


## Anforderungen an Cloud-Computing

Was ist vor dem Einsatz von Cloud-Computing aus datenschutzrechtlicher Sicht zu beachten? Die nachfolgende Checkliste soll Ihnen eine erste Orientierung ermöglichen.

*Hinweis: Es handelt sich nur um allgemeine Aussagen, die eine erste Einschätzung ermöglichen sollen. Bitte wenden Sie sich im Einzelfall an Ihren Datenschutzbeauftragten.*

<b>1. Sollen Daten mit Personenbezug in der Cloud gespeichert werden?</b>	
<p><b>Ja,</b> es werden beispielsweise Kunden- oder Mitarbeiterdaten gespeichert – oder auch interne Log-/Protokolldateien, die Rückschlüsse auf Mitarbeiter zulassen.</p> <p>Die Datenschutzregeln sind zu beachten. Prüfen Sie weiter.</p> <p style="text-align: center;">↓</p>	<p><b>Nein</b></p> <p>Das Datenschutzrecht ist nicht anwendbar; Datenschutzanforderungen sind nicht zu beachten.</p> <p style="text-align: center;">Die Prüfung ist beendet.</p> <p style="text-align: center;">_____</p>
<b>2. Hat der Cloud-Anbieter seinen Sitz in der EU oder dem EWR?</b>	
<p style="text-align: center;">„Drittstaaten“ oder</p> <p style="text-align: center;">↓</p> <p><b>Sitz außerhalb von EU/EWR:</b></p> <p>Wenn der Cloud-Anbieter in einem Drittstaat sitzt, prüfen Sie mit Frage 3 weiter.</p> <p style="text-align: center;">↓</p> <p style="text-align: center;">↓</p>	<div style="text-align: center;">  </div> <p><b>Sitz innerhalb von EU/EWR:</b></p> <p>Es ist mit dem Cloud-Anbieter ein Vertrag zur <b>Auftragsdatenverarbeitung nach § 11 BDSG</b> abzuschließen.</p> <p>Weitere Hinweise finden Sie im Praxisleitfaden zur Auftragsdatenverarbeitung.</p> <p>(Hinweis: Der Cloud-Anbieter muss seinerseits mit allen Subunternehmern (z.B. Rechenzentren) ebenfalls Verträge zur Auftragsdatenverarbeitung abschließen; sitzen seine Subunternehmer außerhalb von EU/EWR, sind Verträge entsprechend § 11 BDSG abzuschließen)</p> <p style="text-align: center;">Die Prüfung ist beendet.</p> <p style="text-align: center;">_____</p>

<b>3.</b>	<b>Sollen „besondere Arten von personenbezogenen Daten“ in der Cloud gespeichert werden?</b>		
	<p>Darunter fallen Angaben über die Gesundheit, das Sexuelleben, die rassische/ethnische Herkunft, politische Meinungen, religiöse/philosophische Überzeugungen und Gewerkschaftszugehörigkeit.</p>		
	↓		↓
	<p><b>Nein,</b></p> <p>es werden zwar personenbezogene Daten in der Cloud gespeichert oder verarbeitet, aber nicht die oben genannten „besonderen Arten“.</p> <p>Prüfen Sie weiter.</p>	<p><b>Ja</b></p> <p>Es muss eine <b>explizite Einwilligung</b> der Betroffenen in die Verarbeitung dieser besonderen Daten in der Cloud eingeholt werden. Ansonsten ist die Cloud-Verarbeitung in der Regel nicht zulässig.</p>	
	↓		↓
<b>4.</b>	<b>Liegt eine zusätzliche Rechtsgrundlage für eine Datenübermittlung an eine Stelle in einen Drittstaat vor?</b>		
	<p>In Betracht kommen hier mehrere Möglichkeiten. Mindestens eine davon muss vorliegen:</p>		
	↓	↓	↓
	<p><b>EU-Standardvertrag für Auftragsverarbeiter:</b></p> <p>Datenexporteur und Datenimporteur haben einen Vertrag mit dem Wortlaut der EU-Standardvertragsklauseln für Auftragsverarbeiter abgeschlossen (Beschluss der EU-Kommission, Az. K(2010)593 endgültig vom 5.2.2010)</p>	<p><b>Safe Harbor (USA):</b></p> <p>Der Datenimporteur ist dem "Safe Harbor"-Abkommen beigetreten (nur bei Importeur mit Sitz in den USA möglich).</p> <p>Es muss hier zusätzlich geklärt werden:</p> <ul style="list-style-type: none"> <li>a) ob die Selbstzertifizierung das Cloud-Computing erfasst</li> <li>b) ob die Selbstzertifizierung noch gültig ist (vgl. <a href="http://export.gov/safeharbor/">http://export.gov/safeharbor/</a>)</li> <li>c) ob ein Nachweis (Bestätigung) durch den US-Cloud-Anbieter vorliegt, dass und wie er seine Informationspflichten gegenüber den Betroffenen wahrnimmt</li> </ul> <p>Diese Prüfung ist zu dokumentieren (z.B. per Protokoll).</p>	<p><b>Andere Rechtsgrundlage:</b></p> <p>vgl. Hinweise im Praxisleitfaden zum Auslandstransfer</p>
	↓		↓
	↓	↓	↓

**5. Es muss ein zusätzlicher Vertrag zur Auftragsdatenverarbeitung abgeschlossen werden**

Sie müssen einen weiteren, zusätzlichen Vertrag mit dem Cloud-Anbieter abschließen, der den inhaltlichen Anforderungen des § 11 BDSG entspricht.

Unter anderem muss der Vertrag folgende Inhalte besitzen:

- Bestimmung und Zweck der Datenverarbeitung
- Nennung aller möglichen Orte der Datenverarbeitungen (v.a. Rechenzentren)
- Nachverfolgbarkeit der Datenverarbeitung
- Vereinbarung von technischen und organisatorischen Maßnahmen, die der Cloud-Anbieter und ggf. Subunternehmer einhalten müssen (z.B. Zugangsregeln für Mitarbeiter und Subunternehmer)
- Übergabe von Kopien der Prüfbescheinigungen bzw. Zertifikate
- Regeln für die Einschaltung von Subunternehmern:
  - grundsätzlich ist eine Zustimmung des Kunden erforderlich, wobei auch eine Liste aller Unterauftragnehmer mit Standorten vereinbart werden kann
  - Cloud-Anbieter und Subunternehmer müssen einen Vertrag schließen, der dem Kunden Ansprüche bei Verstößen gewährt
- Löschungstechniken für Kunden
- Benachrichtigung über Auskunftersuchen von Sicherheitsbehörden