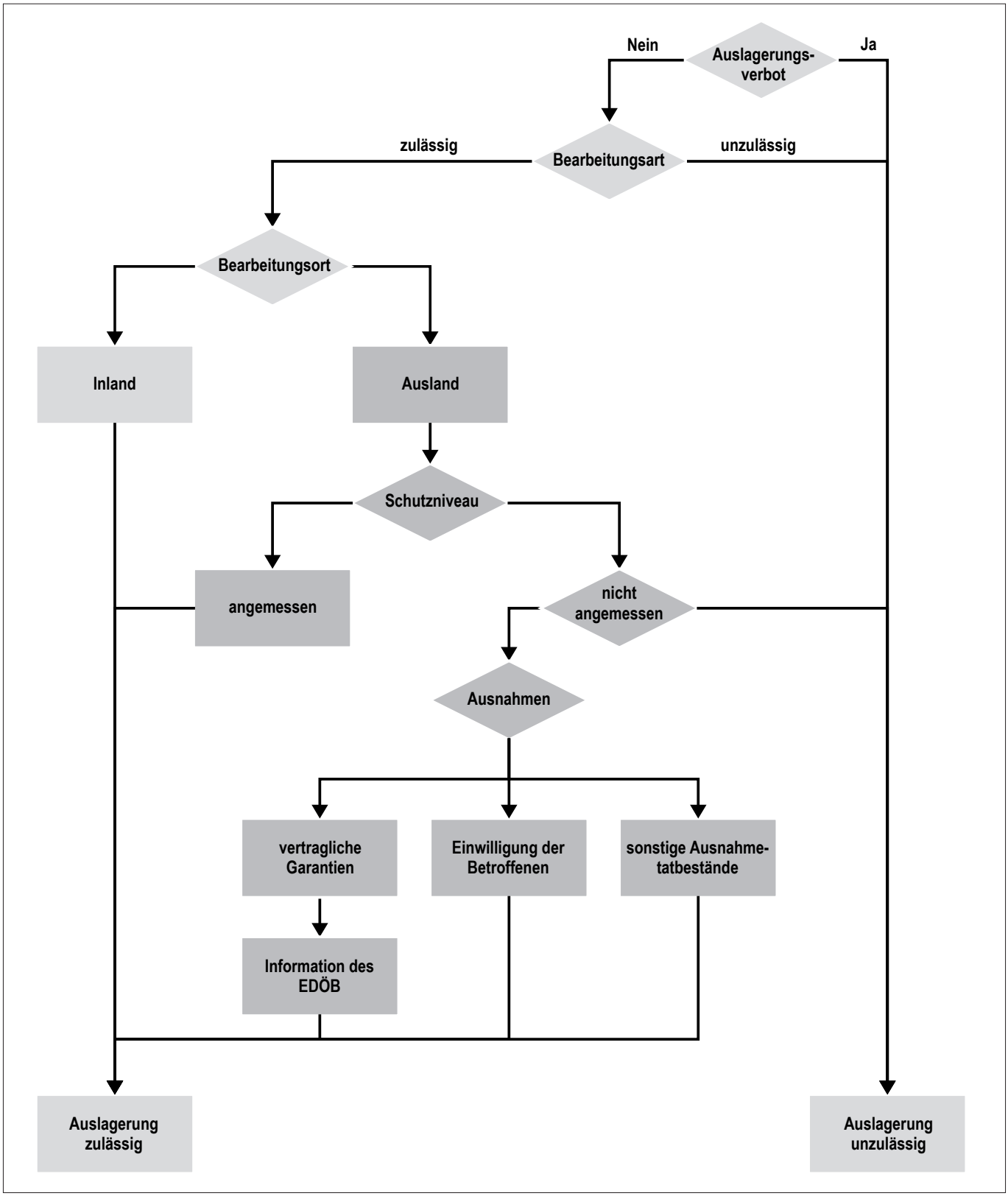
114 Wenn es sich beim Auftraggeber um ein Gemeinwesen handelt, stellt sich zusätzlich zur Gefahr der Verletzung von Geheimhaltungsvorschriften die Problematik eines möglichen Souveränitätsverlusts.

115 Nicht nur ausländische, sondern auch schweizerische Behörden können unter bestimmten Voraussetzungen auf Daten des Auftraggebers zugreifen, z.B. im Rahmen einer Überwachung nach Art. 273 StPO, dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1) oder dem künftigen Nachrichtendienstgesetz. Siehe auch de la Cruz (FN 12), Rz. 31; Rolf H. Weber/Dominic N. Staiger, Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA, jusletter IT vom 15.5.2014, Rz. 12 ff. und 20 ff. Damit verbundene Risiken können vertraglich weder ausgeschlossen noch auf dem Provider überwälzt werden.

116 In Bezug auf Gerichtsverfahren enthält Art. 6 Abs. 2 lit. d DSG eine Spezialbestimmung. Die Interessen der vom Prozess betroffenen und diejenigen der von der Datenherausgabe betroffenen Personen sind letztlich gegen einander abzuwägen. Die Anwendung dieser Sondernorm bringt allerdings zahlreiche Rechtsfragen mit sich, auf welche hier nicht näher eingegangen werden kann (z.B. ob auch im Rahmen ein*es pre-trial discovery*-Verfahrens Daten bekannt gegeben werden dürfen). Siehe dazu im Einzelnen Rosenthal/Jöhri (FN 32), N. 63 ff. zu Art. 6 DSG; Jürg Schneider/Ueli Sommer/Michael Cartier, in: Catrien Noorda/Stefan Hanloser (Hrsg.), E-Discovery and Data Privacy – A Practical Guide, Alphen aan den Rijn 2011, 277–294.

117 Siehe in diesem Zusammenhang auch Art. 271 und 273 StGB.

118 Siehe dazu auch Weber/Staiger (FN 115), Rz. 28 ff.; Weber/Staiger (FN 57), Rz. 101; Rosenthal/Jöhri (FN 32), N. 35, 54,



Grafik 4
Schematische Darstellung der Voraussetzungen einer Datenauslagerung

Gegen eine aus schweizerischer Sicht unzulässige *extra-territoriale Anwendung von US-Recht* vertragliche Schranken aufstellen zu wollen, ist unbehelflich. Vom Cloud Provider kann immerhin verlangt werden, dass er den Auftraggeber – soweit rechtlich zulässig – vorgängig über entsprechende Zugriffsersuchen[119] informiert und mögliche Rechtsbehelfe ergreift.[120]

Cloud Services von ausländischen Providern sollten deshalb grundsätzlich nur dann verwendet werden, wenn *keine sensiblen*[121] *Daten* verarbeitet werden oder wenn ein ausreichender Schutz durch technische Massnahmen sichergestellt werden kann (z.B. indem die Daten vorgängig entsprechend dem State of the art verschlüsselt wurden und der Schlüssel in der Schweiz bleibt oder indem Personendaten anonymisiert[122] wurden, so dass keine Rückschlüsse auf die betreffenden Personen mehr möglich sind). Die Wahl eines ausländischen Providers kann allerdings auch dann sinnvoll sein, wenn der Auftraggeber selbst ohnehin bereits dem Recht des betreffenden Landes untersteht.

6. Weitere datenschutzrechtliche Problemfelder

Daten und Systeme müssen vom Provider regelmässig gesichert werden. Bei Vertragsende besteht ein Anspruch auf *Löschung*[123] aller Daten des Auftraggebers. Bereits vor Vertragsende kann eine Berichtigung oder Löschung einzelner Daten notwendig sein.[124] Theoretisch beziehen sich solche Ansprüche auch auf alle Backups. Faktisch lässt sich dies indessen oft kaum durchführen. – Eine analoge Problematik besteht auch nach dem Erlöschen von Lizenzen für Software, welche auf Backupmedien mitgesichert wurde.[125] Einer Vernichtung können zudem Aufbewahrungsvorschriften auf Seiten des Providers entgegenstehen.[126] Nach der hier vertretenen Auffassung sollte ein vertragliches Verbot der Wiederherstellung und Weiterbearbeitung der betreffenden Daten ausreichen, wenn davon ausgegangen werden kann, dass sich der Provider an dieses halten wird.

Eine konsequente *Datentrennung* zwischen den einzelnen Kunden des Cloud Providers ist in verschiedener Hinsicht relevant: Einerseits geht es um die Verhinderung von Querzugriffen zwischen den Kunden, andererseits um die Beschränkung der Auswirkungen bei Angriffen gegen einen Kunden auf die anderen[127]. Datensicherungen sollten möglichst auf dedizierte Medien erfolgen.[128]

Beim Cloud Provider handelt es sich in der Regel um eine juristische Person. Letztlich nehmen aber stets einzelne Menschen Einblick in Daten und Geschäftsgeheimnisse. Alle Mitarbeitenden des Cloud Providers und seiner Konzerngesellschaften und Subunternehmer, welche Einblicksmöglichkeiten in solche Daten erhalten, sollten eine entsprechende *Geheimhaltungs- und Verwertungsverbotserklärung* unterzeichnen, damit sie auch nach Ende ihres eigenen Anstellungsverhältnisses weiterhin an die Geheimhaltungsvorschriften gebunden bleiben.[129] Um die Rechte der Betroffenen (z.B. auch über einen Konkurs des Providers hinaus) sicherzustellen, sollte die Vereinbarung direkte Ansprüche der Betroffenen auf Einhaltung der Geheimhaltung vorsehen.

---

67 und 85 zu Art. 10a DSG sowie den Entscheid des Southern District Court of New York, 2014 U.S. Dist. LEXIS 59296 (S.D.N.Y. April 25, 2014) auch online verfügbar unter *http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398,* wonach US-Unternehmen gegebenenfalls auch im Ausland gespeicherte Daten herausgeben müssen. Dieser Entscheid ist allerdings noch nicht rechtskräftig und wurde von Microsoft weitergezogen. Siehe dazu Steve Lohr, Microsoft Protests Order to Disclose Email Stored Abroad, New York Times of June 10, 2014, *http://www.nytimes.com/2014/06/11/technology/microsoft-protests-order-for-email-stored-abroad.html?ref=technology&_r=0.*

119 Gemäss dem Patriot Act können US-Unternehmen Behörden aber auch freiwillig eine direkte Verbindung zu ihren Daten gestatten. Siehe dazu Weber/Staiger (FN 115), Rz. 40.

120 Siehe zu den Anfechtungsmöglichkeiten von Herausgabeverfügungen auch Weber/Staiger (FN 115), Rz. 38.

121 Sensible Daten können in diesem Zusammenhang sowohl Personendaten als auch sonstige Daten umfassen, bei denen ein Geheimhaltungsinteresse gegenüber ausländischen Behörden besteht (z.B. militärisch klassifizierte Daten). Umgekehrt sind aber nicht sämtliche Personendaten sensibel (z.B. allgemein zugängliche Informationen aus öffentlichen Registern).

122 Siehe zur Datenverschlüsselung und Anonymisierung von Personendaten Abschnitt 3.

123 Technisch gesehen kann eine Löschung auf unterschiedliche Weise erfolgen. Oft werden nicht die eigentlichen Daten, sondern nur entsprechende Verweise auf Datenträgern überschrieben. Auch im Fall einer Löschung können die Daten unter Umständen mit speziellen Tools wieder hergestellt werden. Welches Verfahren der Datenlöschung im konkreten Fall erforderlich ist, hängt insbesondere von der Sensitivität der Daten und vom Life Cycle Management der Datenträger im betreffenden Rechenzentrum ab. Siehe dazu Hon/Millard/Walden (FN 7), 118.

124 Siehe Art. 5 DSG.

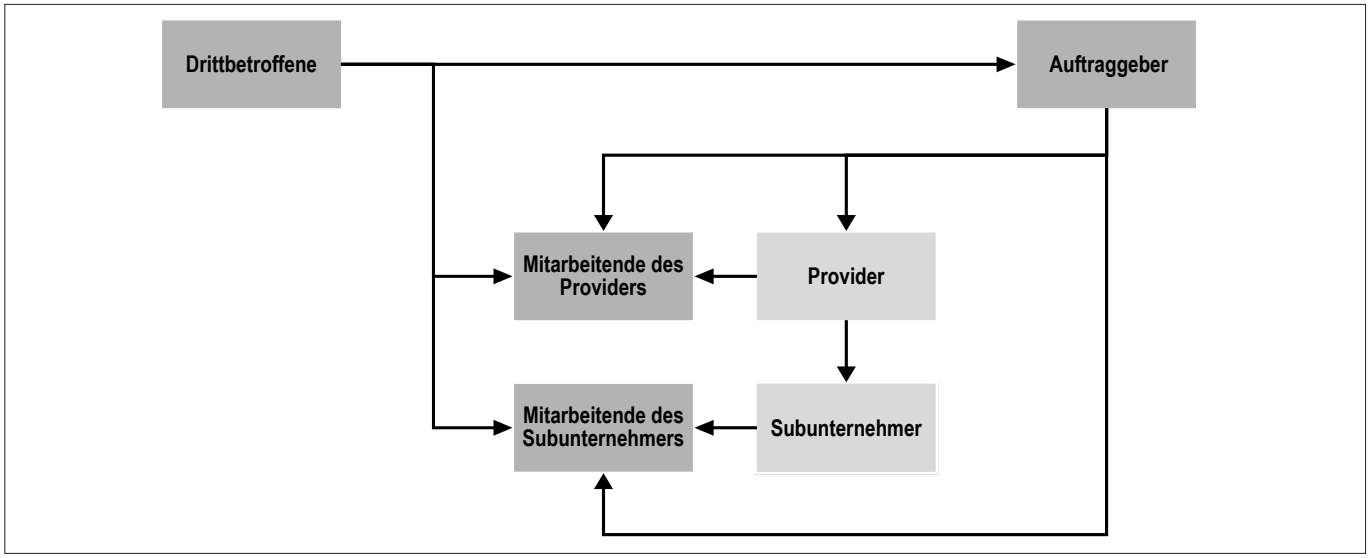
125 Siehe dazu auch Straub (FN 31), Rz. 217 und 237.

126 Siehe etwa Art. 5 GeBüV und Art. 15 Abs. 3 BÜPF.

127 Bei gemeinsam genutzter Infrastruktur *(Multi-Tenant*-Architektur) besteht insbesondere die Gefahr, dass durch *Distributed Denial of Service*-Attacken auf einen Kunden auch der Zugang zu den Daten anderer Kunden blockiert wird.

128 Siehe dazu auch Abschnitt 9.

129 Banken müssen zudem alle internen und externen Schlüsselmitarbeitenden erfassen, welche Zugriff auf eine grössere Menge von Kundenidentifikationsdaten haben. Siehe dazu FINMA Rundschreiben Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 34.



Grafik 5
Schematische Darstellung der Geheimhaltungsansprüche

Cloud Service Verträge sollten *Audit- und Kontrollrechte*[130] des Auftraggebers gegenüber dem Cloud Provider umfassen. Deren Ausübung ist in der Praxis allerdings oft mit Schwierigkeiten verbunden.[131] Wie weit das Auditrecht[132] gehen muss, hängt vor allem von der Sensibilität der bearbeiteten Daten ab. Ein wirkungsvoller Audit setzt einerseits voraus, dass der Auditor die erforderliche technische Kompetenz dazu hat[133], andererseits dass der Provider ihm tatsächlich entsprechenden Einblick in Systeme und Prozesse gewährt – dabei hat er sowohl seine eigenen Geschäftsgeheimnisse als auch die Vertraulichkeit von Daten anderer Kunden zu wahren. Audits werden in der Regel durch unabhängige externe Experten durchgeführt, welche sich ihrerseits zur Geheimhaltung gegenüber Dritten verpflichten. Dabei kann es sich auch um eine juristische Person handeln.

Im Cloud Service Vertrag ist insbesondere zu regeln, nach welchem Verfahren der *Auditor* bestimmt wird, *was im einzelnen geprüft* werden kann, ob Audits auch *Subunternehmer* mit einschliessen können, *wie häufig* sie stattfinden dürfen, ob sie auch *unangemeldet* erfolgen können und wer die *Kosten* zu tragen hat (z.B. Kostenverteilung entsprechend dem Auditergebnis).[134]

7. Wahrung der eigenen Handlungsfähigkeit

Um eine zu grosse Abhängigkeit vom Cloud Provider zu vermeiden, sollte der Auftraggeber auf die Wahrung der

[130] Siehe in Bezug auf Banken FINMA Rundschreiben 2008/7 Outsourcing Banken, Rz. 21 ff., sowie Rundschreiben der FINMA Operationelle Risiken Banken 2008/21, Anhang 3, Rz. 48.

[131] Siehe dazu auch Fuchs (FN 36) Rz. 23 f.; Schwaninger/Lattmann (FN 22) Rz. 22; Halpert (FN 38); Rosenthal/Jöhri (FN 32), N. 120 zu Art. 10a DSG; Hon/Millard/Walden (FN 7), 108 und 113 f.

[132] Siehe dazu auch Rosenthal/Jöhri (FN 32), N. 40 zu Art. 6 und N. 129 f. zu Art. 10a DSG. In der Praxis werden vertraglich eingeräumte Auditrechte vom Auftraggeber oft gar nicht wahrgenommen. Dies kann im Fall von Datenschutzverletzungen, welche durch entsprechende Audits hätten erkannt und vermieden werden können, ein Mitverschulden des Auftraggebers darstellen.

[133] Siehe dazu auch EDÖB, Erläuterungen zu Cloud Computing (FN 57), 3. Danach muss sich der Auftraggeber vergewissern, dass der Provider die Datensicherheit gewährleistet, indem er periodisch die technischen und organisatorischen Massnahmen vor Ort überprüft. Audits können grundsätzlich auch im Rahmen von Zertifizierungsprogrammen des Providers erfolgen. Es muss aber sichergestellt werden, dass das Prüfprogramm auch allfällige spezifische Anforderungen des Aufraggebers abdeckt (z.B. angemessener Schutz der Daten von juristischen Personen). Zusätzlich zu individuellen Auditrechten kann vertraglich z.B. auch eine Berichterstattung nach ISAE 3402 vorgesehen werden. Siehe zur Bedeutung von Audits auch Meier (FN 28), Rz. 1238; Rosenthal/Jöhri (FN 32), 124 ff. zu Art. 10a DSG; Epiney/Fasnacht (FN 39), S. 595, Rz. 54.

[134] Der Mustervertrag des EDÖB (Swiss Transborder Data Agreement for outsourcing of data processing, Kap. 5) sieht allerdings nur eine sehr allgemein gehaltene Formulierung zum Auditrecht vor: *«The Data Exporter has the right to, at any time, in any reasonable manner and with the Data Importer's full cooperation, audit the Data Importer's (and any Subprocessor's) compliance with the Agreement or to have such audit performed by a qualified third party bound by a duty of confidentiality. The costs will be borne by the Data Exporter; if any non-compliance is revealed which may be of significance for Persons Affected, the Data Importer shall bear the costs.»*

eigenen Handlungsfähigkeit achten. Technische *«Lock-in-Effekte»* sind wenn möglich zu vermeiden.

Wenn Daten auf einer proprietären Plattform des Providers bearbeitet werden, kann sich – insbesondere bei Vertragsende – die Frage stellen, in welchem Format diese dem Auftraggeber zur Verfügung gestellt werden bzw. wie die Daten in ein Format gebracht (migriert) werden, das vom Auftraggeber selbst oder durch einen neuen Provider weitergenutzt werden kann (Portierbarkeit)[135]. In Cloud Service Verträgen sollte im Interesse des Auftraggebers daher eine Auslieferung der Daten in einem *standardisierten Format* bzw. eine Verpflichtung zur Migrationsunterstützung bei Vertragsende vorgesehen werden.

Die in der Cloud betriebenen Applikationen müssen eventuell während der ganzen Vertragsdauer mit Systemen des Auftraggebers interoperabel sein. Das setzt voraus, dass der Cloud Provider bestimmte Schnittstellen für den Datenimport/Datenexport unterstützt. Zur *Aufrechterhaltung der Interoperabilität* kann sowohl bei Releasewechseln der Cloud Applikationen als auch bei Veränderungen der Umsysteme des Auftraggebers erheblicher Aufwand entstehen. Es ist daher vertraglich zu regeln, welche Schnittstellen vom Provider unterstützt werden müssen, wer den entsprechenden Aufwand zu tragen hat und mit welchen Fristen wesentliche Änderungen vorangekündigt werden müssen.[136] Dabei sind auch die entsprechenden Software-Releasezyklen zu berücksichtigen (d.h. ab wann neue Versionen und wie lange alte Versionen von Applikationen und Middleware unterstützt werden müssen).

Oft sind für den Auftraggeber nicht nur Daten im engeren Sinn relevant, sondern auch *Metadaten*[137], Benutzerverwaltungsinformationen (z.B. welche Nutzer welche Rechte auf der Plattform haben), Parametrisierungseinstellungen von Software, Skripts, Tools etc. In der Praxis können sich diesbezüglich zahlreiche Detailfragen stellen. Es sollte vertraglich möglichst präzise geklärt werden, welche Informationen wann zu liefern sind und inwieweit sie auch auf andere Systeme übertragbar sein müssen. Bei *Infrastructure as a Service* und *Platform as a Service* kann ein Bedürfnis bestehen, vollständige Installationen virtueller Maschinen zu übertragen.[138]

Um eine möglichst grosse Flexibilität zu bewahren, hat der Auftraggeber ein Interesse daran, den Vertrag jederzeit durch die Ausübung von *Auflösungsoptionen* beenden zu können. Das bedeutet keineswegs, dass die Beendigung stets kostenlos sein muss. Hingegen sollte die Höhe der Ablösungskosten zum voraus berechenbar sein.

8. Kostenkontrolle

Cloud Services werden meistens gewählt, um Kosten zu sparen. Tatsächlich können standardisierte Leistungen von Cloud Providern aufgrund von Skaleneffekten oft zu viel günstigeren Preisen angeboten werden. Hingegen kann eine Anpassung an individuelle Bedürfnisse sehr teuer werden. Ein *Vergleich der Kosten* in der Cloud mit denjenigen einer Inhouse-Lösung über längere Zeiträume hinweg ist allerdings mitunter schwierig, weil sich die tatsächlich bezogenen Leistungen gegenüber den ursprünglich ausgelagerten oft erheblich verändern.

Beim Abschluss von Cloud Service Verträgen sind insbesondere folgende *Kostenrisiken* im Auge zu behalten:

– *Sorgfältige Leistungsbeschreibung:* Welche Leistungen sind durch Pauschalen abgedeckt, welche sind mit zusätzlichen Kosten verbunden?
– *Miteinbezug von Zusatzaufwand in die Kalkulation,* z.B. Kosten für die Adaptierung der Services an die Anforderungen des Auftraggebers und die Pflege von Schnittstellen, beizustellende Drittlizenzen, Supportkosten, Kommunikationskosten für die Datenübertragung, Kosten für allfällige vom Provider für den Zugriff auf die Systeme vorgegebene Hard- und Softwarekomponenten
– *Kontrolle der effektiven Leistung:* Wie und durch wen werden die relevanten Parameter für nutzungsabhängige Vergütungen erfasst? Wie wird die Einhaltung der Service Levels gemessen?[139] Besteht die Möglichkeit, diese Angaben durch externe Experten überprüfen zu lassen?
– *Limitierung von nutzungsabhängigen Gebühren:* Mitunter werden Services von den Endbenutzern in weit höherem Umfang genutzt als ursprünglich erwartet.

---

[135] Gemäss Markus Vehlow/Cordula Golkowsky, Cloud Computing – Navigation in der Wolke, S. 34, online verfügbar unter *http://www.pwc.de/de_DE/de/prozessoptimierung/assets/Cloud_Computing_deutsch.pdf* enthielten im Jahr 2011 nur 60% der Cloud Service Verträge Regelungen zur Datenrückgabe.

[136] Siehe dazu auch Hon/Millard/Walden (FN 7), 123 f.

[137] Siehe zu Metadaten und Randdaten auch FN 47.

[138] Siehe dazu auch Hon/Millard/Walden (FN 7), 116.

[139] Die Frage der Einhaltung von Service Levels ist insbesondere im Hinblick auf Key Performance Indicators (KPIs) relevant, wenn das Unterschreiten von Schwellenwerten einen Malus oder die Übererfüllung einen Bonus auslöst. Gemäss Hon/Millard/Walden (FN 7), 96, enthalten grössere Cloud Service Verträge typischerweise 5–10 KPIs. Als KPI kann insbesondere auch die Kundenzufriedenheit durch die statistische Auswertung eines Umfrageformulars gemessen werden.

Beim Erreichen bestimmter Schwellenwerte sollte informiert und eventuell das Gebührenmodell angepasst werden.

– *Vermeidung von falschen wirtschaftlichen Anreizen*. Diese können z.B. durch Konventionalstrafen/Malus etc. entstehen, wenn die Bezahlung der Pönale für den Provider günstiger ist als eine korrekte Leistungserbringung. Aus der Sicht der Auftraggeber ist daher insbesondere die gängige Deckelung von Pönalen durch einen Maximalbetrag problematisch. Es ist auch darauf zu achten, dass der Provider während der ganzen Vertragsdauer ein finanzielles Interesse an Innovationen hat.

9. Insolvenz

Der Auftraggeber hat ein Interesse daran, wirtschaftliche Probleme des Cloud Providers möglichst *frühzeitig zu erkennen*. Wenn durch den Provider geschäftskritische Leistungen erbracht werden, kann dessen Insolvenz besonders fatal sein. Zur Vermeidung von Überraschungen kommen z.B. eine periodische Überprüfung der Kreditwürdigkeit durch eine Agentur und eine Verpflichtung des Providers zur regelmässigen Information über finanzielle Kennzahlen in Betracht.

Die *Bestimmung des anwendbaren Insolvenzrechts* kann in internationalen Verhältnissen sehr anspruchsvoll sein (z.B. wenn es sich beim Provider um einen ausländischen Konzern handelt, welcher Rechenzentren durch Tochtergesellschaften in unterschiedlichen Ländern betreiben lässt).[140]

An Daten können in der Schweiz im Insolvenzfall keine *Aussonderungsansprüche* geltend gemacht werden, da sich solche Ansprüche nach der herrschenden Lehre nur auf körperliche Gegenstände beziehen.[141] Hingegen ist eine Aussonderung von Datenträgern möglich, welche im Eigentum eines bestimmten Kunden stehen. Der Auftraggeber sollte sich wenn möglich fortlaufend Kopien aller relevanten Daten ausliefern lassen (z.B. Bereitstellung zum Download oder automatischer Upload auf die Systeme des Auftraggebers via Schnittstelle). Ergänzend sollten gegebenenfalls dedizierte Datenträger mit Sicherungskopien als Eigentum des jeweiligen Kunden gekennzeichnet werden, so dass eine Konkursverwaltung ohne weiteres erkennen kann, wer daran berechtigt ist. Dies setzt allerdings voraus, dass individuelle und nicht lediglich kollektive Sicherungen erfolgen und dass der Auftraggeber Eigentum an den Datenträgern (Tapes, Disks etc.) erwirbt.

Im Cloud Service Vertrag sollte vorsichtshalber festgehalten werden, dass der Provider auf allfällige *Retentionsrechte* an Daten[142] verzichtet und dass jegliche *Verwertung von Daten des Auftraggebers* – auch für den Insolvenzfall[143] – ausgeschlossen ist.

Allerdings besteht dennoch ein Restrisiko, dass vertrauliche Inhalte (z.B. aufgrund einer unvollständigen *Löschung von Datenträgern* bei der Verwertung von Storage Medien) in unberechtigte Hände gelangen. Solche Risiken können durch eine wirksame Verschlüsselung der Datenablagen, durch eine Anonymisierung[144] der Datensätze oder durch eine Architektur der verteilten Datenspeicherung vermieden werden.

Wenn im Rahmen des Cloud Service Vertrages *Software* individuell entwickelt bzw. angepasst wird, so sollte vertraglich definiert werden, welche Entwicklungen dem Auftraggeber gehören. Die entsprechende Software inklusive der zu ihrer Verwendung notwendigen Bibliotheken, Tools, Skripts etc. sollte periodisch ausgeliefert werden (z.B. Bereitstellung zum Download). Individualisierte Softwarekomponenten können allenfalls aber auch bei einem Escrow-Agenten hinterlegt werden, der diese im Insolvenzfall herausgeben muss.[145]

---

[140] Siehe dazu auch Schwaninger/Lattmann (FN 22), Rz. 51 ff.

[141] Siehe dazu Marc Russenberger in: Adrian Staehelin/Thomas Bauer/Daniel Staehelin (Hrsg.), Basler Kommentar Schuldbetreibungs- und Konkursgesetz, 2. A., Basel 2010, N. 10 zu Art. 242 SchKG, mit weiteren Hinweisen; Schwaninger/Lattmann (FN 22), Rz. 55. In diesem Zusammenhang ist auch der Entscheid des Kantonsgerichts Graubünden vom 29.10.2007 (Ref. Chur SKA 07 22, E 4.2) interessant, wonach die Aussonderung von Urheberrechten an einem Computerprogramm nicht in Betracht kommt. Hingegen ist gemäss diesem Entscheid die Aussonderung eines Datenträgers möglich, welcher das Computerprogramm enthält. Siehe demgegenüber etwa das Urteil des Oberlandesgerichts Düsseldorf vom 27.9.2012 (I-6, U 241/11, online verfügbar unter *www.datenschutzticker.de/index.php/2013/03/olg-duesseldorf-herausgabe-und-ausonderung-von-kundendaten-vom-insolvenzverwalter)*.

[142] Im Auftragsrecht hat der Beauftragte zur Sicherung seiner Ansprüche ein Retentionsrecht bzw. ein obligatorisches Zurückbehaltungsrecht an den herauszugebenden Vermögenswerten. Es ist fraglich, ob darunter auch Daten fallen. Nach der hier vertretenen Auffassung ist dies jedenfalls dann zu verneinen, wenn die Daten nicht wirtschaftlich verwertbar sind (z.B. aufgrund eines vertraglichen Verwertungsverbotes). Siehe dazu auch BGE 122 IV 322 E. 3a sowie Rolf H. Weber in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang (Hrsg.). Basler Kommentar Obligationenrecht I, 5. A., Basel 2011, N. 19 zu Art. 400 OR, mit weiteren Hinweisen.

[143] Siehe zur Verwertbarkeit von Kundendaten im Insolvenzfall auch Schwaninger/Lattmann (FN 22), Rz. 59.

[144] Siehe zur Datenverschlüsselung und zur Anonymisierung von Personendaten Abschnitt 3.

[145] Escrow-Verhältnisse bringen in der Praxis allerdings zahlreiche Detailfragen mit sich, welche hier nicht näher vertieft werden kön-

10. Vertragsbeendigung

Bereits vor dem Abschluss eines Cloud Service Vertrages sollte an dessen Beendigung gedacht werden. Mitunter werden die Portierbarkeit von Applikationen und die Migrationsmöglichkeiten[146] schon im Rahmen einer vorvertraglichen Due Diligence geprüft. Im Vertrag sollten insbesondere folgende Aspekte möglichst genau beschrieben werden:

- *Vertragsdauer* und ordentliche Vertragsauflösungsmöglichkeiten.[147]
- *Ausserordentliche Vertragsauflösungsgründe*.[148] Typische ausserordentliche Auflösungsgründe sind schwerwiegende Vertragsverletzungen[149], Insolvenz einer Partei[150], Nichtbezahlung der Servicegebühren[151], Verletzung Allgemeiner Nutzungsbedingungen[152], *Change of Control* auf Seiten des Providers[153].
- *Form*[154] *und Fristen* einer Kündigung
- Anspruch des Auftraggebers auf eine *Mindestdauer der Services*[155], eventuell zusätzlich Anspruch auf Weiterführung während einer bestimmten Dauer zu vorausdefinierten Konditionen für den Fall von Verzögerungen beim Backsourcing
- Formate der *Datenübermittlung,* Migration auf neue Formate und Systeme, Abnahmeverfahren
- Modalitäten der *Zugangsbeendigung,* Übergabe elektronischer Schlüssel etc.
- Verpflichtung *zur Beendigungsunterstützung* (z.B. Erstellung eines Migrationskonzepts) und zur Zusammenarbeit mit einem allfälligen neuen Provider, Festlegung der massgebenden Ansätze[156]
- *Abrechnungsmodalitäten.*

---

nen (z.B. ob tatsächlich alle relevanten Softwarekomponenten hinterlegt werden, wie deren fortlaufende Aktualisierung sichergestellt wird und in welchen Fällen sie herauszugeben sind). Siehe zum Escrow generell *www.escrow.ch;* Stefan Eisenhut, Escrow-Verhältnisse: Das Escrow Agreement und ähnliche Sicherungsgeschäfte, Diss. Basel 2009; Leonz Meyer, Source Code-Escrow, in: Florian S. Jörg/Oliver Arter (Hrsg.), Internet-Recht und IT-Verträge, Bern 2006, S. 65–88; Kurt U. Blickenstorfer, Der Sourcecode-Escrow, in: Felix H. Thomann/Georg Rauber (Hrsg.), Softwareschutz, Bern 1998, 211–249; Josef Gellis, Softwarelizenz: Die Stellung des Lizenznehmers bei Veräusserung des Schutzrechts durch den Lizenzgeber oder bei dessen Konkurs, sic 2005, 439–452; Straub (FN 8), 84 ff.

146 Siehe zur Portierbarkeit Abschnitt 7.

147 Gemäss der Studie von Vehlow/Golkowsky (FN 135), 30, sah rund die Hälfte von 51 Providern in ihren Standardverträgen eine Kündigungsfrist von einem Monat vor. Ein einziger Provider ermöglichte eine ordentliche Auflösung innerhalb von 24 Stunden, 8% der Provider stellten jeweils auf das Quartalsende ab.

148 Siehe dazu auch Hon/Millard/Walden (FN 7), 121 ff.

149 Datenschutzverletzungen können vertraglich z.B. generell als schwerwiegende Vertragsverletzung definiert werden.

150 Da der Auftraggeber auch im Insolvenzfall eventuell ein erhebliches Interesse an der Weiternutzung seiner Daten hat (z.B. im Hinblick auf die Gründung einer Auffanggesellschaft), sollte für diesen Fall keine automatische Vertragsauflösung vorgesehen, sondern dem Auftraggeber Gelegenheit gegeben werden, die Services z.B. gegen vorschüssige Bezahlung der Gebühren weiter zu benutzen.

151 Da eine kurzfristige Leistungsbeendigung für den Auftraggeber sehr gravierende Folgen haben kann, sollte für den Fall von Auseinandersetzungen über die Höhe bestimmter Vergütungen eine Hinterlegungsmöglichkeit auf einem Sperrkonto mit befreiender Wirkung sowie ein Eskalationsverfahren bezüglich der Herausgabe der Zahlung vorgesehen werden. Siehe dazu auch Straub (FN 5), Rz. 278.

152 Provider sehen oft allgemeine Nutzungsbedingungen für ihre Services vor. Diese untersagen z.B. Verwendungen, welche gegen Immaterialgüterrecht, Strafrecht etc. verstossen. Der Auftraggeber kann die Handlungen seiner Mitarbeiter aber oft nicht wirksam kontrollieren. Dadurch entsteht die Gefahr, dass aufgrund einer unzulässigen Handlung eines einzelnen Mitarbeiters der ganze Cloud Service Vertrag dahinfällt, was für den Auftraggeber einschneidende Wirkungen haben kann. Vertraglich kann für solche Konstellationen vorgesehen werden, dass der Provider den Auftraggeber zuerst über die Verletzung der Nutzungsbedingungen informieren und abmahnen muss und dass innerhalb einer bestimmten Zeitspanne eine einvernehmliche Lösung gesucht werden soll. Siehe dazu auch Hon/Millard/Walden (FN 7), 122.

153 Der Auftraggeber kann etwa ein Interesse an der Vertragsauflösung haben, wenn der Provider durch einen Konkurrenten des Auftraggebers übernommen wird. In solchen Konstellationen besteht ein erhöhtes Interesse an der Vertraulichkeit der Daten.

154 Siehe dazu auch de la Cruz (FN 12), Rz. 14, wonach für *Infrastructure as a service* gegebenenfalls die Formvorschriften für die Mietkündigung von Art. 226l OR einzuhalten sind. Nach dem hier vertretenen Verständnis ist Mietrecht allerdings höchstens analog auf Cloud Service Verträge anwendbar, da der Servicegedanke gegenüber der Gebrauchsüberlassung im Vordergrund steht. Auch bei *Infrastructure as a service* vermietet der Provider in der Regel nicht ein bestimmtes Gerät, sondern verpflichtet sich, Speicherkapazität mit bestimmten Leistungsmerkmalen zur Verfügung zu stellen. Nach der hier vertretenen Auffassung ist Art. 226l OR daher auf Cloud Services grundsätzlich nicht anwendbar.

155 Gemäss der Untersuchung von Hon/Millard/Walden (FN 7), 120, war eine dreijährige Mindestvertragsdauer am gebräuchlichsten.

156 Gemäss Vehlow/Golkowsky (FN 135), 30, stellten 25% der Provider ihren Kunden nach Vertragsbeendigung Zusatzkosten – vorwiegend in Zusammenhang mit gesetzlichen Aufbewahrungsfristen – in Rechnung.