von **Matthias Petzold**

Cloud Computing und Datenschutz - Eine Einführung

Wissen Sie, von welchen Unternehmen und in welchen Ländern Ihre Daten in der Cloud ("Wolke") verarbeitet werden? Haben Sie Ihren Cloud-Anbieter, der Ihre Daten "in der Wolke verarbeitet", unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt? Vergewissern Sie sich regelmäßig von der Einhaltung der beim Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen?

I. Vorbemerkung

Der Beitrag soll einen Einblick darüber geben, inwieweit sich in der Praxis das Geschäftsmodell des Cloud-Computing, d.h. die "Datenverarbeitung in der Wolke", und der Datenschutz miteinander vereinbaren lassen.

> *Es existiert eine Vielzahl von Definitionen des Cloud Computing. Nach einer der pragmatischsten Definitionen "steht Cloud Computing für einen Pool aus abstrahierter, hochskalierbarer und verwalteter IT-Infrastruktur, die Kundenanwendungen vorhält und falls erforderlich nach Gebrauch abgerechnet werden kann".*

In der Praxis bedeutet dies, dass es sich bei Cloud Computing um eine Form des Outsourcings, also um die Auslagerung von unterschiedlichsten Datenverarbeitungsleistungen eines Unternehmens an einen IT-Anbieter, handelt. Cloud Computing versteht sich als eine Bereitstellung von IT-Diensten, einschließlich Hard- und/oder Software, durch den Cloud-Anbieter, die der Nutzer über einen Internetbrowser auf Zeit nutzt. Sinn und Zweck dieses Modells aus Sicht des Nutzers ist es, eigene Resourcen und damit Kosten zu sparen oder eigene Bedarfsspitzen auszulagern.

In diesem Beitrag wird auf die wirtschaftlichen, organisatorischen, technischen und rechtlichen Aspekte, mit Ausnahme des Datenschutzes und der Datensicherheit, des Cloud Computing nicht eingegangen. Dennoch soll nicht unerwähnt bleiben, dass aus rechtlicher Sicht bei der Inanspruchnahme von Diensten in einer Cloud insbesondere zu prüfen ist, die vertragstypologische Einordnung cloud-basierter Leistungen, die Pflegemaßnahmen und die Maßnahmen zur Fehlerbehebung, die Spezifikation der Anforderungen an die zu erbringenden Leistungen (Service Level Agreement), die Maßnahmen zur Einhaltung von Sicherheitsstandards (Security Level Agreement), die Maßnahmen zur Abwehr von potentiellen Störern und urheberrechtliche Fragen zur Einräumung der cloud-relevanten Nutzungsrechte.

Auf dem Markt werden unterschiedliche Modelle des Cloud Computing angeboten.

Im Wesentlichen sind dies:

- Platform-as-a-Service (PaaS): Das zur Verfügung stellen einer Anwendungsplattform/von Applikationen in der Cloud bzw. von OnDemand Diensten in Rechenzentren;
- Infrastructure-as-a-Service (IaaS): Das zur Verfügung stellen einer umfassenden IT-Infrastruktur bzw. von bedarfsgerechten Rechen- und Speicherkapazitäten;
- Software-as-a-Service (SaaS): Das zur Verfügung stellen von fertigen Softwarelösungen im Netz bzw. in Cloud Rechenzentren.

Bei der Cloud wird unterschieden zwischen sog. Private Clouds, in der sich Anbieter und Nutzer im selben Konzern bzw. Unternehmen befinden, die entsprechend vernetzt sind sowie sog. Public Clouds, die öffentlich sind, d.h. Rechenleistungen, die von beliebigen (externen) dritten Unternehmen genutzt werden können. Vor allem bei einer Public Cloud stellt sich somit die zentrale Frage der Sicherheit der Daten.

Einer der wesentlichen Fragen des Outsourcings von IT-Leistungen, wie beispielsweise beim Hosting und Application Service Providing (ASP), so auch beim Cloud Computing, ist es, zu klären und vertraglich zu regeln, ob bzw. wie der Datenschutz, die Datensicherheit und die Vertraulichkeit, einschließlich die Betriebs- und Geschäftsgeheimnisse, des Nutzers der Cloud-Dienste gewährleistet werden können.

II. Datenschutz

1. Anwendungsbereich

Aus Sicht des Bundesdatenschutzgesetztes (BDSG) sind dessen Regelungen im Zusammenhang mit dem Cloud Computing nur dann anwendbar, wenn personenbezogene Daten im Inland (Ort der Datenverarbeitung) erhoben, verarbeitet oder genutzt werden (§§ 1, 3 BDSG).

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, dem sog. Betroffenen.

Betroffene können Mitarbeiter des Cloud-Nutzers sowie Kunden und Lieferanten des Nutzers sein, deren personenbezogene Daten von dem Unternehmen (Nutzer) an den Cloud-Anbieter übermittelt werden.

Eine Anwendbarkeit des Datenschutzrechts ist somit nicht gegeben, wenn beim Cloud-Computing keine personenbezogenen Daten verarbeitet werden. Seitens des Cloud-Nutzers kann aber häufig nicht

zweifelsfrei geklärt werden, ob es sich bei Daten, die an den Cloud-Anbieter übermittelt werden, um personenbezogene Daten handelt oder nicht.

Einerseits kann dieses Dilemma so gelöst werden, alle Daten, insbesondere die zweifelsfrei personenbezogenen Daten, aber auch die Daten, die nicht zweifelsfrei als personenbezogene Daten bestimmbar sind, etwa mit Hilfe einer "Anonymisierungs-Software", zu anonymisieren.

Anderseits ist es technisch durch Abgleiche und Vernetzung durchaus möglich, nicht identifizierbare Daten einer bestimmbaren Person zuzuordnen.

Die personenbezogenen Daten von Betroffenen dürfen nur dann an einen Dritten, den Cloud-Anbieter, übermittelt werden, wenn der Betroffene seine Einwilligung erteilt hat oder ein gesetzlicher Erlaubnistatbestand vorliegt (§ 4 BDSG). Da das Datenschutzrecht kein Konzernprivileg kennt, ist auch eine Tochtergesellschaft in einem Konzernverbund, die als Cloud-Anbieter fungiert, sog. Dritter im Sinne des Datenschutzrechtes.

2. Einwilligung

In der Praxis stößt man bei dem Versuch, eine Einwilligung des Betroffenen einzuholen, sehr schnell an rechtliche und tatsächliche Grenzen.

Eine solche Einwilligung ist nur dann rechtswirksam, wenn diese freiwillig und grundsätzlich schriftlich gegeben worden ist. Bei Mitarbeitern des Nutzers kann diese Freiwilligkeit zweifelhaft sein, zumal wenn der Mitarbeiter Konsequenzen befürchtet, wenn er die Einwilligung nicht gibt. Ebenso ist der Betroffene auf den Zweck der Erhebung der Daten, deren Verarbeitung oder Nutzung in der Cloud hinzuweisen (§ 4 a BDSG). In diesem Zusammenhang müssen den betroffenen Mitarbeitern auch alle an den Cloud-Diensten beteiligten Unternehmen und deren Unterauftragnehmer sowie in der Folge etwaige Wechsel mitgeteilt und deren erneute Einwilligung eingeholt werden; dies ist in der Praxis kaum möglich.

Das Einholen der datenschutzrechtlichen Einwilligung durch den Cloud-Nutzer bei Mitarbeitern von Kunden und Lieferanten ist ungleich aufwändiger und schwerer umzusetzen als bei den Mitarbeitern des Cloud-Nutzers selbst. Ganz davon abgesehen, dass in der Regel keine 100%ige Rücklaufquote erzielt werden kann.

3. Gesetzlicher Erlaubnistatbestand

Das Übermitteln personenbezogener Daten oder ihre Nutzung ist als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (§ 28 Abs. 1 Nr. 1 BDSG).

In der Regel ist dieser Tatbestand bei einem Outsourcing von IT-Diensten in eine Cloud nicht erfüllt, da der Zweck eines Arbeitsvertrages, den bspw. ein Mitarbeiter mit dem Cloud-Nutzer geschlossen hat oder ein Vertrag den ein Kunde bzw. ein Lieferant mit dem Cloud-Nutzer geschlossen hat, grundsätzlich nicht umfasst, dass personenbezogene Daten der Betroffenen in eine Cloud übermittelt werden.

Eine andere Alternative ist, dass das Übermitteln personenbezogener Daten oder ihre Nutzung zur Wahrung berechtigter Interessen der verantwortlichen Stelle, d.h. des Cloud-Nutzers, erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Nr. 2 BDSG).

Bei der Interessenabwägung zwischen den berechtigten Interessen (in der Regel wirtschaftlichen Interessen) des Unternehmens (Nutzers) und des Betroffenen ist ein strenger Maßstab anzulegen und dieser Tatbestand ist im Einzelfall restriktiv auszulegen.

4. Auftragsdatenverarbeitung

Beim Cloud Computing handelt es sich als einer Form des Outsourcings nach allgemeiner Auffassung um sog. Auftragsdatenverarbeitung (§ 11 BDSG). Der Cloud-Nutzer bleibt für die Verarbeitung der in die Cloud übermittelten personenbezogen Daten verantwortlich und der Cloud-Anbieter erbringt als "Gehilfe" die an ihn ausgelagerten IT-Leistungen nach den Weisungen des Cloud-Nutzers.

4.1 Auftragsdatenverarbeitung im Inland, in der EU und EWR

Die Auftragsdatenverarbeitung ist soweit diese durch den Cloud-Anbieter im Inland, einem anderen Mitgliedsstaat der Europäischen Union (EU) oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) (derzeit Lichtenstein, Norwegen und Island) privilegiert. Ein Cloud-Anbieter gilt insoweit nach § 3 Abs. 8 BDSG und § 2 Abs. 9 DSG-LSA nicht als Dritter im Sinne des Datenschutzgesetzes und es finden daher bei der klassischen Auftragsdatenverarbeitung nicht die einschränkenden Regelungen über den Datenaustausch, wie der Einwilligung (siehe oben Ziff. II, 2.), Anwendung.

Der Cloud-Anbieter muss also die Cloud iSd Auftragsdatenverarbeitung nach § 11 BDSG in dem wie vor bezeichneten Gebiet betreiben; dies gilt jedoch nicht nur für den Cloud-Anbieter selbst, sondern auch für alle Unterauftragnehmer, derer sich der Cloud-Anbieter zu Erbringung der Cloud-Dienste bedient.

Der Cloud-Nutzer bleibt dafür verantwortlich, dass die einschlägigen Datenschutzbestimmungen bei der Erbringung der Cloud-Services durch den Cloud-Anbieter eingehalten werden und dieser darf nur im Rahmen der Weisungen des Cloud-Nutzers tätig werden. Der Cloud-Nutzer bleibt Herr der Daten, hat somit die Pflicht, den Cloud-Anbieter sorgfältig auszuwählen und sich von dessen Eignung unter besonderer Berücksichtigung der vom Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (vgl. § 11 Abs. 2 S. 1 BDSG).

Der Cloud-Nutzer muss während der Vertragslaufzeit die Einhaltung der technischen und organisatorischen Maßnahmen beim Cloud-Anbieter ständig kontrollieren.

In der Praxis ist der damit verbundene Kontrollaufwand, zumal vor Ort bei dem Cloud-Anbieter, ob der gegebenen tatsächlichen Gegebenheiten (wie Zugangsrecht zu den Rechenzentren, Verteilung der Rechenzentren) oft nicht praktikabel. Es ist daher anerkannt, dass der Cloud-Anbieter in Form einer Selbstbindung dem Cloud-Nutzer detaillierte Prüfberichte zur Verfügung stellt oder die Kontrollrechte an eine unabhängige, fachlich und zuverlässige Stelle übertragen werden, die einschlägig zertifiziert ist.

Über die Erbringung der Cloud-Dienste ist weiterhin schriftlich ein Vertrag zu vereinbaren, der insbesondere die Vorgaben von § 11 BDSG Abs. 2 BDSG zu berücksichtigen hat.

Besonders zu erwähnen ist, dass u.a. vertraglich festzulegen sind:

- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen (vgl. § 11 Abs. 2 Nr. 2 BDSG),
- die nach § 9 BDSG iVm Anlage zu § 9 S. 1 BDSG zu treffenden technischen und organisatorischen Maßnahmen (§ 11 Abs. 2 Nr. 3 BDSG),
- -die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen (vgl. § 11 Abs. 2 Nr. 6 BDSG) sowie
- die Kontrollrechte des Cloud-Nutzers und die entsprechenden Duldungs- und Mitwirkungspflichten des Cloud-Anbieters (vgl.11 Abs. 2 Nr. 7 BDSG).

Eine Privilegierung nach § 11 BDSG liegt mithin nicht vor, wenn der Empfänger der Daten ein Dritter iSv § 3 Abs. 8 S. 2 BDSG ist, also verantwortliche Stelle außerhalb des Inlands, der EU oder des EWR.

4.2. Auftragsdatenverarbeitung in einem Dritt(aus)land, außerhalb der EU und des EWR

Bei der Übermitlung von personenbezogenen Daten in eine Cloud im Ausland, also außerhalb der EU oder des EWR, müssen zusätzlich die Voraussetzungen von § 4 b BDSG erfüllt sein.

Im Zuge der Globalisierung - da die IT-Unternehmen, die Cloud-Dienste anbieten, in der Regel international agieren und um den Sinn und Zweck des Cloud-Computing zu erfüllen (siehe dazu oben Ziff. I) - werden Cloud-Dienste regelmäßig im Ausland, außerhalb der EU/des EWR, erbracht.

Aus diesem Grunde werden personenbezogenen Daten vom Inland zwangsläufig in eine Cloud im Dritt(aus)land übermittelt. Eine solche Übermittlung ist aber nur dann zulässig, wenn es dafür eine Rechtsgrundlage gibt.

Für eine Legitimation einer Datenübermittlung ins Dritt(aus)land an einen Cloud-Anbieter kommt insbesondere in Betracht:

- Wenn die Europäische Kommission die Feststellung getroffen hat, dass in dem Dritt(aus) land ein der EU vergleichbares "angemessenes Datenschutzniveau besteht" (wie beispielsweise in Argentinien, Guernsey, Insel Man, Kanada, Schweiz);
- wenn die von der Europäischen Kommission zur Verfügung gestellten "Standardvertragsklauseln für die Übermittlung von Daten in Drittländer" vereinbart werden;
- wenn der Cloud-Anbieter in den USA seinen Sitz hat und sich den sog. "Safe Harbor Principles", einschließlich den sog. "Frequently Asked Questions", verpflichtet hat;
- wenn eine verbindliche Unternehmensregelung nach § 4 c Abs. 2 S. 1 BDSG zwischen den an der Cloud beteiligten Unternehmen getroffen wird (sog. Corporate Binding Rules) und diese durch die

zuständige Datenschutzbehörden genehmigt wurde.

Es gibt Stimmen, die eine Zertifizierung nach den "Safe Harbor Principles" in den USA, insbesondere im Zusammenhang mit dem Cloud-Computing, nicht als ausreichend ansehen, um den datenschutzrechtlichen Vorgaben bei einer Datenübermittlung in die USA zu genügen.

Zu berücksichtigen ist in diesem Zusammenhang auch, dass sich in den USA ansässige Cloud-Anbieter oftmals Unterauftragnehmer zur Erbringung der Cloud-Dienste bedienen, die ihren Sitz außerhalb der USA, wie in Indien oder Singapur, haben. Um in diesen Fällen dem Grundsatz eines "angemessenen Datenschutzniveaus" Rechnung zu tragen, empfiehlt es sich, mit diesen Unterauftragnehmern die von der Europäischen Union festgestellten "Standardklausel für die Übermittlung von Daten in Drittländer" zu vereinbaren. Da diese Unterauftragnehmer aus unterschiedlichsten Gründen oft wechseln, hat der (Neu) Abschluss dieser EU-Standardklauseln für den Cloud-Anbieter einen enormen administrativen Aufwand zur Folge. Um sich diesem Aufwand zu entziehen, sind aus der Praxis Fälle bekannt, in denen der Cloud-Anbieter versucht, sich seiner Pflicht dadurch zu entledigen, in dem er den Cloud-Nutzer auffordert, dafür Sorge zu tragen, dass ihm keine personenbezogenen Daten übermittelt werden. Inwieweit dieses Verlangen eine Lösung darstellt und mit angemessenem Aufwand möglich ist, ist eine Frage des Einzelfalles.

II. Datensicherheit und Vertraulichkeit

Die Regelungen der Datenschutzgesetze, insbesondere des Bundesdatenschutzgesetzes (BDSG) sind, wie oben unter Ziff. II. ausgeführt, dann anwendbar, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden.

Mithin unterliegen Daten, die keine personenbezogenen Daten sind, nicht den datenschutzrechtlichen Bestimmungen. Dennoch sind auch solche nicht personenbezogenen Daten, wie beispielsweise technische Daten und Finanzdaten, für Unternehmen oder natürliche Personen mindestens genauso schutzwürdig wie personenbezogene Daten.

Wenn derartige nicht personenbezogene Daten an den Cloud-Anbieter übermittelt werden, auf die unbefugte Dritte keinen Zugriff haben sollen, ist dieser Sachverhalt mit dem Cloud-Anbieter entsprechend, etwa in Form eines Security Level Agreements, vertraglich zu regeln, einschließlich der Sanktionierung von etwaigen Verstößen.

Zwar bestehen gesetzliche Regelungen, wie §§ 17 ff UWG und §§ 202 a, 263 a, 303 a, 303 b StGB, die im Einzelfall der Sicherheit des Nutzers dienen können. Diese Regelungen gelten ob der nationalen Geltung für Inlandstaten jedoch dann nicht, wenn ein Verstoß im Ausland im Rahmen einer internationalen Cloud

vorliegt (vgl. §§ 3 ff StGB).

Auch ist bei der Übermittlung von Daten ins Ausland zu prüfen, inwieweit in dem jeweiligen Land Zugriffsmöglichkeiten oder gar (gesetzlich normierte) Zugriffsrechte des Cloud-Anbieters oder Dritter, wie durch öffentliche Stellen und Gerichte, bestehen.

III. Fazit

Als Fazit bleibt festzuhalten, dass Vorstände, Geschäftsführer und sonstige in einem Unternehmen Verantwortliche, wie aus IT-, Einkaufs- und Rechtsabteilungen, die sich für das Cloud Computing entscheiden, vorab eine Bestandaufnahme darüber vornehmen, ob das Geschäftsmodell und die einschlägigen Schutzstandards des Cloud-Anbieters geeignet sind, den (datenschutz-) rechtlichen und tatsächlichen Vorgaben zu genügen.

Nicht zuletzt aus Compliance-Gesichtpunkten gilt es Risiken für das Unternehmen zu vermeiden und eine persönliche Haftung der verantwortlichen Personen auszuschließen.

Autor:
Matthias Petzold
Rechtsanwalt