Jusletter

# Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke 2.0.

**Autoren/Autorinnen:** David Schwaninger / Michelle Merz
**Beitragsart:** Beiträge
**Rechtsgebiete:** Datenschutz, Informatik und Recht
**DOI:** 10.38023/622c3a33-9a87-454e-844e-b88c37e4e46e
**Zitiervorschlag:** David Schwaninger / Michelle Merz, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke 2.0., in: Jusletter 21. Juni 2021

*Die Nutzung cloudbasierter Lösungen wächst ungebrochen. Bereits im Jusletter vom 11. März 2013 haben die damaligen Autoren zum Cloud Computing rechtliche Probleme beleuchtet – seither hat sich im Datenschutzrecht viel getan. So trat die DSGVO in Kraft und das DSG wird totalrevidiert. Das hat die Autoren veranlasst, erneut rechtliche Probleme in der Wolke zu diskutieren. Der Artikel geht auf die (revidierten) datenschutzrechtlichen Regelungen ein, behandelt Besonderheiten bei gesetzlich geschützten Daten und die Rückgabe der Daten an den Cloud Nutzer und legt dar, welche Risiken beim Auslagern der Daten in die Wolke beachtet werden müssen.*

## Inhaltsverzeichnis



## I. Einleitung und technische Grundlagen

### A. Einleitung

[1] Immer mehr Unternehmen lagern ihre bisher intern erledigten Datenbearbeitungen an externe Unternehmen aus und nutzen dafür Cloud Computing. Beim Cloud Computing werden Speicherkapazitäten, Rechnerleistungen oder Software über ein Netzwerk (Internet)[1] bedarfsorientiert genutzt – die IT-Infrastruktur wird ausgelagert. Beim Bezug solcher cloudbasierter Lösungen steht die IT-Landschaft typischerweise nicht mehr im Eigentum des Unternehmens und wird auch nicht mehr von diesem betrieben, sondern als Dienstleistung von einem oder mehreren Cloud Anbietern bezogen. Sämtliche Dienstleistungen in der Wolke werden auf den Servern der Cloud Anbieter, d.h. auf vom Dienstleister zur Verfügung gestellter Hardware erbracht. Die Vorteile des Einsatzes von Cloud-Computing-Systemen liegen auf der Hand – geringere Kosten und Wartung für eigene IT-Infrastruktur und Software, höhere Rechenleistung, dynamischer Speicherplatz, schnelle und einfache Verfügbarkeit, Skalierbarkeit und teilweise auch erhöhte Sicherheit. Allerdings ist die Auslagerung von Daten in die Cloud auch immer mit Risiken wie dem Kontrollverlust über die Daten, fehlender Portabilität und Isolierung der verschiedenen Datenbearbeitungen, Compliance Risiken sowie allenfalls möglichen Zugriffen von ausländischen Behörden auf die Daten verbunden. Zu diesen Risiken und deren (vertraglich zu regelnden) Minimierung wird nachfolgend Stellung genommen.

[2] Für die Definition der datenschutzrechtlichen Pflichten und Rechte für Cloud Anbieter ist die funktionale Abgrenzung zwischen Verantwortlichem und Auftragsdatenbearbeiter zentral. Als Verantwortlicher gilt diejenige Person, die über die Zwecke und Mittel der Bearbeitung von Personendaten entscheidet. Im Gegensatz dazu ist der Auftragsdatenbearbeiter eine Person, die Personendaten im Auftrag des Verantwortlichen bearbeitet. Im Bereich des Cloud Computing dürfte der Cloud Anbieter in den meisten Fällen als Auftragsdatenbearbeiter qualifiziert werden. Diese Qualifikation gilt unter der Einschränkung, dass der Cloud Anbieter überhaupt Personendaten bearbeitet (da andernfalls die Datenschutzgesetze gar keine Anwendung finden). Es ist jedenfalls für die Abgrenzung von Verantwortlichem und Auftragsdatenbearbeiter im Einzelfall zu prüfen, bei wem die Entscheidkompetenz betreffend der Datenbearbeitung liegt.

[3] Da dieser Artikel ein Update zum im Jahre 2013 gleichnamig erschienenen Artikel darstellt, wird auf die Nennung der bereits dort abgehandelten allgemeinen datenschutzrechtlichen Grundlagen und -sätze verzichtet. Einzig auf die Definition von Personendaten wird hier nochmals hingewiesen, da der Fokus dieses Artikels in der Auslagerung von Personendaten in der Cloud liegt. Datenschutzrechtlich gelten als Personendaten alle Angaben, welche sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[2] Für die Qualifikation wird jeweils aus der Sicht desjenigen, der Zugang zu einer Information hat, beurteilt, ob dieser (a) in der Lage ist, herauszufinden, auf welche natürliche Person sich die Information bezieht und (b) ob er auch bereit ist, den für die Identifikation erforderlichen Aufwand zu betreiben.[3]

## B. Technische Grundlagen

[4] Es sind unterschiedliche *Organisationsformen* des Cloud Computing zu unterscheiden. Bei einer sog. Public Cloud bewirtschaftet der Cloud Anbieter die Infrastruktur an einem oder mehreren von ihm bestimmten Serverstandorten. Bei einer Private Cloud hingegen wird die Infrastruktur durch ein Unternehmen oder einen externen Dritten betrieben und ist nur auf das jeweilige Unternehmen ausgerichtet. Bei einer parallelen Nutzung von Public und Private Cloud spricht man von einer Hybrid Cloud. Bei der Community Cloud nutzen verschiedene Organisationen dieselbe Infrastruktur gemeinsam aber im Unterschied zur Public Cloud nur für sich.

[5] Bei den Servicemodellen werden drei unterschiedliche *Typen*[4] unterschieden. Bei der IaaS (Infrastructure as a Service) wird dem Cloud Nutzer ein Server zur Verfügung gestellt, wobei das Funktionieren der IT-Infrastruktur allein in der Verantwortung des Cloud Anbieters liegt. Der Cloud Nutzer kann auf dem fremden Server selbstständig eigene Software installieren. Entwickelt der Cloud Anbieter eine Anwendung und stellt diese den Nutzern in der Cloud zur Verfügung, spricht man von PaaS (Platform as a Service). Hierbei erfolgt die Bewirtschaftung der Daten durch den Nutzer selbst. Bei PaaS behält der Cloud Nutzer somit die Kontrolle über seine selbst entwickelte Software, benötigt aber keine eigene Entwicklungsumgebung. Bei der SaaS (Software as a Service) wird eine Software über das Internet resp. über einen Web-Browser zur Verfügung gestellt und genutzt. Der Cloud Nutzer bewirtschaftet die Software nicht mehr selber. In der Cloud wird dem Nutzer eine Funktionalität zur Verfügung gestellt, um dort Daten bearbeiten zu können.

## II. Allgemeine datenschutzrechtliche Vorgaben bei der Auslagerung in eine Cloud

### A. Nach rev-DSG

#### 1. Auslagerung der Daten in eine Cloud in der Schweiz

[6] Auch nach dem revidierten Datenschutzgesetz (rev-DSG) liegt eine Datenbearbeitung durch einen Auftragsbearbeiter vor, wenn bei der Nutzung von Cloud Computing Personendaten bearbeitet werden. Nach Art. 10a DSG (bzw. Art. 9 rev-DSG) darf das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz einem Auftragsbearbeiter wie dem Cloud Anbieter übertragen werden, wenn die Daten nur in der Weise bearbeitet werden, wie der Auftraggeber (hier der Cloud Nutzer) es selbst tun dürfte und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten die Übertragung verbieten. Eine Auftragsdatenbearbeitung ist sowohl nach aktuell gültigem DSG wie auch nach dem revidierten DSG ohne Einwilligung der betroffenen Person zulässig, sofern die obgenannten Voraussetzungen eingehalten sind. Unzulässig hingegen wäre die Bearbeitung von Personendaten durch einen Cloud Anbieter zu eigenen Zwecken. Um sicherzustellen, dass der Cloud Anbieter die Daten nicht anders bearbeitet, als es der Cloud Nutzer darf, sollte die Art der Bearbeitung der Daten im Vertrag schriftlich geregelt werden.[5] Der Auftraggeber muss sich dabei vergewissern, dass der Dritte die Datensicherheit gewährleistet. Mit anderen Worten muss der Cloud Anbieter verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden bzw. an die anwendbaren Datenschutzbestimmungen zu halten. Dies erstreckt sich in gleichem Umfang auf allfällige durch den Cloud Anbieter eingesetzte Subunternehmer. Nach dem revidierten DSG darf der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen (Abs. 3 von Art. 9 rev-DSG).

[7] Da der Cloud Anbieter als Hilfsperson des Cloud Nutzers zu qualifizieren ist, sind die Cloud Nutzer zur sorgfältigen Auswahl, Instruktion und Überwachung des Cloud Anbieters verpflichtet.[6] Im Rahmen der Datensicherheit muss der Cloud Anbieter die Personendaten durch angemessene technische und organisatorische Massnahmen[7] gegen unbefugtes Bearbeiten schützen sowie für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sorgen (Art. 8 Abs. 1 VDSG).[8]

[8] Nach dem revidierten DSG werden mit einer Busse bis zu CHF 250’000.00 private Personen[9] auf Antrag bestraft, die vorsätzlich die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die obgenannten Voraussetzungen erfüllt sind (Art. 61 lit. b rev-DSG).

Dieselbe Busse droht, wenn die Mindestanforderungen an die Datensicherheit nicht eingehalten werden (lit. c).

### 2. Auslagerung der Daten in eine Cloud mit Auslandberührung

[9] Häufig bedingt die Nutzung von Cloud Computing eine Datenbekanntgabe ins Ausland, da die Bearbeitung oftmals auf Servern in verschiedenen Ländern stattfindet. Grundsätzlich gilt, dass Personendaten ohne weitere Massnahmen in diejenigen Länder bekanntgegeben werden dürfen, die über einen aus Schweizer Sicht angemessenen Datenschutz verfügen.[10] Bei der Auslagerung in eine Cloud geht es aber oft auch um Länder, die ein tieferes Datenschutzniveau als die Schweiz aufweisen. Unter diesen Umständen dürfen Personendaten nur ins Ausland bekannt gegeben werden, wenn die Voraussetzungen nach Art. 6 Abs. 2 DSG erfüllt sind (Art. 16 f. rev-DSG). Dasselbe gilt, wenn Personen ausserhalb der Schweiz auf die in der Cloud gespeicherten Daten zugreifen können.[11] Danach hat in vielen Fällen der Cloud Nutzer mit dem Cloud Anbieter vertragliche Datenschutzgarantien abzuschliessen, möchte er nicht von einer (widerrufbaren) Einwilligung von betroffenen Personen abhängig sein. Weiter trägt der Cloud Nutzer die Nachweispflicht, dass alle erforderlichen Massnahmen getroffen wurden, um ein angemessenes Schutzniveau zu gewähren. Als vertragliche Datenschutzgarantie kommt insbesondere der Abschluss von sogenannten Standardvertragsklauseln in Frage. Der EDÖB hat insbesondere die Standardvertragsklauseln der EU, den Mustervertrag des Europarates für die Sicherstellung eines angemessenen Datenschutzes im Rahmen des grenzüberschreitenden Datenverkehrs wie auch den Mustervertrag des EDÖB für das Outsourcing von Datenbearbeitungen im Ausland als angemessen anerkannt.[12] Es können auch andere Vertrags- oder Garantieformen angewendet werden, wobei die spezifischen Datenschutzklauseln ein angemessenes, d.h. DSG-konformes Datenschutzniveau garantieren müssen. Diesfalls besteht eine Informationspflicht an den EDÖB.[13]

[10] Cloud Anbieter haben häufig ihre Server in den USA stationiert. Aus Schweizerischer Sicht verfügen die USA über kein angemessenes Datenschutzniveau und dementsprechend sind Datenschutzgarantien abzuschliessen. Während früher unter dem Safe Harbor Abkommen Datenübermittlungen ohne entsprechende vertragliche Vorkehrungen in die USA übermittelt werden durften, konnten sich seit dem 12. April 2017 amerikanische Unternehmen für das Swiss-US Privacy Shield zertifizieren lassen, nachdem das Safe Harbor Abkommen als ungültig erklärt wurde. War der Cloud Anbieter entsprechend zertifiziert, konnten bis anhin Personendaten ohne weiteren Handlungsbedarf übermittelt werden. Wie unten näher zu erörtern ist, hat der EuGH mit Urteil vom 16. Juli 2020 entschieden, dass der EU-Privacy Shield ungültig ist.[14] Auch der EDÖB hält den Privacy Shield für ungenügend.

[11] Nach dem revidierten DSG werden mit einer Busse von bis zu CHF 250’000.00 private Personen auf Antrag bestraft, die vorsätzlich Personendaten ins Ausland bekannt geben, ohne dass die obgenannten Voraussetzungen erfüllt sind (Art. 66 lit. a rev-DSG). Der rechtskonformen Auslagerung von Personendaten ins Ausland ist somit unbedingt Rechnung zu tragen.

## B. Nach DSGVO

[12] Die in der Europäischen Union geltende Datenschutz-Grundverordnung (DSGVO) wirkt extraterritorial und findet somit unter Umständen auch für Schweizer Unternehmer und Cloud Nutzer Anwendung. Die Verordnung gilt nämlich auch für die Verarbeitung personenbezogener Daten,[15] wenn der Verantwortliche oder Auftragsverarbeiter nicht über eine Niederlassung in der Union verfügt, seine Waren oder Dienstleistungen aber in der EU anbietet (Art. 3 Abs. 2 lit.

a DSGVO) oder das Verhalten von betroffenen Personen in der Union beobachtet (lit. b).[16] Als Hinweise auf ein Angebot nach Art. 3 Abs. 1 lit. a DSGVO gilt z.B. die Verwendung einer Sprache, die in der EU zwar gebräuchlich, im Land des Anbieters aber eine Fremdsprache ist sowie der Hinweis auf den EURO oder wenn Kunden aus der EU erwähnt werden.[17] Unter Beobachtung nach lit. b der Bestimmung fällt die Erhebung personenbezogener Daten zwecks Profiling, bspw. zu Werbezwecken. In der Praxis dürften doch so einige Schweizer Unternehmen in den Anwendungsbereich der DSGVO fallen. Aus diesem Grund werden nachfolgend die Voraussetzungen betreffend eine Auslagerung in die Cloud auch unter der DSGVO kurz dargelegt.

[13] Auch nach der DSGVO kann der Verantwortliche Auftragsdatenbearbeiter benennen (nach DSGVO-Wortlaut sog. Auftragsverarbeiter; Art. 28 Abs. 1 DSGVO), muss diesen allerdings gesetzeskonform einbinden.[18] So darf der Verantwortliche nur Auftragsverarbeiter beiziehen, welche die Einhaltung des Datenschutzes gewährleisten und zwischen den Parteien muss eine Vereinbarung mit den Mindestinhalten von Art. 28 Abs. 3 DSGVO geschlossen werden (schriftlich oder in Textform). Auch unter der DSGVO muss der Verantwortliche die Tätigkeit des Auftragsverarbeiters angemessen überwachen.

[14] Die DSGVO sieht bei der Übermittlung von personenbezogenen Daten in sog. Drittländer (neben den EU-Staaten gelten auch die EWR-Staaten Island, Liechtenstein und Norwegen nicht als Drittländer) besondere Voraussetzungen vor. Nach Art. 45 ff. DSGVO muss alternativ ein Angemessenheitsbeschluss der Europäischen Kommission vorliegen, es müssen geeignete Garantien oder Binding Corporate Rules vorliegen oder es muss eine sog. Ausnahmevorschrift (Einwilligung oder Ausnahmen nach Art. 49 Abs. 1 lit. b–f DSGVO) erfüllt sein.

[15] Die EU-Kommission hat für die Schweiz ein Angemessenheitsbeschluss erlassen und festgestellt, dass die Schweiz ein angemessenes Schutzniveau bietet, sodass eine Datenübermittlung keiner besonderen Genehmigung bedarf. Zurzeit überprüft die Kommission gerade diesen Beschluss. Für Datenübermittlungen in die USA galt bisher zunächst das Safe Harbor Abkommen mit den USA, später der EU-U.S. Privacy Shield als Angemessenheitsbeschluss. Mit Urteil des EuGH vom 16. Juli 2020 wurde nun auch das EU-U.S. Privacy Shield als unwirksam erklärt. Die USA bietet nach Ansicht der EU kein angemessenes Datenschutzniveau. Somit müssen für Datenübermittlungen in die USA wie auch in andere Länder ohne angemessenem Niveau entweder Garantien vorliegen oder eine Ausnahmevorschrift erfüllt sein.

[16] Falls kein Angemessenheitsentscheid vorliegt, dürfen personenbezogene Daten nur in ein Drittland übermittelt werden, sofern geeignete Garantien vorgesehen sind und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Geeignete Garantien sind namentlich sog. Standardvertragsklauseln (Standard Contractual Clauses, SCC), welche entweder von der Kommission oder von einer mitgliedschaftlichen Aufsichtsbehörde erlassen werden. Weiter können verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) von der mitgliedstaatlichen Aufsichtsbehörde genehmigt werden.

[17] Zu beachten ist, dass die vorgenannte Europäische Kommission am 4. Juni 2021 neue Standardvertragsklauseln veröffentlich hat, welche die bisherigen SCC ersetzen und ab dem 27. September 2021 zu verwenden sind. Zudem müssen Verträge, die auf den bisherigen SCC basieren während einer Übergangsfrist von 15 Monaten, mithin bis zum 27. Dezember 2022 an die neuen Standardvertragsklauseln angepasst werden.[19]

[18] Werden die Pflichten des Verantwortlichen respektive des Auftragsverarbeiters gemäss Art. 28 bzw. 32 DSGVO durch den Verantwortlichen oder einen Auftragsverarbeiter verletzt, haften diese nicht nur für den allenfalls eingetretenen Schaden der betroffenen Personen, sondern können zusätzlich durch die Aufsichtsbehörden mit einer Busse bis EUR 10 Mio. oder 2% des Jahresumsatzes sanktioniert werden.

### C. Der US-Cloud Act im Besonderen

[19] Die USA hat per Ende März 2018 den U.S. Clarifying Lawful Overseas Use Of Data Act (Cloud Act) in Kraft gesetzt. Danach können amerikanische Behörden für strafrechtliche Zwecke auch ohne Rückgriff auf internationale Rechtshilfeabkommen Auskunftsbegehren betreffend Personendaten stellen, welche sich im Besitz, in Gewahrsam oder unter Kontrolle eines in den USA domizilierten Unternehmens befinden. Dies gilt unabhängig davon, ob die Personendaten sich innerhalb oder ausserhalb der USA befinden.[20] Es stellt sich nun die Frage, ob der US-Cloud Act der Auslagerung von Personendaten in die Wolke im Weg steht. Festzuhalten ist zunächst, dass unter dem Cloud Act nur ein Zugriff auf Personendaten möglich ist, wenn es sich um gerichtlich festgestellte schwere Straftaten handelt, nicht jedoch bei zivilrechtlichen Ansprüchen oder aufsichtsrechtlichen Abklärungen. Dies schränkt den Anwendungsbereich des Cloud Acts entsprechend ein. Zudem muss der Cloud Anbieter technisch überhaupt Zugriff auf die Personendaten verschaffen können, was beispielsweise bei einer Totalverschlüsselung Stand heute nicht möglich ist. DAVID ROSENTHAL hat für die Beurteilung des Risikos eines solchen Zugriffes u.a. nach dem Cloud Act ein entsprechendes Modell veröffentlicht.[21] Jedenfalls ist dem Risiko eines Zugriffs gestützt auf den Cloud Act Rechnung zu tragen.

## III. Besonderheiten bei gesetzlich geschützten Daten

### A. Auslagerung von durch ein Berufsgeheimnis geschützten Daten

[20] Nach Art. 321 StGB werden Berufsgeheimnisträger und deren Hilfspersonen auf Antrag bestraft, wenn sie ein geschütztes Geheimnis einem unberechtigten Dritten offenbaren und dabei vorsätzlich und ohne Rechtfertigungsgrund handeln. Das Bundesgericht hat in einem Entscheid festgehalten, dass der Cloud Anbieter als Hilfsperson nach Art. 321 StGB qualifiziert.[22] Der Beizug von Hilfspersonen ist nicht schrankenlos zulässig, es müssen auch diesfalls alle zumutbaren Massnahmen ergriffen werden, um einen hinreichenden Schutz der auszulagernden Informationen sicherzustellen.

[21] Der objektive Tatbestand von Art. 321 StGB ist erfüllt, wenn der Geheimnisträger das Geheimnis einem dazu nicht ermächtigten Dritten zur Kenntnis bringt oder diesem die Kenntnisnahme ermöglicht. Sowohl nach der h.L. wie auch nach der Rechtsprechung des Bundesgerichts wird die Kenntnisnahme durch einen Dritten für die Vollendung der Tat vorausgesetzt.[23] Bei anonymisierten oder verschlüsselten Informationen wird eine Kenntnisnahme verunmöglicht, folglich liegt kein Offenbaren vor.[24] In der Regel werden beim IaaS Modell die Daten im Archiv verschlüsselt, bei SaaS hingegen hat der Cloud Anbieter technisch gesehen Zugang zu den gespeicherten Daten. Somit ist beim SaaS Modell eine Kenntnisnahme grundsätzlich möglich, im IaaS Modell i.d.R. hingegen ausgeschlossen.

[22] Hilfspersonen sind nach wohl h.L. keine Dritten. Somit ist das Offenbaren von Geheimnissen gegenüber dem Cloud Anbieter straflos, wenn die weiteren Voraussetzungen gegeben sind. Diesfalls dürfen Anwälte oder auch Ärzte dem Cloud Anbieter als Hilfsperson die durch das Berufsgeheimnis geschützten Informationen zugänglich machen, ohne dass ein

unzulässiges Offenbaren vorliegt.[25] Zusammenfassend darf ein Berufsgeheimnisträger geschützte Personendaten in die Wolke auslagern, wenn die Personendaten angemessen geschützt sind, die betroffene Person zumindest nach dem revidierten DSG darüber informiert ist und ein effektives Subordinationsverhältnis zwischen dem Cloud Anbieter und dem Cloud Nutzer mit den entsprechenden Weisungsrechten besteht.[26] Darauf hinzuweisen ist aber insbesondere, dass das Bundesgericht in Bezug auf das Berufsgeheimnis es als unzulässig erachtet, dass der Anwalt der Hilfsperson erlaubt, die Haftung mit Bezug auf Verletzungen des Berufsgeheimnisses auszuschliessen bzw. auf das gesetzlich sonst zulässige Minimum zu reduzieren.[27] Zudem darf die Hilfsperson von ihr übernommene Aufgaben nicht einfach von einem Dritten ausführen lassen (Subdelegation).[28] Dies kann jedoch nur dann gelten, wenn dieser Dritte auf vom Berufsgeheimnis geschützte Daten zugreifen kann, ohne dass er verpflichtet ist, vorgängig das Einverständnis des Anwaltes einzuholen. Ebenfalls zulässig wäre die direkte Beauftragung des Dritten durch den Anwalt selbst. Nach verschiedenen Lehrmeinungen genügt es auch, wenn die Hilfsperson vom Anwalt verpflichtet wird, ihre genehmigten Untergehilfen zur Wahrung des Berufsgeheimnisses zu verpflichten, was u.E. zutreffend ist.[29]

### B. Auslagerung von Bankkundendaten im Besonderen

[23] Die Auslagerung von Bankkundendaten hat längst auch die Bankenwelt erreicht. Unter dem Begriff «Cloud Banking» wird die Bereitstellung und Erbringung von Bank- und Finanzdienstleistungen auf Grundlage der Cloud-Technologe definiert.[30] Es stellt sich die Frage, ob das Übertragen von Bankkundendaten in eine Cloud mit dem Bankkundengeheimnis vereinbar ist oder nicht. Nach Art. 47 des Bankengesetzes (BankG) wird bestraft, wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Organ, Angestellter, Beauftragter oder Liquidator einer Bank anvertraut worden ist. Unzulässig wäre demnach die Auslagerung der Bankkundendaten in die Cloud nur, wenn sie als Offenbarungshandlung im Sinne von Art. 47 BankG qualifiziert. Sofern die Bank ausreichende technische und organisatorische Massnahmen zum Schutz gegen unbefugte Zugriffe einsetzt, macht sie sich nach Art. 47 BankG nicht strafbar.[31] Zudem besteht nach der wohl h.L. die Ansicht, dass Cloud Anbieter als Beauftragte im Sinne von Art. 47 Abs. 1 lit. a BankG bestellt werden können, was bedeutet, dass die Bank mit dem Cloud Anbieter auch geheimnisgeschützte Informationen austauschen darf.[32] Dabei ist ein Beizug eines Beauftragten grundsätzlich auch zulässig, wenn sich der Beauftragte im Ausland befindet.[33]

## IV. Rückgabe von Daten an den Cloud Nutzer

### A. Allgemeines

[24] Sind die Daten einmal in der Cloud, bestimmt in den meisten Fällen der Cloud Anbieter über die Verwaltung dieser Daten. Will der Cloud Nutzer den Cloud Anbieter wechseln oder geht der Cloud Anbieter Konkurs, stellt sich die Frage nach der Herausgabe der Daten. Wichtig ist, dass die Daten dem Cloud Nutzer in einem Format übergeben werden, welches ihm erlaubt, diese wieder in eine eigene IT-Umgebung oder in die Cloud eines anderen Cloud Anbieters zu integrieren. Zudem ist bei der Rückgabe sicherzustellen, dass der Cloud Anbieter alle entsprechenden Daten herausgibt bzw. diese zu gegebener Zeit vernichtet. Daher ist entsprechend wichtig, die Form und Modalitäten der Rückgabe von Daten bzw. die Löschung von Backups vertraglich klar zwischen dem Cloud Nutzer und dem Cloud Anbieter zu regeln. Nach Ansicht der Autoren muss aber gerade bei der Löschung von Backups der Verhältnismässigkeit und Umsetzbarkeit Rechnung getragen und ein sinnvoller Zeitraum vereinbart werden.

### B. Konkurs eines Cloud Anbieters

[25] In der Schweiz fehlt eine gesetzliche Normierung betreffend Rechte in Bezug auf die Daten wie die Berechtigung zur Übertragung, die Ausübung von Abwehrrechten oder die Zwangsvollstreckung.[34] Fällt der Cloud Anbieter in den Konkurs, stehen dem Cloud Nutzer nur beschränkte Möglichkeiten zur Verfügung. Falls die Daten einen Wert haben, wird die Forderung auf Rückgabe nach Art. 211 Abs. 1 SchKG in eine Geldforderung von entsprechendem Wert umgewandelt. Der Cloud Nutzer erhält am Ende des Konkursverfahrens allenfalls eine Konkursdividende, die in aller Regel nur einen kleinen Teil der Konkursforderung beträgt. Die Herausgabe der Daten kann so aber nicht erwirkt werden. Steht die Übermittlung der gespeicherten Daten im Interesse der Masse, kann die Konkursmasse nach Art. 211 Abs. 2 SchKG in den Vertrag eintreten. Andererseits kann der Cloud Nutzer versuchen, ein Aussonderungsrecht an den Daten geltend zu machen. Nach einem Teil der Lehre besteht de lege lata ein konkursfester Herausgabeanspruch (Aussonderung), sofern die Daten beim Cloud Anbieter ohne Ermächtigung zur Weiterveräusserung einfach gespeichert werden.[35] Dies wird dadurch begründet, dass bei der Möglichkeit der Aussonderung der Daten eine Lücke vorliegt, welche durch analoge Anwendung des Gesetzesrechts gefüllt werden muss. Voraussetzung ist, dass die auszusondernde Sache oder Forderung nur einem ganz bestimmten Berechtigten zugeordnet werden kann. Da der Cloud Nutzer bei der Speicherung von Personendaten in einer Cloud ähnlich gelagerte Interessen verfolge wie der Hinterleger oder der Mieter eines Lagerraumes, der seine Sachen im Konkurs aussondern soll, lasse sich eine analoge Anwendung auf Daten rechtfertigen. Zudem könne unter den Sachenbegriff auch Daten subsumiert werden.[36] Ein anderer Teil der Lehre vertritt die Ansicht, dass es sich bei Daten nicht um bewegliche Sachen im sachenrechtlichen Sinn handelt[37] und daher eine Aussonderung nicht möglich sei. Ausserdem fehle es an einer rechtlichen Grundlage, um bei einer Konkursverwaltung den Antrag auf Rückgabe der hinterlegten Daten zu stellen. Jedenfalls kann nicht darauf abgestellt werden, dass Daten in einem Konkurs herausverlangt werden können.[38] Zusammenfassend ist damit die Rechtslage betreffend Herausgabe der Daten im Konkursfall des Cloud Anbieters zurzeit unklar. Durch die Verbreitung der Blockchain Technologie haben sich Bundesrat und Parlament veranlasst gesehen, für kryptobasierte Vermögenswerte ein Aussonderungsrecht zu schaffen (Art. 242a E-SchKG). Dabei soll in einem neuen Art. 242b E-SchKG auch ein Zugangs- und Herausgaberecht für Daten eingeführt werden.[39] Da der Begriff Daten in besagtem Art. 242b E-SchKG allgemein genannt und nicht nur auf kryptobasierte Vermögenswerte bezogen wird, wird die Frage in Zukunft geklärt sein. Auch dann ist aber zu beachten, dass eine Herausgabe von Daten Zeit in Anspruch nimmt und keine Gewähr besteht, dass die Daten bis dann keinen Schaden genommen haben. Aus dem Grund sollten bei der Auslagerung von Daten immer Alternativen evaluiert werden (z.B. Backups).

## V. Risikoanalyse

[26] Wie oben dargelegt, ist der Einsatz von Cloud Computing mit verschiedenen Risiken verbunden, einerseits auf der technischen Seite, welchen mit entsprechend technischen Lösungen begegnet werden muss, andererseits bestehen auch rechtliche Risiken, welche mit vertraglichen Vorkehrungen minimiert werden können.

[27] Cloud-spezifische technische Risiken sind insbesondere folgende:

- Vertraulichkeit der Daten (Verschlüsselung und Geheimnisschutz);
- Umsetzung der notwendigen IT-Sicherheitsmassnahmen;
- Überprüfbarkeit der Abläufe und Prozesse;
- Datenverlust und Datenmissbrauch;
- Portabilität und Interoperabilität.

[28] Rechtliche Risiken beim Einsatz von Cloud Computing Dienstleistungen:

- Unklare Zuteilung der Verantwortlichkeiten zwischen dem Cloud Nutzer und dem Cloud Anbieter und unklarer Leistungsbeschrieb;
- Transparenz über die Standorte der Server;
- Verlust der Kontrolle[40] oder Verunmöglichen der Kontrollpflichten;
- Durchsetzbarkeit der datenschutzrechtlichen Ansprüche (Löschungs- und Berichtigungsansprüche);
- Gewährleistung eines gleichwertigen Datenschutzniveaus.

## VI. Technische Massnahmen und Vertragsgestaltung

[29] Wie oben dargelegt, bleibt die Verantwortung betreffend Einhaltung der datenschutzrechtlichen Vorgaben beim Verantwortlichen. Der Cloud Nutzer hat bei der Inanspruchnahme von Cloud Dienstleistungen die spezifischen technischen und rechtlichen Risiken durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren.

### A. Technische Massnahmen

[30] Es ist sicherzustellen, dass die *technischen Risiken* mit organisatorischen und technischen Massnahmen minimiert werden. Selbstverständlich muss die Umsetzung der technischen und organisatorischen Massnahmen auch im Vertragswerk Eingang finden, insbesondere sollen die technischen Verantwortungen, welche sich aus den jeweiligen Typen ergeben, in den Verträgen klar zugeteilt werden. Der unberechtigte Zugriff sowie böswillige Löschungen oder Mutationen sollten durch Authentifizierungs- und Identifizierungsverfahren verhindert werden. Zudem sollten alle Veränderungen mittels Protokollierungsmassnahmen aufgezeichnet werden. Eine Möglichkeit in technischer Hinsicht besteht darin, dass die Daten vor der Übertragung und Auslagerung in die Wolke durch Anonymisierung oder Pseudonymisierung geschützt werden.[41] Dann handelt es sich datenschutzrechtlich gesehen nicht mehr um Personendaten und das Datenschutzgesetz ist nicht mehr anwendbar. Allerdings würde dabei in den meisten Fällen der Zweck der Auslagerung von Personendaten nur teilweise erreicht. Zudem ist die Verschlüsselung entsprechend zu regeln.

[31] Sowohl das DSG wie auch die DSGVO halten geeignete technische und organisatorische Massnahmen fest, welche eingehalten werden müssen. Nach dem aktuell geltenden DSG ist insbesondere auf den entsprechenden Leitfaden des EDÖB zu verweisen.[42] Nach dem revidierten DSG wurden die Anforderungen an die technischen und organisatorischen Massnahmen ausgebaut und insbesondere sind nach Art. 8 rev-DSG der Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen vorausgesetzt.[43] Weitere Mindestanforderungen an die Datensicherheit wird der Bundesrat zum revidierten DSG noch erlassen. Nach der DSGVO hat der Verantwortliche namentlich die Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO), die Sicherheit der Datenverarbeitung gemäss Art. 32 DSGVO wie auch die Vorgaben zur Auftragsverarbeitung nach Art. 28 DSGVO zu berücksichtigen. Geeignete technische und organisatorische Massnahmen sind nach Art. 24 Abs. 1 DSGVO unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen festzulegen. Bei Nichterfüllung dieser Vorgaben drohen dem Verantwortlichen Schadenersatzansprüche und Geldbussen nach Art. 82 ff. DSGVO.

### B. Vertragsgestaltung

[32] Die *rechtlichen Risiken* sind bei der Vertragsgestaltung zu beachten und auszuschliessen bzw. zu reduzieren. Bei den rechtlichen Risiken ist folgenden Punkten besondere Beachtung zu schenken:

- Detaillierte Umschreibung der Services: Je nach Typ des Servicemodelles ist entsprechend der Umfang der Dienstleistung im Einzelnen zu umschreiben. Bei IaaS-Verträgen ist insbesondere die Beschreibung der Infrastruktur, Verfügbarkeiten und Service Levels, Lizenzen und Nutzungsrechte sowie Backup-Themen zentral, wohingegen bei SaaS insbesondere die Beschreibung der zur Verfügung gestellten Software, das Nutzungsmodell sowie die Datenmigration wesentlich zu definierende Punkte darstellen.[44]
- Zusicherung der Einhaltung sämtlicher datenschutzrechtlicher Vorgaben: Der Cloud Anbieter sollte vertraglich zusichern, dass er sämtliche anwendbaren datenschutzrechtlichen Vorgaben jederzeit und vollumfänglich erfüllt.
- Ort der Datenbearbeitung: Es sollte schriftlich vereinbart werden, dass der Cloud Anbieter über sämtliche möglichen Datenbearbeitungsorte Auskunft erteilen muss bzw. an welchen Orten der Cloud Anbieter überhaupt Datenbearbeitungen vornehmen darf. Standortwechsel sollten gemeldet und vom Cloud Nutzer vorgängig schriftlich bewilligt bzw. abgelehnt werden können, wenn sonst Risiken drohen.
- Kontroll- und Weisungsrechte: Kontroll- und Weisungsrechte des Cloud Nutzers sind vertraglich festzuhalten, damit der Cloud Nutzer prüfen kann, dass der Cloud Anbieter die Daten nur in einer Weise bearbeitet, wie es auch der Cloud Nutzer selber darf.
- Rechte Betroffener: Es sind vertragliche Regelungen zu vereinbaren, welche die Gewährleistung der Betroffenenrechte sicherstellen. Insbesondere ist zu empfehlen, dass nur der Cloud Nutzer die Betroffenenrechte selbst wahrt und der Cloud Anbieter sofort den Cloud Nutzer zu informieren hat, wenn bei ihm entsprechende Gesuche von betroffenen Personen eingehen. Zudem hat der Cloud Anbieter vertraglich die Durchsetzung der Rechte der Betroffener auf Berichtigung und Löschung bzw. das Recht auf Vergessen[45] bei entsprechender Aufforderung des Cloud Nutzers zu gewährleisten.
- Meldepflichten des Cloud Anbieters: Neben den Gesuchen von betroffenen Personen zur Wahrung ihrer Rechte ist der Cloud Anbieter vertraglich zu verpflichten, Sicherheitsvorfälle jeglicher Art unverzüglich dem Cloud Nutzer zu melden. Das ist wichtig, damit der Cloud Nutzer seiner Pflicht zur entsprechenden Meldung an Datenschutzbehörden rechtmässig nachkommen kann.
- Gleichwertiges Datenschutzniveau: Sofern die Nutzung von Cloud Services eine Datenbearbeitung im Ausland beinhaltet, sind weitere vertragliche Massnahmen notwendig. Wie oben dargelegt, dürfen Personendaten nur ins Ausland ausgelagert werden, wenn ein im Vergleich zur Schweiz gleichwertiges Datenschutzniveau besteht und/oder zusätzliche Sicherheitsmassnahmen umgesetzt werden.
- Verzeichnis der Bearbeitungstätigkeiten: Sowohl nach der DSGVO wie auch nach dem rev-DSG sind Auftragsdatenbearbeiter grundsätzlich verpflichtet, ein entsprechendes Verzeichnis über Datenbearbeitungen zu erstellen.[46] Dies sollte der Cloud Anbieter vertraglich zusichern.
- Jederzeitiges Rückgaberecht auf die in der Cloud gespeicherten Daten bzw. Vernichtungspflicht: Der Cloud Nutzer sollte sich vertraglich ein jederzeitiges Rückgaberecht auf die in der Cloud gespeicherten Daten in einem gängigen Format zusichern lassen, ebenso die Vernichtung der Daten beim Cloud Anbieter.
- Haftung des Cloud Anbieters: Werden datenschutzrechtliche Vorgaben verletzt, haftet grundsätzlich dafür der Verantwortliche. Somit ist die Haftung des Cloud Anbieters entsprechend zu vertraglich zu regeln. In der DSGVO ist ein Rückgriffsrecht vorgesehen, falls der Auftragsverarbeiter seine auferlegten Pflichten verletzt oder eine Weisung des Verantwortlichen missachtet hat (Art. 82 Abs. 2 DSGVO).

- Geheimhaltung: Der Cloud Anbieter ist zur Geheimhaltung zu verpflichten.
- Konventionalstrafe: Für die Verletzung von vertraglichen Pflichten ist die Vereinbarung einer Konventionalstrafe denkbar, allerdings wird diese in der Praxis häufig vom Cloud Anbieter im Rahmen der Vertragsverhandlung nicht akzeptiert.
- Unterauftragsverhältnisse: Unterauftragsverhältnisse des Cloud Anbieters müssen vor Vertragsabschluss offengelegt werden. Nachträgliche Vereinbarungen dürfen nur mit Kenntnis und vorgängiger schriftlicher Zustimmung des Cloud Nutzers unterzeichnet werden. Insbesondere sind Unterauftragsnehmer zu verpflichten, Weisungen des Cloud Anbieters zu beachten.
- Organisatorische und technische Sicherheitsmassnahmen: Der Cloud Anbieter muss Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nachvollziehbarkeit sowie Portabilität und Interoperabilität sowie Mandantentrennung gewährleisten.

## VII. Fazit

[33] Die Auslagerung von Personendaten in die Wolke stellt datenschutzrechtlich eine Herausforderung dar. Ausgangspunkt der Nutzung von Cloud Computing Services sollte eine Risikoanalyse sein, welche die Anforderungen an den Cloud Anbieter und im Weiteren den Inhalt des schriftlich zu vereinbarenden Vertrages wesentlich bestimmt. Die Umsetzung der vertraglich festgehaltenen Massnahmen muss durch den Cloud Nutzer regelmässig kontrolliert werden, bleibt er als Verantwortlicher für die Einhaltung der anwendbaren Datenschutzgesetze verantwortlich und ist strafrechtlich belangbar. Trotzdem, Cloud Computing ist heutzutage Realität und nicht mehr wegzudenken. Daher müssen sich Cloud Nutzer, die Personendaten bearbeiten und, wie viele andere auch, Cloud Dienstleistungen nutzen, den Herausforderungen stellen. In der praktischen Umsetzung ist es dann aufgrund von vielen bereits bestehenden Standardverträgen und Hilfsmitteln überschaubar und keine Herkulesaufgabe.

---

David Schwaninger, Rechtsanwalt, LL.M. und Michelle Merz, Rechtsanwältin, sind beide bei Blum & Grob Rechtsanwälte AG in Zürich unter anderem im Datenschutz- und IT-Recht und den damit zusammenhängenden Rechtsgebieten tätig.

---

1 Aus Sicherheitsgründen wird oft ein sog. Virtual Private Network (VPN) genutzt.

2 Nach zurzeit in der Schweiz geltendem Recht gehören auch Angaben, welche sich auf eine bestimmte oder bestimmbare juristische Person beziehen, zu den Personendaten. Mit dem neuen Datenschutzgesetz und der europäischen Datenschutz-Grundverordnung (DSGVO) beschränkt sich der Schutzbereich auf natürliche Personen.

3 BGE 136 II 508, E. 3.2.

4 Hierzu und zum Folgenden: vgl. EDÖB, Erläuterungen zu Cloud Computing; Carmen De la Cruz, Cloud Computing: Alter Wein in neuen Schläuchen?, in: Jusletter IT 15. Mai 2013, N. 8 ff.

5 Dabei kann beispielsweise festgehalten werden, dass die Daten nur zur Vertragserfüllung bearbeitet werden dürfen.

6 BBl 1988 II 413, S. 463 f.

7 Vgl. hierzu den Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes vom 21. Mai 2015.

8 Insbesondere muss der Cloud Anbieter die Daten gegen folgende Risiken schützen: unbefugte oder zufällige Vernichtung und zufälligen Verlust, technische Fehler, Fälschung, Diebstahl, unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Datenbearbeitungen.

9 Geschäftsbetriebe werden gemäss Art. 64 rev-DSG generell nur subsidiär gebüsst.

10 Gemäss rev-DSG führt der Bundesrat diesbezüglich eine Länderliste.

11 Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller/Damian George, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, in: Anwaltsrevue 1/2019, Zürich 2019. S. 25 ff., S.

31; David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, N 67.

12 Vgl. hierzu Leitfaden des EDÖB zur Datenübermittlung ins Ausland kurz erklärt vom Dezember 2018.

13 Art. 6 Abs. 3 DSG bzw. Art. 16 Abs. 2 lit. b rev-DSG.

14 Urteil des EuGH C-311/18 vom 16. Juli 2020 – Facebook Ireland und Schrems.

15 In der DSGVO wird an Stelle des in der Schweiz etablierten Begriffes «Personendaten» der Terminus «personenbezogene Daten» verwendet.

16 Für einen guten Überblick über den Anwendungsbereich der DSGVO: David Roth, Cloud-basierte Dienstleistungen im Licht der DSGVO, in: Aktuelle Juristische Praxis, 2020, S. 68ff., S. 71 sowie David Vasella, Zum Anwendungsbereich der DSGVO, in: digma 2017, S. 220 ff.

17 Für weitere Hinweise: Lukas Bühlmann/Michael Reinle, Extraterritoriale Wirkung der DSGVO, in: digma 2017, S. 8 ff.

18 Vgl. hierzu auch: David Vasella, Auftragsbearbeitung im Privatbereich, in: Zeitschrift für Datenrecht und Informationssicherheit 2019, S. 110 ff., S. 114.

19 Vgl. Art. 4 des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021.

20 18 U.S.C. § 2713.

21 Vgl. hierzu: David Rosenthal, Mit Berufsgeheimnis in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020.

22 Urteil des BGer 2C_1083/2017 vom 4. Juni 2019.

23 Urteil des BGer 6B_1403/2017 vom 8. August 2017, E. 1.2.2.

24 Schwarzenegger/Thouvenin/Stiller/George (Fn. 11), S. 25 ff., S. 28.

25 Schwarzenegger/Thouvenin/Stiller/George (Fn. 11), S. 25 ff., S. 29; a.M. Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis, Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Zürich, 2016, S. 13.

26 David Rosenthal, Mit Berufsgeheimnis in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020, N 68, N 73.

27 BGE 145 II 229, E. 7.5.

28 Urteil des BGer 2C_1083/2017 vom 4. Juni 2019.

29 Walter Fellmann/Yvonne Burger, Unabhängigkeit und Berufsgeheimnis bei Subdelegation durch Hilfsperson – BGer 2C_1083/2017 vom 4. Juni 2019, in: Anwaltsrevue, 8/2019, S. 341 ff.; vgl. auch Rosenthal (Fn. 26) N 58 ff.

30 Schweizerische Bankiervereinigung, Cloud-Leitfaden, Wegweiser für sicheres Cloud Banking, März 2019, S. 8.

31 Christian Laux/Alexander Hofmann/Mark Schieweck/Jürg Hess, Rechtsgutachten zur Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG, 14. Februar 2019, N 27, publiziert in: Jusletter 27. Mai 2019.

32 Laux/Hofmann/Schieweck/Hess (Fn. 31), N 39; Michael Isler/Oliver M. Kunz/Thomas Müller/Jürg Schneider/David Vasella, Rechtsgutachten zur Zulässigkeit der Bekanntgabe von Bankkundendaten durch schweizerische Banken an Beauftragte im Ausland unter Art. 47 BankG, 15. Februar 2019, N 5 ff.

33 Isler/Kunz/Müller/Schneider/Vasella (Fn. 32), N 7.

34 Bruno Pasquier/Aurélien Pasquier, Daten im Konkurs – Vertragsforderungen den Daten und Verwertung, in: Aktuelle Juristische Praxis 2019, S. 1316 ff., S. 1319.

35 Pasquier/Pasquier (Fn. 34), S. 1316 ff., S. 1320.

36 Martin Eckert, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 112/2016, S. 245 ff., S. 249.

37 Alain Schmid/Kirsten Johanna Schmidt/Herbert Zech, Rechte an Daten – zum Stand der Diskussion, in: Sic! 11/2018, S. 627 ff., S. 629 m.w.H.

38 Anders würde es sich im Fall verhalten, bei dem die Daten auf einem Medium gespeichert sind, das sich zwar beim konkursiten Cloud Anbieter befindet, aber im Eigentum des Nutzers steht. Problematisch ist dann aber, dass die Aussonderung des betreffenden Mediums Zeit in Anspruch nimmt.

39 Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register (BBl 2020 7801, 7806).

40 Der Cloud Nutzer begibt sich in eine gewisse Abhängigkeit zum Cloud Anbieter. Das Szenario des Ausfalls einer Cloud oder einer Zugangsbeschränkung ist daher zu berücksichtigen. Mit dem Cloud Anbieter sollten Lösungen vereinbart werden, welche solche Risiken entschärfen.

41 Bei der Pseudonymisierung ist besonders sicherzustellen, dass die betroffenen Personen nicht mehr bestimmbar sind.

42 Vgl. hierzu Fussnote 6.

43 Die entsprechende Verordnung zum rev-DSG, die sog. VDSG, wird ab Mitte Juni 2021 in die Vernehmlassung gehen. Es ist zu erwarten, dass die neue VDSG Präzisierungen zur Datensicherheit bzw. zu den technischen Massnahmen beinhalten wird.

44 Weitere Hinweise dazu: De la Cruz (Fn. 4), N 16 ff.

45 Das Recht auf Vergessen (Art. 30 Abs. 2 lit. b und Abs. 3 rev-DSG) gilt nicht absolut, sondern ist durch die Rechtfertigungsgründe von Art. 31 rev-DSG beschränkt.

46 Für Unternehmen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt, sollen gemäss Art. 12 Abs. 5 rev-DSG auf Verordnungsstufe Ausnahmen vorgesehen werden.

## *0* Kommentare

### Es gibt noch keine Kommentare

** Pflichtfelder*

## Was ist Ihr Kommentar?

Titel:

Ihr Kommentar: *

Name: *

Eliane Locher

Senden

Ihr Kommentar wird durch eine Moderatorin bzw. einen Moderator geprüft und in Kürze freigeschaltet.