EuroCloud Deutschland_eco e.V.

Leitfaden

Cloud Computing
Recht, Datenschutz & Compliance

1. Impressum

EuroCloud Deutschland_eco e. V.
Lichtstraße 43h
50825 Köln

Tel.: 0221 / 70 00 48 – 0
Fax: 0221 / 70 00 48 – 111
E-Mail: info@eurocloud.de
Web: www.eurocloud.de

Vorstand: *Bernd Becker (Vorsitzender)*
Thomas von Bülow (stv. Vorsitzender)
Oliver J. Süme

Vereinsregister: Amtsgericht Köln – VR 16215
Sitz des Vereins: Köln

2. Inhalt

2. Vorwort

Liebe Leser,

Innovationen sind der Motor der Wirtschaft, eine verlässliche Innovationsumsetzung gleichsam der Treibstoff des wirtschaftlichen Erfolges.

Cloud Computing ist ohne Frage ein Megatrend, der Kunden und Anbietern eine Vielzahl innovativer Vorteile erschließt und so zu einer völlig neuen Art der IT-Nutzung führen wird.

Die mit der Markteinführung neuer und innovativer Lösungen oftmals verbundenen Unsicherheiten bei Anbietern und Anwendern gelten in besonderem Maße auch für Services aus der Cloud.

Gerade für mittelständische Unternehmen ist Cloud Computing eine höchst attraktive Möglichkeit, die Wettbewerbsfähigkeit durch Einbindung von externen Serviceangeboten zu erhalten und auszubauen.

Jedoch verfügen gerade diese Unternehmen oftmals nicht über ausreichende Möglichkeiten einer individuellen Prüfung potentieller rechtlicher Implikationen. Die Frage, wie Cloud-Computing-Verträge vor dem Hintergrund der rechtlichen Ausgestaltung und unter Berücksichtigung datenschutzrechtlicher Aspekte zu gestalten sind, stellt Anbieter wie Anwender vor besondere Herausforderungen. Erst recht, wenn der gebotene Cloud Service grenzüberschreitend bereitgestellt oder genutzt werden soll.

Die mit dem Internet verbundenen, oft und grundsätzlich diskutierten Sicherheitsproblematiken gelten gleichermaßen auch für die Cloud und werden im Zweifelsfall durch die Cloud noch verstärkt. Technologische Voraussetzungen für eine sichere Servicebereitstellung sind durchaus gegeben, doch sind die Anbieter durch die teilweise in Europa geltenden, nicht immer eindeutigen rechtlichen Rahmenbedingungen verunsichert.

Insofern stellen die mit Cloud Computing verbundenen, gravierenden und dynamischen Marktveränderungen auch die Politik vor besondere Aufgaben. Es gilt, den nationalen und europäischen Rechtsrahmen auf eine globale Servicebereitstellung aus der Cloud zu überprüfen und ggf. anzupassen.

Mit Start der EuroCloud Deutschland_eco e.V. im Februar 2010 wurde die Arbeitsgruppe Recht ins Leben gerufen, um die zum Teil komplexen rechtlichen Aspekte bei Cloud Computing aufzubereiten. Ziel war es, Anwendern und Anbietern von Cloud Services zu den Themenfeldern Recht, Datenschutz und Compliance Orientierung und Unterstützung zu geben. Die Ergebnisse dieser Arbeit sind nunmehr eingeflossen in den hier vorliegenden Leitfaden „Cloud Computing: Recht, Datenschutz & Compliance".

Die fachliche Expertise, die diesem Leitfaden zugrunde liegt, ist auch Teil der neutralen, unabhängigen Zertifizierung „Eurocloud Star Audit Software as a Service", welche ab Anfang 2011 von Eurocloud Deutschland_eco e.V. am Markt angeboten wird.

Wir danken den Cloud- und Rechtsexperten für die inhaltliche Aufbereitung und dem Team von eco – Verband der deutschen Internetwirtschaft, das sich der vielen organisatorischen Aufgaben angenommen hat.

Köln, November 2010

Bernd Becker
Vorstandsvorsitzender EuroCloud Deutschland_eco e.V.
Vizepräsident EuroCloud Europe

3. Einleitung

Beim Cloud Computing stehen Sicherheit und Compliance als wichtigste Themen an erster Stelle. Mit dem Leitfaden Recht, Datenschutz & Compliance bekommen sowohl Anbieter als auch Anwender eine Richtlinie an die Hand, die bei der sicheren Vertragsgestaltung und der Auswahl des richtigen Dienstleisters hilft.

Der Leitfaden bildet die Grundlage für die richtige Einordnung der rechtlichen Bestimmungen. Dabei konzentriert er sich auf den Bereich „Software as a Service“ als „Public Cloud“-Dienst und erörtert die besonderen Anforderungen hinsichtlich des Datenschutzes und die – je nach Anwendungszweck – erweiterten Vorgaben im steuerrechtlichen und betrieblichen Bereich.

Die Themenübersicht ist abgeleitet aus den Prüfkriterien des EuroCloud SaaS-Gütesiegels, das „Software as a Service“-Angebote in Bezug auf Serviceerbringung, Datensicherheit, Datenschutz, Vertragsgestaltung und Interoperabilität untersucht.

Der Verband EuroCloud Deutschland_eco e.V. vertritt seit 2009 die deutsche Cloud-Computing-Industrie als nationale Organisation des europäischen EuroCloud-Netzwerkes. Die Verbindung zu eco – Verband der deutschen Internetwirtschaft, der über 15 Jahre Erfahrung in der Internet-Branche verfügt, ergänzt die Arbeit zu Cloud-Computing-Themen ideal. Cloud Computing ist ein globales Thema und hat einen wichtigen Status in der Planung zukünftiger IT-Strategien erhalten.

EuroCloud hat mit der Initiative SaaS-Gütesiegel und der grundlegenden Aufbereitung des rechtlichen Hintergrunds (Outsourcing von IT Dienstleistungen und Auftragsdatenverarbeitung) wichtige Projekte gestartet, um die Rahmenbedingungen für einen erfolgreichen Einsatz von Cloud-Diensten aus den verschiedenen Bereichen (Software, Plattform und Infrastruktur) zu verbessern.

4. Rechtliche Anforderungen

Ein Schwerpunkt unter dem Aspekt „Recht, Datenschutz und Compliance“ bei Cloud Computing ist der Datenschutz. Der Leitfaden befasst sich mit den Besonderheiten, die sich bei der Nutzung von Cloud Computing unter dem Gesichtspunkt der vertraglichen Vereinbarungen zwischen Nutzer und Anbieter ergeben.

Die datenschutzrechtlichen Vorgaben werden stets dann relevant, wenn personenbezogene Daten – z. B. Kundendaten oder Mitarbeiterdaten – betroffen sind. Zu beachten ist, dass der Begriff der „personenbezogenen Daten“ im Sinne des Bundesdatenschutzgesetzes (BDSG) sehr weit gefasst ist. Alle Daten, die einen Personenbezug haben oder bei denen der Anbieter, der Nutzer oder ein Dritter einen Personenbezug herstellen könnte, gelten aus Sicht der Datenschutzbehörden als „personenbezogene Daten“. In der Praxis wird es nur sehr wenige Cloud-Anwendungen geben, bei denen Daten verarbeitet werden, die nicht zumindest teilweise personenbezogen sind.

Die zivilrechtlichen Vertragsbestandteile über die zu erbringenden SaaS-Leistungen und Service Levels sowie die zivilrechtlich flankierenden Regelungen über insbesondere die Haftung und Kündigung sind nicht Gegenstand der folgenden datenschutzrechtlichen Ausführungen.

Im Folgenden werden Hinweise zur Umsetzung der Anforderungen des Datenschutzes (§ 11 BDSG) bei Verträgen zwischen Anbietern von SaaS bzw. Cloud Computing und deren Kunden gegeben. Der Leitfaden konzentriert sich auf die Darstellung spezifischer Datenschutzprobleme des Cloud Computings und zeigt, wie Fragen der Auftragsdatenverarbeitung Cloud-spezifisch geregelt werden können. Die Darstellung ist im Folgenden am Aufbau eines Vertrages bzw. der datenschutzrechtlichen Bestimmungen in einem Vertrag für ein Cloud-spezisches Angebot angelehnt.

» Verantwortlich für die rechtmäßige Datenverarbeitung ist auch beim Cloud Computing der Nutzer, also der Auftraggeber (§ 11 BDSG)

» Auch für einen reinen Test einer Cloud-Computing-Anwendung muss bereits ein Vertrag mit dem Anbieter abgeschlossen werden, wenn „Realdaten“ verarbeitet werden

Vorab ist Folgendes zu beachten:

- Der Nutzer bleibt auch bei der Nutzung von Cloud Computing im Rahmen des § 11 BDSG für die Rechtmäßigkeit der Datenverarbeitung im Rahmen der Nutzung des Dienstes verantwortlich. Er darf also auch mittels des Dienstes nur solche datenschutzrelevanten Verarbeitungen vornehmen lassen, die er auch selbst vornehmen dürfte.

- Der Abschluss eines Vertrags über die Auftragsdatenverarbeitung als datenschutzrechtliche Grundlage ist auch dann erforderlich, wenn der Einsatz der Cloud-Computing-Anwendung nur getestet werden soll. Um den Aufwand für den Abschluss eines solchen Vertrags zu vermeiden, bietet es sich an, Testzugänge ohne „Realdaten“ zu nutzen.

5. Kernpunkte zur Auswahl des Cloud-Anbieters

Der Auftraggeber (Nutzer) hat den Auftragnehmer (Anbieter) sorgfältig auszuwählen und sich auch vor Beginn der Datenverarbeitung (und sodann regelmäßig) von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

In der Praxis bedeutet dies, dass der Nutzer sich von der Eignung des Anbieters vor dem Vertragsschluss „ein Bild machen“ muss, um seiner gesetzlichen Pflicht zur sorgfältigen Auswahl des Anbieters Rechnung zu tragen. Bereits diese Auswahl ist für den Nutzer erleichtert, wenn der Anbieter Standards eines Gütesiegels erfüllt oder über eine entsprechende Reputation verfügt.

» *Der Auftraggeber ist gesetzlich verpflichtet, den Anbieter sorgfältig auszuwählen*

» *Nach Vertragsschluss muss der Auftraggeber regelmäßig prüfen, ob der Anbieter die erforderlichen technischen und organisatorischen Maßnahmen einhält*

6. Kernpunkte eines Vertrages aus datenschutzrechtlicher Sicht

6.1 Form

» Der Vertrag bedarf der Schriftform, ein Online-Abschluss mit qualifizierter elektronischer Signatur ist möglich

Der Vertrag bedarf für seine Wirksamkeit der sog. Schriftform. Für die Praxis bedeutet dies, dass entweder eine Vertragsurkunde handschriftlich durch den Nutzer und den Anbieter unterzeichnet wird oder qualifizierte elektronische Signaturen genutzt werden müssen.

Mögliches Vorgehen bei Online-Vertragsschluss, wenn dieser nicht den Anforderungen einer qualifizierten elektronischen Signatur genügt: Der Kunde erhält auf Anfrage vom Anbieter unverzüglich ein schriftliches Vertragsangebot, welches von einer vertretungsberechtigten Person des Anbieters unterschrieben ist und inhaltsgleich mit den online geschlossenen Vertragsbedingungen ist. Hierbei kann klargestellt werden, dass die Rechte und Pflichten (z. B. zur Zahlung des Entgelts) aus dem Vertrag bestehen auch ohne schriftlichen Vertrag.

6.2 Gegenstand des Auftrags

» Sind personenbezogene Daten betroffen, muss bei der Beschreibung der Auftrag spezifiziert werden: Hosting, Betrieb, Migration von Daten?

Der Gegenstand der erbrachten Leistung ist grob zu umschreiben. Soweit der Umgang mit personenbezogenen Daten betroffen ist, bedarf es detaillierter Beschreibungen (z. B. Hosting, Betrieb, Pflege und Zurverfügungstellung zum Online-Abruf einer bezeichneten Anwendung, Migration von Daten). Bei Parametrisierungen und kundenspezifischer Anpassung (Customizing) ist danach zu unterscheiden, ob dies vor dem „Einspielen“ der Daten oder danach erfolgt.

» Customizing: Erfolgt dies vor oder nach der Übertragung personenbezogener Daten?

Die gesetzliche Pflicht zur Festlegung des Gegenstands der Verarbeitung (§ 11 Abs. 2 S. 2 Nr. 1 BDSG) fällt in der Praxis der Gestaltung des Vertrags mit der Pflicht zusammen, den Umfang, die Art und den Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und den Kreis der Betroffenen festzulegen (§ 11 Abs. 2 S. 2 Nr. 1 BDSG).

» Werden personenbezogenen Daten verarbeitet? Wenn ja, wie?

Es kann auf deren Funktionsbeschreibung oder die Datenschutzhinweise des Anbieters verwiesen werden, sofern sich aus diesen Dokumenten ergibt, welche Daten im Rahmen der Anwendung auf welche Weise erhoben, verarbeitet und genutzt werden. Vorzugswürdig ist eine individuelle Beschreibung des Dienstes in Bezug auf den Umgang personenbezogener Daten, wobei dies bei Cloud-Angeboten oft wenig pragmatisch ist. Ein bloßer Verweis auf die bestehende und eventuell durch den Kunden getestete Anwendung oder auf Online-Benutzerhandbücher genügt hingegen nicht, da

diese einseitig vom Anbieter geändert werden können; dies gilt jedenfalls, sofern nicht ein Versionsstand explizit festgelegt und dokumentiert wird.

Auf folgende Aspekte sollte in jedem Fall näher eingegangen werden:

- Klarstellung, ob und gegebenenfalls in welcher Weise „besondere Arten personenbezogener Daten“ im Sinne des § 3 Abs. 9 BDSG erhoben und/oder verwendet werden. Solche besonderen Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Wenn solche Daten verarbeitet werden, ist fallspezifischer datenschutzrechtlicher Rat einzuholen.

- Erläuterung, welche Dritte Zugriff auf die Daten haben können (über Schnittstellen, als Wartungsunternehmen, Subunternehmer etc.).

» Welche Dritte haben darauf Zugriff?

» Hinweis, dass Daten jederzeit auf Wunsch des Auftraggebers genutzt werden können

6.3 Auslandssachverhalte (einschließlich eingesetzter ausländischer Ressourcen und Subunternehmer)

Das Bundesdatenschutzgesetz privilegiert Auftragsdatenverarbeitungsverhältnisse, indem es die Datenverarbeitung des Auftragnehmers dem Auftraggeber zurechnet und keine Erlaubnisnorm mehr für die Übermittlung an den Auftragnehmer fordert. Diese privilegierende Wirkung greift ohne weiteres jedoch nur bei einem Auftragnehmer, der seinen Sitz in der EU oder dem Europäischen Wirtschaftraum (EWR) hat (§ 3 Abs. 8 S. 3 BDSG). Bei einer Beauftragung von Nutzern mit Sitz in einem Drittstaat – also außerhalb der EU und/oder des EWR – oder einer tatsächlichen Datenverarbeitung in einem solchen Drittstaat müssen zusätzliche Anforderungen erfüllt werden, damit eine Übertragung von Daten in einen solchen Drittstaat erfolgen darf.

» Ohne weiteres ist Auftragsdatenverarbeitung nur mit Auftragnehmern mit Sitz in der EU oder im EWR möglich

Die nahe liegende Gestaltung ist, auf den von der Europäischen Union abgesegneten Standardvertrag zur „Auftragsdatenverarbeitung“ zurückzugreifen (sogenannte „Standard Contract Clauses“ für „Data Processing“). Dieser Vertrag hat zwar nicht dieselbe Wirkung wie eine Auftragsdatenverarbeitung im Sinne des BDSG, sie führt aber zu einer weitgehenden Gleichberechtigung der Datenübertragung in den Drittstaat mit einer Datenübertragung innerhalb der EU und/oder des EWR.

» Bei Auftragnehmern in Drittländern müssen ergänzend besondere vertragliche Regelungen getroffen werden

Allerdings fordern deutsche Datenschutzaufsichtsbehörden eine Ergänzung dieses Standardvertrags um Vorgaben aus dem deutschen § 11 Abs. 2 BDSG. Dies ist problematisch, weil Veränderungen des EU-Standardvertrags aus Sicht der EU zum Verlust der oben beschriebenen Wirkung der Gleichstellung mit Datenübertragungen innerhalb der EU und/oder des EWR führen. Die Umsetzung der Vorgaben der deutschen Datenschutzaufsichtsbehörden muss daher so erfolgen, dass diese Vorgaben zusätzlich aufgenommen werden, ohne dabei – direkt oder indirekt – Regelungen des Standardvertrags einzuschränken. Auf diese Weise wird man allen Anforderungen gerecht.

6.4 Verantwortlichkeit

» Die datenschutzrechtlichen Verantwortlichkeiten müssen im Vertrag klar geregelt sein

Im Interesse des Anbieters sollten die grundsätzlichen datenschutzrechtlichen Verantwortlichkeiten (der Anbieter ist nur Auftragnehmer, der Nutzer ist als Auftraggeber hauptverantwortlich wie bei Datenverarbeitung im eigenen Unternehmen) im Vertrag klarstellend geregelt und der Nutzer dazu verpflichtet werden, nur datenschutz-konforme Nutzungen vorzunehmen.

Im Interesse des Nutzers sollte vertraglich klargestellt werden, dass allein ihm die Außenkommunikation – auch bei Datenschutzpannen – obliegt, der Anbieter ihn aber unverzüglich über jeden Datenschutz- und / oder Sicherheitsverstoß – bzw. über den Verdacht von solchen – umfassend zu informieren hat.

Der Anbieter sollte den Nutzer dazu anhalten, dass dieser im Außenverhältnis zu den Betroffenen deutlich kommuniziert, dass allein der Nutzer für die Ansprüche der Betroffenen – insbesondere auf Auskunft, Berichtigung und Löschung – der Verantwortliche ist.

Nach § 11 Abs. 3 S. 2 BDSG ist der Anbieter verpflichtet, den Nutzer unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung des Kunden gegen Vorschriften über den Datenschutz verstößt. Diese Regelung wird in der Praxis von Cloud-Anwendungen kaum eine Rolle spielen. Denn der Anbieter stellt dem Nutzer eine standardisierte Anwendung bereit und wird kaum spezielle Weisungen des Kunden an den Anbieter zum Umgang mit personenbezogenen Daten erhalten.

Dennoch ist es sinnvoll, im Vertrag klarzustellen, dass der Anbieter gegebenenfalls auf einen solchen Verstoß hinweist, er allerdings keine rechtliche Prüfung vornimmt und im Zweifel die Anweisung des Nutzers dennoch auszuführen hat. Erkennbar strafbare Weisungen darf der Anbieter aber in keinem Fall ausführen.

6.5 Kontrollrechte des Nutzers

Der Nutzer muss sich gegenüber dem Anbieter Kontrollrechte einräumen lassen.

» Der Auftraggeber muss sich gegenüber dem Auftragnehmer Kontrollrechte einräumen

Das bedeutet, dass der Nutzer berechtigt sein muss, die Datenverarbeitung einschließlich der Schutzmaßnahmen beim Anbieter – auch vor Ort – kontrollieren zu dürfen oder durch Dritte kontrollieren zu lassen. Das muss sich auf alle Orte beziehen, an denen die Daten verarbeitet werden. Gerade bei vielen verschiedenen und/oder weit entfernten Orten bietet sich eine Kontrolle durch Dritte, etwa im Rahmen zertifizierter, gegebenfalls standardisierter Audits an. Allerdings fordern die Datenschutzbehörden (zumindest derzeit) wohl, dass der Nutzer zumindest das Recht hat, selbst die Kontrollen individuell vorzunehmen. Entsprechendes sollte daher im Vertrag auch geregelt werden.

Der Nutzer sollte neben diesem Kontrollrecht vor Ort auch die Pflicht des Anbieters regeln, dass der Anbieter die für eine Kontrolle erforderlichen Informationen bereitstellt und anderweitig angemessen mitwirkt. Die Kontrollen können für den Regelfall auf die Geschäftszeiten und auf eine Voranmeldung beschränkt werden. Typischerweise wird eine angemessene Kontrolle ohnehin nur unter diesen Voraussetzungen tatsächlich möglich sein.

Darüber hinaus sollten – soweit einschlägig – auch die Kontrollen durch Aufsichtsbehörden vertraglich geregelt werden.

Da es sich hierbei um eine gesetzliche Pflicht zur Ausgestaltung einer Auftragsdatenverarbeitung handelt, ist es auch für Anbieter nicht sinnvoll, sich diesen Regelungen zu verschließen. Sie sollten vielmehr den Nutzern geeignete Standardverfahren anbieten. Das Gesetz fordert allerdings nicht, dass diese Unterstützung entgeltfrei erfolgen muss. Ein sinnvoller Interessensausgleich könnte darin bestehen, ab einem gewissen Aufwand eine Kostentragung des Nutzers zu regeln.

6.6 Technisch-organisatorische Maßnahmen

» Technisch-organisatorische Maßnahmen zum Schutz der personenbezogenen Daten müssen vertraglich und konkret geregelt sein

Gesetzliche Anforderung an den Inhalt eines Vertrags über die Auftragsdatenverarbeitung ist die Regelung technisch-organisatorischer Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten. In der Anlage zu § 9 BDSG sind Vorgaben enthalten, welche Aspekte geregelt sein müssen.

Es muss also ein konkretes, den tatsächlichen Gegebenheiten entsprechendes Sicherheitskonzept vertraglich als Leistungspflicht des Anbieters festgelegt werden. Abstrakte oder pauschale Beschreibungen genügen dieser Vorgabe nicht, sondern müssen so konkret sein, dass klar ist, welche Maßnahmen ergriffen sind. Diese Maßnahmen müssen ein angemessenes Schutzniveau sicherstellen, sodass es für die Bewertung der Schutzmaßnahme auf die verarbeiteten personenbezogenen Daten ankommt.

In der Praxis bietet es sich an, dass der Anbieter ein Sicherheitskonzept für seine Dienstleistung erstellt, das durch den Nutzer geprüft und dann als vertragliche Anforderung festgelegt wird. Dabei ist allerdings klar, dass bei standardisierten SaaS- oder Cloud-Angeboten eine Prüfung durch den Nutzer nicht bedeuten kann, dass auf individuelle Wünsche des Nutzers eingegangen werden kann. Der Nutzer ist aber dazu verpflichtet, zu überprüfen, ob das Sicherheitskonzept den datenschutzrechtlichen Anforderungen genügt und der Sensibilität der involvierten Daten gerecht wird, bevor er die Daten auslagert.

Das Sicherheitskonzept muss entsprechend der technischen Entwicklung dynamisch angepasst werden, um das Schutzniveau aufrecht zu erhalten.

Zur Einhaltung dieses Schutzes sind sowohl der Nutzer als auch der Anbieter jeweils für sich gesetzlich verpflichtet.

Von den beim Anbieter getroffenen technisch-organisatorischen Maßnahmen im Sinne des BDSG – also den Maßnahmen zur Sicherheit der Daten – muss sich der Nutzer vor Beginn der Verarbeitung der Daten beim Anbieter überzeugen. Im Interesse beider Parteien kann dies nach dem Vertragsschluss – also der finalen Auswahl – erfolgen, solange sich der Nutzer vor Beginn der tatsächlichen Datenverarbeitung die Überzeugung verschafft hat. In der praktischen Konsequenz bedeutet das, dass die erforderlichen Maßnahmen selbstverständlich bei Vertragsschluss geklärt worden sein müssen.

Eine Überzeugungsbildung muss nicht zwingend vor Ort beim Anbieter erfolgen. Diese kann auch durch Vorlage entsprechender Testate, Zertifikate oder Erklärungen des Anbieters erfolgen. Je schutzbedürftiger die Daten aus der Sicht der Betroffenen – also derjenigen, auf die sich diese Daten beziehen – sind, umso gründlicher muss die Überzeugungsbildung erfolgen.

Diese Überzeugungsbildung muss nach der initialen Überprüfung regelmäßig wiederholt werden. Das sollte so auch im Vertrag vorgesehen werden. Eine konkrete Vorgabe zum Turnus ist dem Gesetz nicht zu entnehmen. Der Turnus ist daher nach der Schutzbedürftigkeit der Daten aus der Sicht der Betroffenen – also derjenigen, auf die sich diese Daten beziehen – zu bewerten. In jedem Fall muss eine erneute Überprüfung dann erfolgen, wenn Zweifel an der Einhaltung der Sicherheitsmaßnahmen durch den Dienstleister auftreten.

Über die Prüfung hinaus ist aus gesetzlicher Sicht die Dokumentation dieser Überzeugungsbildung entscheidend. Das Ergebnis der jeweiligen Prüfung hat der Nutzer zu dokumentieren. Es muss also festgehalten sein, dass und mit welchem Ergebnis die Überzeugungsbildung stattgefunden hat.

Das Bundesamt für Sicherheit in der Informationstechnik hat – mit Stand vom 27.09.2010 – den Entwurf „BSI-Mindestanforderungen an Cloud-Computing[1]“ veröffentlicht. Mit der Finalfassung wird sich eine Handreichung ergeben. Zu beachten ist allerdings, dass diese nicht wie eine Rechtsverordnung kraft Gesetzes zu beachten ist. Sie wird allerdings indirekt über die „ausfüllungsbedürftige“ Beschreibung des § 9 BDSG als Mindeststandard rechtlich relevant werden. Die Entwicklung ist daher genau zu beobachten.

6.7 Einschaltung von Subunternehmern und deren Kontrolle

Das BDSG fordert, dass im Vertrag über die Auftragsdatenverarbeitung „die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen“ zu regeln ist. Von einem Unterauftragnehmer (Subunternehmer) sollte ausgegangen werden, wenn der Zugriff des Subunternehmers auf die für den Nutzer verarbeiteten Daten nicht ausgeschlossen werden kann. Eine Übermittlung an den Subunternehmer ist nicht erforderlich. Zugriff etwa in Form des Remote-Einpflegens von Daten oder der Fernwartung ist ausreichend. Ferner kommt es nicht darauf an, ob der Subunternehmer die Daten verarbeiten soll, sondern ob er tatsächlich darauf zugreifen kann.

[1] siehe „10.2 Cloud Computing und Compliance“ auf Seite 30

» Die mögliche Beauftragung von Subunternehmen muss vertraglich geregelt sein

Das Gesetz fordert damit nach seinem Wortlaut nur eine Regelung über das „Ob“ der Zulässigkeit von Subunternehmern. Eine solch schlichte Regelung wird den datenschutzrechtlichen Bedürfnissen des Nutzers kaum gerecht und wird daher von den Datenschutzbehörden auch nicht so eng verstanden.

Als praxistaugliche Regelung, die sowohl den Interessen des Auftragnehmers als auch des Auftraggebers dient, kann sich eine Gestaltung erweisen, die zwischen Kategorien von Subunternehmern differenziert. Damit können bestimmte Kategorien unter einen Zustimmungsvorbehalt des Auftraggebers gestellt werden, während in anderen Kategorien die Einschaltung von Subunternehmern ohne gesonderte Einwilligung zulässig ist, sofern bestimmte definierte Anforderungen eingehalten sind. In jedem Fall sollte der Auftraggeber über die Subunternehmer und deren Tätigkeit informiert werden.

Die Informationspflicht kann vereinfacht werden, indem der Anbieter online eine zugangsgeschützte Liste von Subunternehmern führt, die der Kunde einsehen kann und über deren Änderungen der Kunde per E-Mail informiert wird. Die Liste enthält Name und Anschrift des Subunternehmers und eine Kurzbeschreibung der erbrachten Dienstleistung. Auf Verlangen des Kunden legt der Anbieter die datenschutzrelevanten Vertragsbedingungen des Subunternehmervertrages offen.

Die Beauftragung von Subunternehmern ist nur zulässig, sofern durch Subunternehmer dasselbe Schutzniveau in Bezug auf die personenbezogenen Daten sichergestellt ist, wie sie der Vertrag zwischen Nutzer und Anbieter für den Anbieter vorgibt. Die Verträge des Anbieters mit Subunternehmern müssen also das gleiche Schutzniveau sicherstellen wie der Vertrag mit dem Kunden, insbesondere hinsichtlich technischer und organisatorischer Sicherheitsmaßnahmen. Der Anbieter sollte dies auch aus Eigeninteresse sicherstellen, um nicht in eine Schere zwischen seinen „hohen“ Pflichten gegenüber dem Nutzer und nur niedrigen Pflichten seines Subunternehmers zu geraten.

Der Nutzer muss sich beim Zulassen von Subunternehmern bewusst sein, dass er im Außenverhältnis für diese genauso haftet wie für den Anbieter als seinen Hauptauftragnehmer.

Der Nutzer muss durch vertragliche Vorgaben sicherstellen, dass er gegenüber den Subunternehmern dieselben, eigenen Kontollrechte hat wie gegenüber dem Anbieter.

6.8 Laufzeit und Rückgabe von Daten

» Der Vertrag muss Angaben zu Laufzeit und Rückgabe der Daten beinhalten

Die Laufzeit des Vertrages ist ebenfalls zwingend zu regeln. Hierbei ergeben sich aber keine Besonderheiten gegenüber sonstigen Auftragsdatenverarbeitungen. Insbesondere muss keine fixe Laufzeit vorgegeben werden, sondern die Verträge können auch auf unbestimmte Zeit mit der Möglichkeit zur ordentlichen Kündigung geschlossen werden.

Unterstützt der Anbieter den Kunden bei der Migration von Daten, gehören die Zeiten der Migration ebenfalls zur Laufzeit der Auftragsdatenverarbeitung.

Die „Rückgabe" der personenbezogenen Daten bei Vertragsbeendigung muss aufgrund der gesetzlichen Vorgabe in § 11 Abs. 2 S. 2 Nr. 10 BDSG ebenfalls geregelt werden.

Die zwei Grundszenarien sind die Rückübertragung der Daten plus Löschung in den Systemen des Anbieters oder die bloße Löschung der Daten in den Systemen des Anbieters. Ein Grundszenario muss ohne zusätzliches Entgelt in dem Vertrag vorgesehen sein. Auch wenn der Vertrag beendet ist, sollte die Auftragsdatenverarbeitung so ausgestaltet sein, dass die Pflichten aus der Auftragsdatenverarbeitung bis zur eindeutigen Bestätigung der Löschung durch den Anbieter fortgelten.

Der Nutzer sollte sich bereits bei Vertragsschluss entscheiden, welche Anforderungen an die Rückgabe – Übertragungsweg (z. B. per sftp) und in welchem Dateiformat oder ob Erläuterungen zur Dateistruktur erforderlich werden – zu stellen sind, damit er zu einem anderen Anbieter wechseln oder die Aufgabe wieder selbst wahrnehmen kann.

Für den Anbieter ist neben dem vorgenannten kostenrelevanten Aspekt auch entscheidend, wann er die Daten löschen kann, falls der Nutzer die Vergütung nicht (mehr) zahlt oder insolvent wird.

7. Produkt- und branchenspezifische Besonderheiten

Besondere Anforderungen können sich in bestimmten Fallkonstellationen ergeben, wie etwa bei Kunden

- aus dem Finanzdienstleistungssektor (§ 25 a KWG, GoBS, § 20 ZAG)
- aus dem Telekommunikationsbereich (TKG)
- als Träger von Berufsgeheimnissen (§ 203 StGB: Ärzte, Anwälte, Lebens-, Kranken- oder Unfallversicherer)
- mit Anwendungen steuerrelevanter Daten (§§ 146, 147 AO, GDPdU, § 41 EstG)

7.1 Finanzdienstleistungen

Der Finanzsektor weist Besonderheiten auf, die an dieser Stelle kurz angerissen werden, aber nicht abschließend besprochen werden können: § 25 a Abs. 1 KWG enthält allgemeine Pflichten von Kreditinstituten zu einer ordnungsgemäßen Geschäftsorganisation. § 25 a Abs. 2 KWG konkretisiert diese Pflichten für den Fall einer Auslagerung von Aktivitäten und Prozessen auf ein anderes Unternehmen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind.

Für Finanzinstitute im Bereich Wertpapiere, Fonds und Versicherungen gelten nach § 33 WpHG, § 16 InvG und § 64 a VAG vergleichbare Regelungen.

Daher muss jeweils im Einzelfall geprüft werden, ob die in die Cloud transferierten Aufgaben und Prozesse „wesentlich“ nach § 25 a Abs. 2 KWG sind und ob sie vom Begriff der „Auslagerung“ erfasst sind. Dann müssen – ebenfalls gemäß § 25 a Abs. 2 KWG – für die Auslagerung angemessene Vorkehrungen zum Datenschutz und zur Vermeidung übermäßiger zusätzlicher Risiken getroffen werden (beispielsweise die sorgfältige Auswahl des Cloud-Anbieters, die Überwachung der Dienstleistung, die Festlegung von Methoden zur Bewertung der Leistung sowie die Vereinbarung einer Notfallplanung).

7.2 Telekommunikationsgesetz

Die Möglichkeit der Nutzung von Cloud Services sind aus der Sicht der Datenschutzaufsichtsbehörde in der Telekommunikationsbranche noch weiter beschränkt. §§ 95 ff. TKG liegt das Prinzip zugrunde, dass eine Übermittlung personenbezogener Daten – Bestands- und Verkehrsdaten – an Dritte nur mit Einwilligung des Betroffenen zulässig ist. Eine Einwilligung des Betroffenen wird nicht in Betracht kommen. Als Alternative verbleibt damit die Gestaltung als Auftragsdatenverarbeitung (§ 11 BDSG). Diese ist jedoch nach § 3 Abs. 8 S. 3 BDSG auf die EU und den EWR beschränkt. Eine Überschreitung dieser Grenzen ist im Rahmen von Cloud Services problematisch. Hinzu kommt, dass argumentiert werden könnte, dass § 92 TKG eine weitere Grenze zieht, in dem er die Bereiche einer zulässigen Auftragsdatenverarbeitung nach § 11 BDSG auf die Bereiche Erbringen von Telekommunikationsdiensten, die Erstellung und Versendung von Rechnungen sowie die Missbrauchsbekämpfung beschränkt. Ob § 92 TKG eine solche Begrenzung tatsächlich enthält oder für diese Bereiche nur die Geltung des § 11 BDSG klarstellen soll, ist rechtlich umstritten.

7.3 Steuerrechtliche Buchführungspflicht

Bei einer Verwendung steuerrechtlich relevanter Daten durch Cloud-Anbieter sind die §§ 146 ff. Abgabenordnung (AO) zu beachten. § 146 AO gibt vor, dass die steuerrechtlich relevanten „Bücher und Aufzeichnungen“ grundsätzlich im Original im Inland zu führen und aufzubewahren sind. Eine Verlagerung in eine ausländische Cloud war bisher nur ausnahmsweise auf Basis „bewilligter Erleichterungen“ nach § 148 AO oder aufgrund stillschweigender Duldung pragmatischer Finanzbehörden möglich. Beides wurde allerdings in der Vergangenheit von den lokalen Finanzbehörden sehr unterschiedlich gehandhabt.

Das hat sich zum 1. Januar 2009 geändert. Nach dem zum 1. Januar 2009 eingefügten § 146 Abs. 2a AO kann die zuständige Finanzbehörde auf Antrag bewilligen, dass elektronische Bücher in einem EU-Mitgliedstaat oder einem EWR-Mitgliedsstaat mit Amtshilfeübereinkommen geführt werden, wenn eine Zustimmung der ausländischen Finanzbehörden und eine Zugriffsmöglichkeit der deutschen Finanzbehörden nach § 147 Abs. 6 AO vorliegen. Allerdings muss sich erst noch zeigen, ob durch die Neuregelung eine Verbesserung eingetreten ist. Zum einen bereitet die erstgenannte Voraussetzung in der Praxis typischerweise Probleme. Eine Lösung für Cloud Services stellt die Regelung zum anderen nur bei Clouds innerhalb der EU bzw. des EWR dar.

Allerdings stellt sich in Anbetracht der ausdrücklichen Regelung in § 146 Abs. 2 a AO nun die Frage, ob die bisher in der Praxis genutzten Lösungen (Stichworte: „Erleichterungen“ nach § 148 AO, stillschweigende Duldung; s. eingangs) weiter möglich bleiben oder ob § 146 Abs. 2 a AO von den Finanzbehörden als abschließende Spezialregelung angesehen wird und damit globale Clouds verhindert werden.

Bestehen bleibt in jedem Fall die Pflicht zur Vorlage und unverzüglichen Verfügbarkeit einer umfassenden Verfahrensdokumentation nach § 147 AO. Das in diesem Kontext hervortretende Problem ist die tatsächliche Verfügbarkeit der Daten. Regelungen für den Fall von Außenprüfungen sollten daher in die Vereinbarungen mit dem Cloud-Anbieter aufgenommen werden.

7.4 Handelsrechtliche Buchführungspflicht

Jeder Kaufmann muss nach dem Handelsgesetzbuch (HGB) Belege für Buchungen in den von ihm nach § 238 Abs. 1 HGB zu führenden Büchern zehn Jahre lang bereit halten. Grundsätzlich ist das unter den Voraussetzungen des § 257 Abs. 3 HGB auch in elektronischer Form auf Datenträgern und auch in Clouds möglich. Das Handelsrecht stellt keine Pflicht auf, Bücher im Inland zu führen. Nach § 257 Abs. 3 Nr. 2 HGB muss allerdings eine Verfügbarkeit und Lesbarkeit der elektronischen Bücher innerhalb angemessener Frist sichergestellt sein.

7.5 Berufsgeheimnisträger

Für die durch § 203 StGB betroffenen Bereiche besonderer Verschwiegenheitspflicht (beispielsweise im Bereich der Rechtsberatung, des Gesundheitswesen oder der Kranken-, Unfall- und Lebensversicherungen) ist die Zulässigkeit (und damit auch die Strafbarkeit) von Auslagerungen auf Dritte, z. B. Cloud-Anbieter, umstritten. Zentraler Ansatzpunkt für eine Zulässigkeit ist die Auslegung des Gehilfenbegriffs des § 203 Abs. 3 S. 2 StGB, da eine Weitergabe ohne Zustimmung der Betroffenen (nur) an „Gehilfen“ erlaubt ist.

Nach traditioneller Ansicht sind solche Gehilfen nicht Personen, die selbständig tätig sind. Demnach wäre Cloud Computing im Bereich von § 203 StGB kaum möglich. Angemessener ist es daher, die Gehilfeneigenschaft nicht am Merkmal der Selbständigkeit, sondern daran festzumachen, ob der primär Schweigepflichtige die Herrschaft über die zur Verfügung gestellten Daten behält. Zur Beurteilung bieten sich die Kriterien des § 11 BDSG an. Dadurch

wird der Dritte in den „informationellen Schutzbereich“ eingebunden und kann als zum „Kreis der zum Wissen Berufenen“ gehörig angesehen werden; ein Verbot solcher Auslagerungen ist bei Einhaltung der strengen Kriterien des § 11 BDSG vor dem Schutzzweck des § 203 StGB daher nicht angezeigt. Die Zulässigkeit ist allerdings noch nicht rechtssicher geklärt.

8. Checkliste Vertragselemente

In Anlehnung an das EuroCloud SaaS Gütesiegel werden die wichtigsten Fragen hinsichtlich der vertraglichen Ausgestaltung aufgeführt. Anbieter, die durch EuroCloud nach diesen Anforderungen geprüft wurden, erfüllen die Basisanforderungen für die rechtskonforme Bereitstellung von Cloud-Diensten.

Es gibt schon heute eine Vielzahl von professionellen und sicheren Lösungen. Das Gütesiegel wird auch Anbietern eine wichtige Hilfestellung dabei liefern, das Vertrauen der Anwender zu fairen Konditionen zu gewinnen.

Es muss eine klare Abgrenzung zu den Anbieter geben, die ihr Angebot nicht mit der gebotenen Sorgfalt betreiben, denn der Anwender kann nur mit erheblichem Aufwand und schlimmstenfalls erst im Eskalationsfall die wirklichen Defizite erkennen.

Konkret werden im Gütesiegel folgende Kategorien erfasst:

- Anbieterprofil
- Vertrag und Compliance
- Sicherheit
- Betrieb der Infrastruktur
- Betriebsprozesse
- Anwendung
- Implementierung

Durch ein Punktesystem und die Vorgabe von Mindestkriterien kann ein Anbieter Gütestufen von ein bis fünf Sternen erreichen.

Im Unterschied zu anderen Initiativen, bei denen entweder nur Teilbereiche berücksichtigt werden oder die Angaben ohne Gegenkontrolle als freiwillige Selbstverpflichtung zu sehen sind, wird beim SaaS Gütesiegel eine Validierung der Angaben durchgeführt und in vereinbarten Zeiträumen wiederholt, damit ein konkreter Nachweis der Angaben vorliegt. Zudem verpflichtet sich der Anbieter, signifikante Änderungen der Rahmenbedingungen (z. B. Ort der Leistungserbringung, Änderung der Subunternehmervereinbarungen) und kritische Vorfälle unverzüglich zu melden.

Das SaaS-Gütesiegel wird ab Anfang 2011 offiziell vergeben. Eine Reihe von Anbietern bereiten sich gerade für die Zertifizierung vor.

8.1 Vertragsabschluss und Vertragsgestaltung

- Wie wird der Vertrag geschlossen?
  - Online
  - Schriftlich

- Kann der Kunde auf einen schriftlichen Vertrag bestehen?

8.2 Wirkung auf Unterauftragnehmer

- Hat der Auftragnehmer seine Unterauftragnehmer an dieselben Verpflichtungen gebunden, die er gegenüber dem Auftraggeber eingeht?

8.3 Leistungsverrechnung

- Wird die Nutzung des Services pauschal oder zeitabhängig berechnet?

- Wird die Nutzung des Services nach Verbrauch berechnet?
  - Existieren Mengenrabatte/unterschiedliche Tarife in Abhängigkeit von der abgenommenen Servicemenge?
  - Kann der Auftragnehmer seinen Tarif bei signifikanter Änderung des Nutzungsumfangs ändern?
  - Gibt es eine Best-Price-Option?

- Wird optional eine Flatrate oder per-User-Flatrate angeboten?

- Gibt es extra zu verrechnende Sonderleistungen?

- Wenn ja, welche?

8.4 Leistungsstörungen

- Leistungsstörung beim Auftragnehmer oder dessen Unterauftragnehmern
  - Bestehen Regelungen zum Schadensersatz bei Leistungsstörungen?

- Streit über Leistungserbringung/Zahlungsverzug
  - Ist ein Zurückbehaltungsrecht an Daten des Auftraggebers oder ihm gegenüber zu erbringenden Leistungen vertraglich ausgeschlossen?
  - Ist auch im Fall von Streitigkeiten zur Leistungserbringung oder Zahlungsverzug ausgeschlossen, dass der Auftragnehmer die Daten ohne Zustimmung des Auftraggebers löscht?

8.5 Vertragskündigung

- Welche Kündigungsfristen sind für den Auftraggeber und den Auftragnehmer definiert?
- Gibt es eine abschließende Liste der möglichen Kündigungsgründe?
- Ist eine „Kündigung aus wichtigem Grund“ möglich?
  - Wenn ja, für wen?
    - Auftraggeber
    - Auftragnehmer
    - Warum?
- Ist eine Vorankündigung von Änderungen bei der Diensterbringung von Subunternehmern vertraglich geregelt?
- Gibt es ein Sonderkündigungsrecht des Auftraggebers, wenn der Auftragnehmer wichtige Subunternehmer wechselt?
- Existieren Regelungen zur Mitwirkung des Auftragnehmers bei der Datenbereitstellung nach einer Vertragskündigung?

8.6 Insolvenz des Auftragnehmers

- Existieren Regelungen zum Schutz der Daten des Auftraggebers und der Verfügbarkeit der Anwendung bei Insolvenz des Auftragnehmers?
  - Existiert ein Source Code Deposit?
  - Ist Software an bestimmte Plattform gebunden?
  - Wird dem Auftraggeber ein Recht auf Herausgabe der letzten Datensicherung und Dokumentation eingeräumt?

8.7 Compliance

- GDPdU[2] -Relevanz
  - Sind für die als SaaS betriebene Anwendung die GDPdU zu beachten?
    a. Werden im Rahmen der Anwendung elektronische Rechnungen verarbeitet?
    b. Werden im Rahmen der Anwendung Daten verarbeitet, die direkt in die Buchführung des Auftraggebers einfließen?
- GDPdU-Fähigkeit
  - Falls GDPdU anzuwenden ist: Werden die Verpflichtungen des Auftraggebers gegenüber der Finanzbehörde durch den Auftragnehmer unterstützt?

[2] Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

- falls a): Werden die Vorgaben zur Prüfung der Signatur und zur Speicherung der Rechnungen im Original- und im Inhouseformat umgesetzt?
- falls b): Bietet die Anwendung die Möglichkeit des Datenzugriffs in allen drei vorgeschriebenen Zugriffsarten (Z1, Z2, Z3)?
- falls b): Bietet das Rollenkonzept der Anwendung eine Prüferrolle, denen die Leserechte des Außenprüfers zugeordnet sind?
- falls b): Sind die steuerrelevanten Daten innerhalb der Anwendung identifiziert?
- für a) oder b): Liefert der Anbieter eine adäquate Verfahrensdokumentation?
- für a) oder b) UND wenn ein Archivierungssystem für Altdaten genutzt wird: Ist sichergestellt, dass das Archivsystem dieselben Zugriffs- und Auswertungsmöglichkeiten besitzt wie das Produktivsystem?

- Datenschutz-Relevanz
  - Werden innerhalb der Anwendung personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG) verarbeitet?

NUR WENN JA, sind die folgenden Fragen zu beantworten.

Zu beachten ist, dass der Begriff der „personenbezogenen Daten" im Sinne des BDSGs sehr weit gefasst ist. Alle Daten, die einen Personenbezug haben oder bei denen der Auftraggeber, der Auftragnehmer oder ein Dritter einen Personenbezug herstellen könnte, gelten aus Sicht der Datenschutzbehörden als „personenbezogene Daten". In der Praxis wird es nur sehr wenige IT- und Cloud-Anwendungen geben, bei denen Daten verarbeitet werden, die nicht zumindest teilweise personenbezogen sind.

- Datenschutz-Organisation
  - Existiert ein Datenschutzbeauftragter, der gegenüber dem Auftraggeber für alle Belange des Datenschutzes beim Auftragnehmer und seinen Unterauftragnehmern als Ansprechpartner zur Verfügung steht?
  - Sind die Mitarbeiter des Auftragnehmers nachweislich auf das Datengeheimnis nach § 5 BDSG verpflichtet?

- Ist geregelt, welche Seite gegenüber den Kunden des Auftragnehmers den Ansprechpartner für den Datenschutz darstellt?
  - Sind Regeln für die Berichtigung, Löschung und Sperrung von Daten auf Antrag eines Betroffenen definiert?

- Auswahl Auftragnehmer und Subunternehmer
  - Bietet der Auftragnehmer genügend Informationen zu seinem Unternehmen und seinen Unterauftragnehmern, um dem Auftraggeber eine fundierte Auswahl des Auftragnehmers gemäß §11 Abs. 2 S.1 BDSG zu ermöglichen?
  - Werden die Unterauftragnehmer bekanntgegeben?

- Datenschutzniveau
  - Ist – soweit einschlägig – auch außerhalb der EU (auch bei beteiligten Unterauftragnehmern) ein angemessenes Datenschutzniveau (z. B. über EU-Standardvertrag, Safe-Harbour-Regelung) hergestellt?
  - Besteht die Möglichkeit, wenn aufgrund von gesetzlichen oder behördlichen Auflagen an den Auftraggeber erforderlich, die Orte der Datenhaltung auf Deutschland oder die EU einzugrenzen?

- Beauftragung und Weisungsrecht
  - Sind die Verantwortlichkeiten zwischen Auftraggeber (grundsätzliche datenschutzrechtliche Verantwortlichkeit) und Auftragnehmer (Umsetzung von Weisungen, technischen Schutzmaßnahmen etc.) sauber definiert?
  - Ist der Umfang des Auftrags zur Datenverarbeitung hinreichend klar spezifiziert, insbesondere:
    - Ist der Dienst grob beschrieben? Sind in der Beschreibung der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen dokumentiert?
    - Sind die Dauer der Verarbeitung und die Löschung der Daten exakt definiert?
    - Ist ein Entscheidungsspielraum des Dienstleisters zur Verarbeitung der Daten ausgeschlossen?
    - Ist dokumentiert, ob und wenn ja wie „besondere Arten personenbezogener Daten“ im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden?
  - Ist das Weisungsrecht des Auftraggebers eindeutig definiert?

- Kommunikation
  - Ist eine Kommunikationsregel etabliert für den Fall, dass Weisungen des Auftraggebers nach Meinung des Auftragnehmers gegen den Datenschutz verstoßen?
  - Sind Sachverhalte definiert, die als mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen dem Auftraggeber anzeigt werden müssen?

- Umsetzung technischer und organisatorischer Datenschutzmaßnahmen
  - Existiert eine Dokumentation/ein Konzept, welche technischen und organisatorischen Maßnahmen umgesetzt werden, um die Vorgaben des Anhangs zu § 9 BDSG zu erfüllen?
  - Hat der Auftraggeber diesem Konzept (und Änderungen daran) zuzustimmen?

- Kontrollmöglichkeiten des Auftraggebers
  - Existieren Regelungen zu Kontrollrechten des Auftraggebers und zu den entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, insbesondere:
    - Ist ein Kontrollrecht des Auftraggebers und/oder eines vom Auftraggeber beauftragten Dritten vor Ort beim Auftragnehmer oder seinen Unterauftragnehmern ausdrücklich vereinbart?
    - Existieren (kumulativ oder alternativ zu Kontrollen durch den Auftraggeber) regelmäßige Kontrollen/Audits und Zertifizierungen, die den Datenschutz beim Auftragnehmer und die Verpflichtungen gegenüber dem Auftraggeber kontrollieren und zertifizieren?
    - Ist eine Regelung zur Mitwirkung des Auftragnehmers und den entstehenden Kosten getroffen?

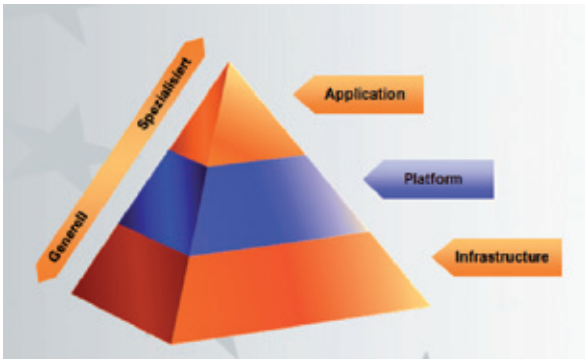
- Datenlöschung bei Vertragsende
  - Existieren Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrages?
    - Wird gewährleistet, dass die Daten auf Wunsch des Auftraggebers tatsächlich gelöscht werden?

9. Glossar Cloud Computing

Cloud Computing

„Cloud Computing ist ein Modell, das on-demand und online den Zugriff auf einen gemeinsamen Pool konfigurierbarer Computing-Ressourcen wie Netzwerke, Server, Speichersysteme, Anwendungen und Dienste ermöglicht. Diese können passgenau, schnell, kostengünstig und mit minimalem Verwaltungsaufwand bereitgestellt und abgerufen werden."
(Definition: NIST; National Institute of Standards and Technology, USA)

Als Grundansatz für die Darstellung der verschiedenen Elemente des Cloud Computings wird oftmals das SPI-Modell herangezogen, welches die drei Serviceebenen – Infrastruktur, Platform und Software – darstellt:



Hierbei werden die Ebenen aufeinander aufbauend dargestellt, wobei die jeweils unteren Ebenen auch unabhängig von der darüber liegenden Ebene genutzt werden können.

Public Cloud

IT-Dienstleistungen werden von einem Cloud-Anbieter bereitgestellt und können von jedem über das Internet genutzt werden.

Private Cloud

IT-Dienstleistungen werden aus den eigenen Rechenzentren bezogen. Alle Dienste und die Infrastruktur unterstehen einer Institution. Die Cloud kann durchaus von Dritten betrieben werden. Auf die Dienste wird entweder über das Intranet oder über VPN (Virtual Private Network) zugegriffen.

Hybride Cloud
ist eine Mischform bestehend aus einer Public Cloud und einer Private Cloud.

Förderierte Cloud
Hybride Cloud mit spezieller Sicherheitstechnik durch vertrauenswürdige Serviceanbieter im Bereich der Identifikation und Verschlüsselung.

Infrastructure as a Service
Bereitstellung von Rechen- und Speicherkapazitäten als Service.

Platform as a Service
Bereitstellung von „Middleware“ als Service.

Software as a Service
Bereitstellung von Applikationen als Service.

X as a Service
Bereitstellung von zusätzlichen Funktionen, wie Geschäftsprozesse, Netzwerke, Kommunikation und weitere als Service.

10. Quellenachweise

Rechtsthemen

- Weichert, Cloud Computing und Datenschutz, DuD 2010, 679, 679
- Niemann/Paul, „Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud-Computing“, K&R 2009, 444
- Niemann/Hennrich, „Kontrollen in den Wolken? Auftragsdatenverarbeitung in Zeiten des Cloud Computings“, CR 2010, 686
- Niemann, „Cloud Compuiting & Recht“, Deutscher Anwaltsspiegel, Ausgabe 08/2010, 14
- Bierekoven, ITRB 2010, 42
- Pohle/Ammann, CR 2009, 273
- Bergmann/Möhrle/Herb, Datenschutzrecht, 40. Ergänzungslieferung – November 2009, § 11 BDSG, Rn. 15a
- Eckhardt, „Rechtsrahmen Cloud Computing“, in: Cloud Computing: Neue Optionen für Unternehmen, Strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis, hrsg. v. Christiana Köhler-Schute, Berlin 2011, ISBN 978 3 9813142 2 9, Erscheinungstermin Jan. 2011
- Eckhardt, „Cloud Computing – ein rechtlicher Überblick“, IM – Die Fachzeitschrift für Information Management und Consulting, Ausgabe 4/2010

Cloud Computing und Compliance

- ENISA Cloud Computing Risk Assessment: **http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment**

- BSI – Eckpunktepapier Cloud Computing: **https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Cloud_Computing_28092010.html**

Auftragsdatenverarbeitung

Begleitend zu den vertraglichen Vereinbarungen wird der Abschluss einer speziellen Datenschutzvereinbarung empfohlen. Eine entsprechende Mustervorlage ist zu beziehen bei der Gesellschaft für Datensicherheit und Datenschutz e. V.: **https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg**

11. Rechtlicher Hinweis

1. Allgemeines

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung der rechtlichen Rahmenbedingungen für Cloud Computing, stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls voraussetzt.

2. Inhalt des Leitfadens

Die Herausgeber/Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereit gestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen die Herausgeber/Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens der Herausgeber/Autoren kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

3. Verweise und Links

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z. B. „Links“), die außerhalb des Verantwortungsbereichs der Herausgeber/Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem die Herausgeber/Autoren von den Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Die Herausgeber/Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben die Herausgeber/Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wurden. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotener Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht diejenigen, die über Links auf die jeweilige Veröffentlichung lediglich verweisen.

4. Urheberrecht

Die auf dieser Webseite dargestellten Inhalte wie Texte, Grafiken oder Bilder sind nach dem deutschen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

12. Autoren

Rechtsanwalt Dr. Jens Eckhardt
JUCONOMY Rechtsanwälte, Düsseldorf

Rechtsanwalt Dr. Marc Hilber LL.M
Partner Oppenhoff & Partner, Köln

Rüdiger Giebichenstein
KPMG AG Wirtschaftsprüfungs-gesellschaft, Köln

Rechtsanwalt Dr. Fabian Niemann
Partner Bird & Bird LLP, Frankfurt

Rechtsanwalt Dr. Thomas Helbing
Rechtsanwaltskanzlei Helbing, München

Andreas Weiss
Direktor EuroCloud Deutschland_eco e. V.

EuroCloud Deutschland_eco e.V.
Lichtstraße 43h
50825 Köln

Tel.: 0221 / 70 00 48 – 0
Fax: 0221 / 70 00 48 – 111
E-Mail: info@eurocloud.de
Web: www.eurocloud.de