CHECKLISTE

Rechtsaspekte im Cloud-Computing

Das sollten Sie bei der Nutzung von Cloud-Dienstleistungen beachten.

Inhalt

Vieldimensionale Rechtsmaterie

Immer mehr kleine und mittlere Unternehmen (KMU) prüfen, ob sie Ressourcen aus der Cloud nutzen sollten. Im Cloud-Monitor 2020 der KPMG AG und Bitcom Research GmbH sagten 76 % Prozent der Befragten aus mittelständischen Unternehmen sowie Konzernmanager, dass sie bereits Services über das Netz einsetzen. Die Vorteile liegen auf der Hand: Die eigene IT spart Investitionen in Hardware und Sicherheit, externe Rechen- und Speicherkapazitäten lassen sich bei Bedarf jederzeit zukaufen. Vor allem Startup-Unternehmen verzichten bereits komplett auf die eigene IT und kaufen neben „Infrastructure as a Service" (IaaS = Rechner- und Server-Kapazitäten) auch „Plattform as a Service" (PaaS = Entwicklungsumgebung für Web-Applikationen). Aber vor allem „Software as a Service" (SaaS) erfreut sich immer größerer Beliebtheit bei KMU. Denn hier kommt neben dem Einsparpotenzial eigener IT-Hard- und Software auch noch der Aspekt hinzu, dass man bei SaaS auch den Pflege-, Wartungs- und Aktualisierungsaufwand auf den Anbieter verlagert und dieser für die Verfügbarkeit geradestehen muss.

Vor allem in der Public Cloud, also der Auslagerung oder Nutzung von SaaS an einen externen Anbieter, müssen Sie sich als CIO oder IT-Leiter mit zahlreichen juristischen Herausforderungen auseinandersetzen. Das beginnt schon mit der Frage, welche Art von Vertrag zustande kommt. Denn in der Regel scheinen Cloud-Verträge zunächst dem Mietvertragsrecht angelehnt, können aber auch Elemente anderer Vertragstypen enthalten. Diese typengemischten Verträge können im Detail sehr knifflig sein. Auch wenn bei einem SaaS-Cloud-Vertrag in der Regel das Mietvertragsrecht zur Anwendung kommt, kann dieser auch Merkmale des Dienst- oder Werkvertragsrechts aufweisen.

Von besonderer Beachtung sind für Sie als Verantwortlicher im Unternehmen Fragen der Datensicherheit und des Datenschutzes. Denn dafür muss immer derjenige geradestehen und haften, der die Daten erhebt und verarbeitet. In der Cloud aber liegen Daten bei einem externen Dienstleister und werden von diesem verarbeitet. Bei dieser Auftragsdatenverarbeitung wird es kompliziert. Hier sind sowohl nationale als auch europäische Gesetze zu beachten, deren Einhaltung immer der Nutzer der Cloud garantieren muss. Das Bundesdatenschutzgesetz erlaubt keine Delegation dieser Verantwortung.

Bei der Auswahl des Cloud-Anbieters müssen Sie deshalb darauf achten, dass dieser die nationalen Gesetze, Verordnungen und Empfehlungen beachtet und dies durch Zertifikate unabhängiger Prüforganisationen nachweisen kann. Darüber hinaus sollte der Provider eine Niederlassung mit einer Rechtsform nach nationalem Recht haben. Dies ist von Bedeutung, wenn es zu einer juristischen Auseinandersetzung kommen sollte. Achten Sie also im Vertrag darauf, welcher Gerichtsstand gilt.

In der Checkliste finden Sie Schritt für Schritt die wichtigen rechtlichen Aspekte, die Sie bei der Nutzung von Cloud-Dienstleistungen für SaaS beachten sollten.

Bestands- und Bedarfserhebung

Wie bei jedem IT-Projekt sollten Sie auch beim Cloud-Computing nichts überstürzen. Am Anfang steht, welche Anwendungen Sie aus der Cloud beziehen wollen und welche Daten dafür in die Cloud übertragen werden müssen. Sie stecken also zunächst die Rahmenbedingungen dafür ab, welche Leistungen Sie einkaufen, was Sie für die Nutzung vorbereiten und welche Voraussetzungen erfüllt sein müssen.

Für welche Abteilungen wollen Sie die Datenverarbeitung in die Cloud verlagern?	**Check**
Rufen Sie aus allen Abteilungen den Bedarf ab.	☐
Klären Sie dabei, auf welche Daten gemeinsam zugegriffen werden soll beispielsweise auf Kundendaten von Vertrieb, Rechnungswesen und Buchhaltung.	☐

Welche Daten wollen Sie in der Cloud beziehungsweise mit der SaaS-Anwendung verarbeiten?	**Check**
Kundendaten	☐
Mitarbeiterdaten	☐
Lieferantendaten	☐
Betriebliche Daten (Zahlungsströme, Lager & Logistik-Daten, Produktionssteuerung)	☐
Buchhaltungsdaten	☐
Steuerdaten	☐

Haben Ihre IT-Mitarbeiter die notwendigen Qualifikationen, Cloud-Dienste einzuführen und verfügen auch die Mitarbeiter, die mit der Cloud arbeiten, über ausreichende Fähigkeiten und Kenntnisse?	**Check**
Ermitteln Sie den Schulungsbedarf der IT-Mitarbeiter beispielsweise in folgenden Fachgebieten:	
1. Projektmanagement	☐
2. Technischer Support für Datenmigration	☐
3. Datenschutz und Compliance	☐
4. Datenbank-Administration	☐
5. Business Intelligence / -Analytics / Big Data	☐
6. Mobile Device Security	☐
7. Application Security	☐
8. Netzwerk Security	☐

Verfügt Ihr Unternehmen über eine schnelle und sichere Verbindung ins Internet?	Check
Mindestens 50 Mbit	☐

Haben Sie für die Mitarbeiter, die mit der Cloud-Anwendung arbeiten, eine sichere Authentifizierung eingerichtet?	Check
Multi-Authentifizierung für Geräte und Nutzer	☐
Sichere und regelmäßige neue Passwörter	☐
Schutz vor Passwort-Diebstahl	☐
Sitzungs-PINs	☐

Sind die Arbeitsplatzrechner, mit denen in der Cloud gearbeitet wird, vor dem Zugriff Unbefugter geschützt?	Check
Zutrittskontrolle für Gebäude und Büros	☐

Wie sichert die IT künftig die Daten, die in der Cloud verarbeitet werden, gegen Verlust ab?	Check
Redundantes Backup-System einrichten mit täglicher, wöchentlicher oder monatlicher Datensicherung	☐

Eine Unternehmens- und Buchhaltungslösung aus einer Hand schafft eine zentrale Quelle für Echtzeitinformationen!
Mehr erfahren

Rechtliche Rahmen-bedingungen

Je nachdem, welche Daten Sie verarbeiten, müssen Sie neben dem Bundesdatenschutzgesetz (BDSG) weitere Gesetze beachten.

1. **Für personengebundene Daten wie Name, Anschrift, Verdienst, Kontonummer oder auch Kaufhistorien müssen Sie sich mit §3 und §9 BDSG auseinandersetzen.**

2. **Einschlägig für die Auftragsdatenverarbeitung ist §11 BDSG.**

   - Personenbezogene Daten dürfen nur innerhalb der EU verarbeitet werden.
   - Die Datenbesitzer müssen in die Auftragsdatenverarbeitung einwilligen.
   - Auch bei der Auftragsdatenverarbeitung muss Ihr Unternehmen für die Einhaltung des Datenschutzes geradestehen.

3. **Neben dem BDSG müssen Sie auch die EU-Datenschutzgrundverordnung beachten, die in neuer Fassung seit Mai 2018 in Kraft getreten ist. Sie verschärft die Auflagen an Unternehmen, die Daten erheben und verarbeiten, und sieht erstmals drakonische Maßnahmen bei Verletzung des Datenschutzes vor.**

4. **Prüfen Sie die Bestimmungen Ihres Landesdatenschutzgesetzes.**

5. **Für Steuer- und Buchhaltungsdaten müssen Sie zudem die Bestimmungen des Bürgerlichen Gesetzbuches (BGB), Handelsgesetzbuches (HGB) sowie der Abgabenordnung (AO) beachten.**

   - Steuerdaten dürfen nur innerhalb des deutschen Hoheitsgebietes verarbeitet werden.

Sicherheitsstandards für Cloud- und SaaS-Anbieter

Der erste Schritt bei der Auswahl eines Cloud-Providers muss der Klärung dienen, ob dieser die Mindeststandards der Auftragsdatenverarbeitung erfüllt.

Liegt ein Zertifikat von einer unabhängigen deutschen Prüforganisation nach ISO 27001:2015 vor?	Check
Diese internationale Industrienorm stellt spezielle Anforderungen an die Einrichtung eines Informations-sicherheitsmanagementsystems. Sie enthält Bestimmungen für die Beurteilung und Behandlung von Sicherheitsrisiken.	☐

Erfüllt der Provider die Kriterien des IT-Grundschutz-Katalogs des Bundesamtes für Sicherheit in der Informationstechnik (BSI)?	Check
Der vom BSI entwickelte IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.	☐

Vertragsinhalte Cloud-Computing

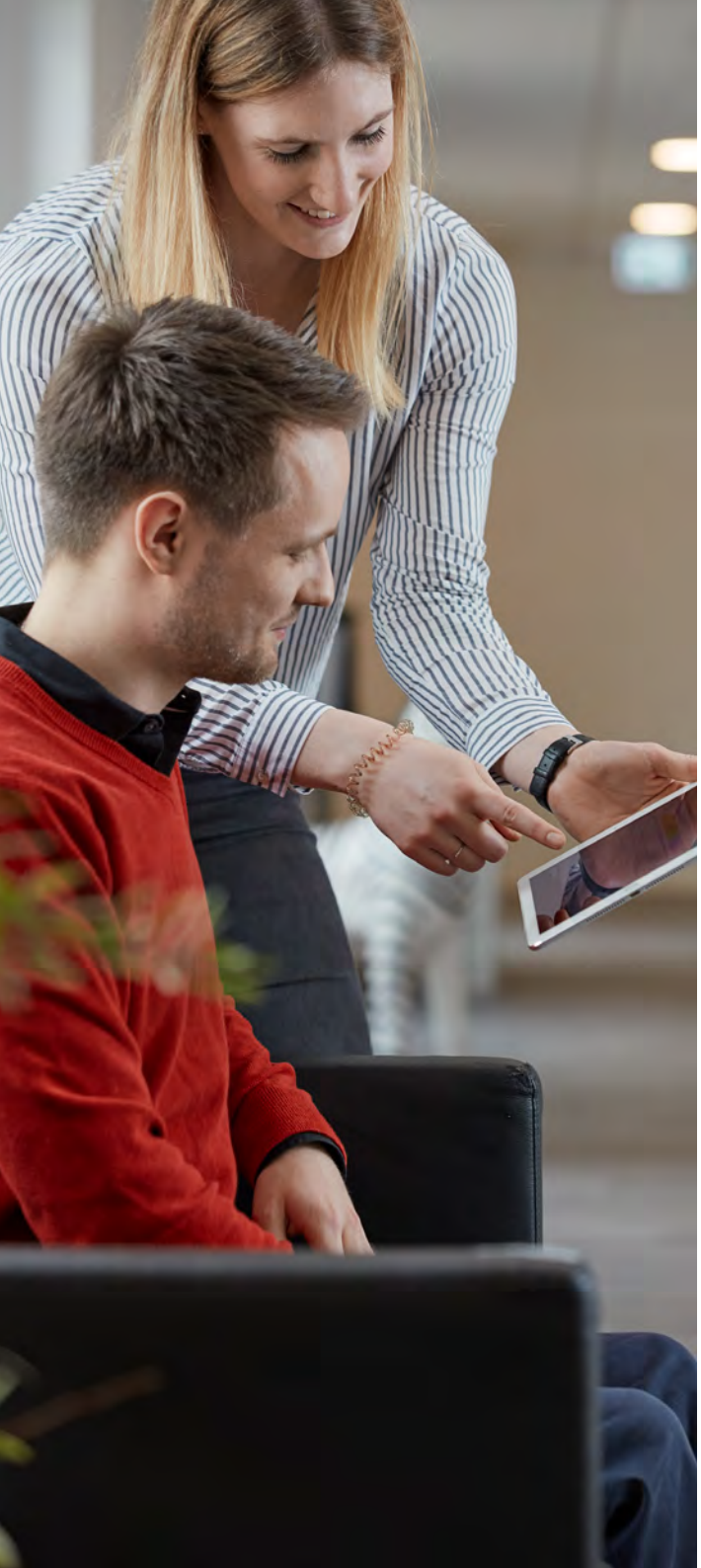
Wie die wenigsten KMU werden auch Sie vermutlich keinen Hausjuristen beschäftigen, der einen Cloud-Computing-Vertrag prüfen kann. Aber da die Entscheidung für eine Cloud-Anwendung sehr weitreichend ist, sollten Sie sich den Vertrag des Providers genau anschauen. Hilfreich dabei sind die Empfehlungen der „Artikel 29 Arbeitsgruppe" der Europäischen Kommission. Dieses unabhängige Beratergremium nach Artikel 29 der Europäischen Datenschutzrichtlinie hat Mindestanforderungen für die Auftragsdatenverarbeitung personenbezogener Daten in der Cloud zusammengestellt. In der Checkliste finden Sie die wichtigsten Prüfungskriterien, die in einem Vertrag geregelt sein sollten.

Organisatorische und technische Maßnahmen zum Datenschutz	Check
1. Der Cloud-Provider verpflichtet sich vertraglich auf Einhaltung der nationalen und europäischen Bestimmungen zum Datenschutz und zur sicheren Datenverarbeitung nach Maßgabe der Gesetze	☐
2. Der Provider ist vertraglich verpflichtet, angemessene technische und organisatorische Maßnahmen für die Datensicherheit zu ergreifen:	☐
- Physische Sicherheit des Rechenzentrums vor Brand, Einbruch, Elementarschäden, unterbrechungsfreie Stromversorgung, Klimatisierung	☐
- Sicherheit vor Cyberkriminellen durch Firewalls, Virenschutz, Beobachtung des Datenverkehrs und sofortige Intervention bei Angriffen	☐
- Transparente Informationen des Providers über seine Sicherheitsmaßnahmen	☐
- Informationen darüber, welche Vorkehrungen der Provider für die Hochverfügbarkeit, Integrität und Vertraulichkeit Ihrer Daten getroffen hat	☐
- Protokollierung aller Datenverarbeitungsvorgänge	☐
- Idealerweise Zertifizierung nach ISO 27001:2015 und BSI IT-Grundschutz-Katalog	☐

Umgang mit Subunternehmern	Check
Der Cloud-Provider verpflichtet sich,	
- alle beauftragten Subunternehmer (beispielsweise externe Dienstleister) zu benennen;	☐
- dass er weitere Subunternehmer (z.B. Rechenzentrumsbetreiber) nur mit Ihrer Zustimmung beauftragt;	☐
- Änderungen bei den Subunternehmen unaufgefordert bekanntzugeben;	☐
- Ihnen ein Sonderkündigungsrecht zuzugestehen, falls Sie mit einem Subunternehmen nicht einverstanden sind;	☐
- dass er mit allen Subunternehmen Datenschutz-Vereinbarungen mit gleichem Inhalt geschlossen hat, zu deren Einhaltung er sich Ihnen gegenüber verpflichtet hat;	☐
- dass Sie im Falle von Vertragsverletzungen diese direkt beim Subunternehmen geltend machen können.	☐

Vereinbarungen zum Serverstandort	Check
Der Cloud-Provider ist vertraglich verpflichtet, an welchem Ort er die Daten verarbeiten darf.	
- Bei personenbezogenen Daten ist er verpflichtet, sie nur innerhalb der EU zu verarbeiten und zu speichern.	☐
- Bei Buchhaltungs- und Steuerdaten ist er verpflichtet, die Daten innerhalb des Hoheitsgebietes der Bundesrepublik Deutschland zu verarbeiten und zu speichern.	☐

Sonstige Pflichten des Cloud-Providers	Check
Der Cloud-Anbieter verpflichtet sich,	
- dass seine Cloud-Anwendung eine Hochverfügbarkeit garantiert;	☐
- die vereinbarten Service Levels einzuhalten und bei Nichteinhaltung eine Vertragsstrafe zu akzeptieren;	☐
- dass er personenbezogene Daten nicht für eigene Zwecke nutzt;	☐
- dass Sie ihm Weisungen für die Datenverarbeitung geben dürfen;	☐
- dass Sie sich über die Einhaltung der vertraglichen Pflichten zur Datensicherheit beim Cloud-Anbieter vor Ort ein Bild machen dürfen;	☐
- dass er jederzeit auf Verlangen Datensätze auf Ihre Anforderung oder auf Bitten Ihrer Kunden sicher löscht;	☐
- dass er Sie informiert, wenn beispielsweise Steuer- oder Strafverfolgungsbehörden Auskunft über Ihre Daten verlangen und dass er rechtlich unzulässige Anfragen ablehnt;	☐
- dass er jede minimale Datenschutzverletzung Ihnen unverzüglich mitteilt;	☐
- dass er Ihre Daten sicher und unwiederbringlich auf Ihr Verlangen löscht;	☐
- dass er seine Mitarbeiter eine Vertraulichkeitsverpflichtung hat unterzeichnen lassen.	☐



Wenn Ihr Cloud-Provider zu allen diesen Prüfkriterien in seinem Vertragsentwurf klare Angaben macht beziehungsweise Vereinbarungen vorsieht, bleibt die Letztverantwortung dennoch immer bei Ihrem Unternehmen. Die Einhaltung des BDSG und der EU-DSGVO müssen immer Sie gegenüber den Datenei-gentümern garantieren können. Umso wichtiger ist es bei der Auswahl eines Cloud-Providers, dass er sich verpflichtet, stets auf der Höhe der technischen Entwicklung für die Sicherheit Ihrer Daten in der Cloud zu sorgen. Und weil die Cloud-Anbieter wissen, dass die Kunden heute sehr sensibel sind, haben Anbieter mit einem eingetragenen Firmensitz in Deutschland auch bisher keine Schwächen gezeigt. Mit dem richtigen Anbieter steht einem erfolgreichen Wechsel in die Cloud also nichts im Wege.

Sie möchten mehr über die Buchhaltungsangebote für Kleinunternehmer von Sage erfahren, mit denen Sie Ihren Cashflow im Griff behalten? Dann besuchen Sie:
www.sage.com/de-de/cp/buchhaltung

Sage GmbH
Franklinstraße 61-63
D-60486 Frankfurt am Main

T: +49 69 50007-6300
E-Mail: info@sage.de

www.sage.com