März 2019

10 Schritte die Sie auf Ihrem Weg in die Cloud beachten sollten

Laut einer aktuellen Studie[1] ist davon auszugehen, dass mehr als die Hälfte aller Unternehmen weltweit mindestens eine Public-Cloud-Plattform nutzen. In Deutschland setzen sogar 66 % der Unternehmen auf Cloud-Computing.[2] Die Auslagerung von Rechenkapazität, Speicherfähigkeit und Anwenderprogrammen bildet dabei einen wesentlichen Treiber für die Datenexplosion im Internet.[3] Auch die Europäische Kommission sieht in der Verwendung von Cloud-Computing große Vorteile für die europäische Wirtschaft.[4] Egal ob es sich um ein Cloud-Konzept von Microsoft, Oracle, Amazon, IBM oder Fabasoft handelt, die rechtlichen Fragestellungen sind oft die gleichen. In diesem Newsletter möchte ich Ihnen 10 Schritte mitteilen, die Sie auf Ihrem Weg in die Cloud beachten sollten.

1. Implementierung eines IT-Projektmanagements

Wussten Sie, dass 52 % aller IT-Projekte von geringem Erfolg sind? 19 % scheitern gar.[5] Das ist ein schockierendes Ergebnis, wenn man bedenkt, dass IT-Projekte regelmäßig mit Auftragswerten im sechsstelligen Bereich verbunden sind. Die Lösung: Ein sauber dokumentiertes und durchgedachtes IT-Projektmanagement. Ein Planungsprozess, Durchführungsprozess, Controlling-Prozess, Kommunikationsprozess und Ressourcenmanagementprozess sind unabdingbar – unabhängig davon, ob es sich um ein sequenzielles oder agiles Projekt handelt oder ob die „Scrum"-Methode angewendet wird. Ordnung kostet Zeit und Geld – aber Unordnung noch viel mehr. Nach einer alten Faustregel lohnt es sich ab einem Auftragswert von EUR 15.000,00 einen organisierten IT-Projektprozess zu implementieren.[6]

2. Zieldefinition

Werden Sie sich im Klaren darüber, was Ihr Unternehmen tatsächlich braucht. Welche Speicherkapazitäten, Datentransferrate, Sicherheitsstandards, Flexibilität, Lizenzen sind

---

[1] https://www.forrester.com/report/Predictions+2018+Cloud+Computing+Accelerates+Enterprise+Transformation+Everywhere/-/E-RES139611 (Abgerufen am 13.2.2019).
[2] https://home.kpmg/de/de/home/themen/2016/03/cloud-computing.html (Abgerufen am 18.2.2019).
[3] *Eberl*, Smarte Maschinen, Hanser-Verlag, S 54.
[4] Europäische Kommission, Pressemitteilung vom 27.9.2012, Digitale Agenda.
[5] *Tiemeyer* in Tiemeyer (Hrsg), IT-Projektmanagment, S 2.
[6] *Jaburek* in Handbuch der EDV-Verträge, S 33.

für Ihr Business-Modell erforderlich? Ist Ihre Infrastruktur mit der präferierten Cloud-Lösung kompatibel? Ist eine Hochverfügbarkeit erforderlich und möglich? Ist ein Datentransfer in ein Drittland für Sie akzeptabel? Wie sieht ein Exit-Szenario aus? Wie verhindern Sie „Lock-in-Effekte"? Welchen Wert legen Sie auf Usability? Wollen Sie eine Standard- oder eine Individualsoftware? Ist Ihr Geschäftspartner auf wirtschaftlich soliden Beinen? Wenn Sie sich über all diese technischen, organisatorischen, betriebswirtschaftlichen, sicherheitsspezifischen und rechtlichen Fragen im Klaren sind, definieren sie ein entsprechende Lastenheft.

3. Cloud versus eigenes Rechenzentrum

Das Unternehmen sollte aus betriebswirtschaftlichen und sicherheitsspezifischen Gesichtspunkten abwägen, ob die Daten in der Cloud gespeichert werden sollen oder „on premise" im eigenen Rechenzentrum. Dabei sollten insbesondere die Aspekte Objektsicherheit (Mechanischer Schutz, Videoüberwachung, Vier-Augen-Prinzip, Sicherheitspersonal), Ausfallsicherheit (redundante Hardware, Netzwerkverbindungen und Stromleitungen), Back-Up-Strategien sowie der Schutz vor digitalen Angriffen gegeneinander abgewogen werden.[7]

4. Datensicherheit

Kann der Auftragnehmer eine angemessene Datensicherheit gewährleisten? Entspricht die Datensicherheit dem Stand der Technik? Zur Überprüfung dieser Anforderungen kann teilweise auf IT-sicherheitsspezifische Zertifikate zurückgegriffen werden. In der Praxis spielt dabei vor allem die ISO 27001 Norm eine wichtige Rolle. Die ISO-Norm 27018 ist in diesem Zusammenhang die „cloud-spezifischere" Norm[8]. Dabei darf jedoch nicht vergessen werden, dass Zertifikate bloß eine Indizwirkung haben. Tatsächlich sollte sich der Auftraggeber in regelmäßigen Abständen ein Bild über die tatsächlichen Gegebenheiten vor Ort verschaffen. Dieses Recht auf Auditierung sollte im Vertragswerk auch ausdrücklich geregelt werden.[9] In diesem Zusammenhang ist darauf hinzuweisen, dass der Auftraggeber für – wenn auch bloß fahrlässige – Verfehlungen „seines" Auftragnehmers (des Cloud-Diensteanbieters) haftbar gemacht werden kann.

---

[7] *Nehmer/Niecke*, IT-Sicherheit 6/2018, Sicherer Weg in die Business-Cloud, S 26 ff.
[8] *Tichy/Leissler/Woller*, Cloud Computing, S 21.
[9] Vgl Art 28 Abs 3 lit h DSGVO.

März 2019

5. Ausarbeitung des Cloud-Computing Vertrages

Erst wenn die unter Punkt 1 bis 4 genannten Punkte abgearbeitet sind, sollte die Vertragsgestaltung beginnen. Dass man sich hier nicht auf „Standardmuster" beziehen darf, soll hier nur der Vollständigkeit halber erwähnt werden. Typische Vertragsbestandteile eines Cloud-Computing Vertrages sind:

- Präambel;
- Definitionen;
- Leistungsbeschreibungen;
- Lizenzeinräumungen;
- Audit-Rechte;
- Entgeltregelungen;
- Gewährleistungsansprüche;
- Change-Request-Verfahren;
- Haftungsausschlüsse;
- Länderspezifische Regelungen;
- Gerichtsstandvereinbarungen;
- Laufzeiten;
- Datenschutzspezifische Regelungen;
- Kündigungsrechte.

6. Verhandlung des Cloud-Computing Vertrages

Bei standardisierten Cloud-Computing-Verträgen greift der Auftragnehmer in aller Regel auf sein Vertragsmuster zurück. Von diesem Muster abzuweichen, ist schwierig, aber nicht unmöglich. Wichtig ist daher, dass sich Ihr Unternehmen so spät wie möglich in ein „Abhängigkeitsverhältnis" zum Auftragnehmer begibt. Je „sicherer" sich der Auftragnehmer fühlt, desto weniger wird er von seiner Vertragsschablone abweichen.

7. Ausarbeitung und Verhandlung des Service Level Agreements

Sofern der Auftragnehmer neben der Infrastruktur auch die laufende Wartung für den Auftraggeber übernehmen soll (Software as a Service), sollte vor Vertragsabschluss eine Wartungsvereinbarung getroffen werden. In sogenannten Service Level Agreements sollte genau definiert werden, welche Leistung der Auftragnehmer schuldet. Wenn dieser nicht die vereinbarte „Uptime" erbringen kann, sollte dem Auftraggeber eine verschuldensunabhängige Pönale oder – in Praxis häufig – sogenannte „Service Credits" (also „Gutschriften") zustehen.

März 2019

8. Lizenzvereinbarungen

Die Software des Auftragnehmers ist in aller Regel urheberrechtlich geschützt.[10] Daher muss im Cloud-Computing-Vertrag genau geregelt sein, wer die Software in welchem Umfang und auf welche Weise verwerten darf. In der Folge sollte über Lizenzmanagementsysteme eine Übersicht der aktuell eingesetzten Softwarelizenzen gewahrt werden. Geschieht dies nicht, drohen im Falle von Lizenz-Audits durch den Auftragnehmer mitunter existenzbedrohende Nachzahlungsverpflichtungen aufgrund Unterlizenzierungen.

9. Auftragsverarbeitervertrag

Der Auftraggeber darf nur Auftragnehmer (Cloud-Diensteanbieter) mit der Verarbeitung personenbezogener Daten beauftragen, die angemessene Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten durchgeführt werden. Sofern der Auftragnehmer tatsächlich personenbezogene Daten im Auftrag des Auftraggebers verarbeitet (bspw speichert), muss ein Auftragsverarbeitervertrag nach Art 28 DSGVO abgeschlossen werden. Dies wird bei SaaS-Modellen („Software as a Service") regelmäßig erforderlich sein. Bei „bloßen" IaaS-Modellen („Infrastructure as a Service") bedarf es hingegen einer genauen Prüfung, ob tatsächlich ein Auftragsverarbeitervertrag abgeschlossen werden muss. Den Auftraggeber trifft bei seiner Auswahl des Auftragnehmers ein Auswahlverschulden. Daher wird er gut daran beraten sein, den Auftragnehmer regelmäßig vor Ort zu auditieren.

10. Internationaler Datentransfer

Im Zuge von Cloud-Computing-Projekten werden personenbezogen Daten regelmäßig in ein Drittland übermittelt. Ein Drittland ist ein Land außerhalb der EU (plus Lichtenstein, Norwegen, Island). Der europäische Gesetzgeber geht davon aus, dass in diesen Drittländern (unter anderem den USA) grundsätzlich kein angemessenes Datenschutzniveau[11] besteht. Aus diesem Grund muss sich der Auftraggeber fragen,(i) ob die Datenübermittlung in ein Drittland gerechtfertigt ist und bejahendenfalls,(ii) wie ein angemessenes Datenschutzniveau in diesem Drittland sichergestellt werden kann. Bei der Sicherstellung des angemessenen Datenschutzniveaus spielen in der Praxis Angemessenheitsbeschlüsse, Privacy-Shield-Zertifizierungen und Standarddatenschutzklauseln eine wichtige Rolle.

---

[10] § 40a UrhG.
[11] Vgl Art 44 ff DSGVO.

März 2019

Zur Kanzlei

Wir sind seit 1.1.2017 Ihre Experten für die Themen, die Unternehmen im 21. Jahrhundert bewegen: Datenschutzrecht, IT-Recht, E-Commerce-Recht, Arbeitsverfassungsrecht und Vertragsrecht

Zum Autor:

Dr. Tobias Tretzmüller, LL.M. ist Rechtsanwalt in ständiger Kooperation mit der Knyrim Trieb Rechtsanwälte OG, Wien. E-Mail: tt@kt.at. Er berät und vertritt Unternehmen in den Bereichen des IT-Softwarevertragsrecht, Datenschutzrechts, Urheberrechts, IT-Sicherheitsrechts und streitigen Behörden- und Zivilverfahren. Regelmäßige Vortrags- und Veröffentlichungstätigkeit (ua imh trainer of the year 2017 und 2018; Jahrbuch Datenschutzrecht 2017, ZIIR, Dako).