Checkliste Cloud Computing

in Anlehnung an "Opinion 5/2012 on Cloud Computing" der Artikel 29 Arbeitsgruppe

Die Checkliste fast datenschutzrechtliche Vorgaben zusammen, welche die Artikel 29 Arbeitsgruppe in ihrer "Opinion 5/2012 on Cloud Computing" formuliert hat. Die Checkliste kann Cloud-Kunden und Cloud-Anbietern gut als erste Orientierung dienen. Sie erhebt keinen Anspruch auf Vollständigkeit.

A) Subunternehmer

1. **Zustimmungsvorbehalt.** Ist vertraglich geregelt, dass der Cloud-Anbieter Subunternehmer nur mit Zustimmung des Kunden einschalten darf?
2. **Transparenz.** Werden alle Subunternehmer einschließlich der Orte der Datenverarbeitung im Vertrag benannt?
3. **Anzeigepflicht.** Ist der Cloud-Anbieter verpflichtet, spätere Änderungen von Subunternehmern dem Kunden anzuzeigen?
4. **Widerspruchs-/Kündigungsrecht.** Hat der Kunde ein Widerspruchsrecht oder das Recht, den Vertrag zu kündigen, wenn er mit einem Subunternehmer nicht einverstanden ist?
5. **Verträge mit Subunternehmern.** Hat der Cloud-Anbieter mit seinen Subunternehmern Verträge geschlossen, durch die dem Subunternehmer die Datenschutz-Verpflichtungen des Cloud-Anbieters entsprechend auferlegt werden?
6. **Direkte Ansprüche.** Ist sichergestellt, dass der Kunde im Falle von Vertragsverletzungen Ansprüche direkt gegen Subunternehmer geltend machen kann?

B) Technische und Organisatorische Maßnahmen

1. **Vertragliche Pflicht.** Wird der Cloud-Anbieter zu angemessenen technischen und organisatorischen Maßnahmen zur Datensicherheit verpflichtet?
2. **Transparenz.** Hat der Cloud-Anbieter *aussagekräftige* Informationen über die technischen und organisatorischen Maßnahmen zum Datenschutz bereitgestellt?
3. **Cloud spezifische Risiken.** Umfassen die technischen und organisatorischen Maßnahmen zum Datenschutz angemessene Mechanismen, um die spezifischen Risiken von Cloud Computing zu reduzieren? Dies gilt insbesondere in Bezug auf die Verfügbarkeit, Integrität und Vertraulichkeit der Daten sowie den Zweckbindungsgrundsatz, die Durchsetzbarkeit von Betroffenenrechten und die Probabilität der Daten.
4. **Protokollierung.** Ist der Cloud-Anbieter zur Protokollierung (Logging) relevanter Datenverarbeitungsvorgänge verpflichtet?

C) Weitere vertragliche Vereinbarungen

1. **Zweckbindung.** Ist vertraglich festgelegt, dass der Cloud-Anbieter personenbezogene Daten des Kunden nicht für eigene wirtschaftliche Zwecke oder andere Zwecke, als die Erbringung des Cloud Services nutzen darf?
2. **Weisungen.** Ist festgelegt, in welchem Umfang der Kunde den Cloud-Anbieter Weisungen zur Datenverarbeitung erteilen kann?
3. **Grenzüberschreitende Transfers.** Ist gewährleistet, dass der Cloud-Anbieter (oder dessen Subunternehmer) in einem Drittland ein angemessenes Datenschutzniveau sicherstellt (z.B. Safe Harbor Zertifizierung, Abschluss von EU Standardvertragsklauseln, Binding Corporate Rules)?
4. **Audit-Rechte.** Hat der Kunde das Recht, die Datenverarbeitungsvorgänge beim Cloud-Anbieter und dessen Subunternehmer zu kontrollieren oder erhält der Kunde Kopien von entsprechenden Berichten oder Zertifizierungen?
5. **Unterstützungspflicht.** Ist der Cloud-Anbieter zur Unterstützung verpflichtet im Zusammenhang mit der Ausübung von Kontrollrechten des Kunden und Datenschutzrechten von Betroffenen (z.B. auf Auskunft, Löschung, Berichtigung)?
6. **Meldung von Auskunftsverlangen.** Wird der Cloud-Anbieter verpflichtet, verbindliche Auskunftsverlangen von Strafverfolgungsbehörden dem Kunden - soweit zulässig - mitzuteilen?
7. **Zurückweisung von Auskunftsverlangen.** Ist der Cloud-Anbieter verpflichtet, rechtlich nicht-bindende Auskunftsverlangen von Strafverfolgungsbehörden zurückzuweisen?
8. **Meldung von Datenschutzverletzungen.** Ist der Cloud-Anbieter verpflichtet, Datenschutzverletzungen in Bezug auf Daten des Kunden dem Kunden mitzuteilen?
9. **Löschung.** Ist vertraglich geregelt, wie sichergestellt wird, dass nicht mehr benötigte Daten gelöscht werden und wie eine sichere Löschung erfolgt (z.B. Zerstörung von Datenträgern, Überschreiben von Daten)?
10. **Service Levels.** Sind messbare Service Levels und die Rechtsfolgen einer Vertragsverletzung (z.B. Vertragsstrafe) geregelt?
11. **Vertraulichkeit.** Wir der Cloud-Anbieter verpflichtet, seine Mitarbeiter zur Vertraulichkeit zu verpflichten?

Anmerkung

Die Angemessenheit technischer und organisatorischer Maßnahme kann auch durch Vorlage von Audit-Berichten oder Zertifizierungen sichergestellt werden. Dabei ist zu beachten:

- Der Audit/die Zertifizierung sollte von einer anerkannten **Stelle** erfolgen
- Der Audit/die Zertifizierung sollte nach einem anerkannten **Standard** erfolgen, der auch die Anforderungen gemäß Opinion 5/2012 abdeckt
- Der Audit/die Zertifizierung sollte nicht nur technische Maßnahmen, sondern auch **organisatorische Maßnahmen** abdecken (z.B. Richtlinien und Verfahren zu Backups oder Zugangsberechtigungen)
- Es ist eine **Kopie** des Zertifikats oder des Audit-Berichtes vorzulegen
- Anmerkung: Daneben ist bei Audits und Zertifikaten zu prüfen, ob alle für den Cloud-Dienst **relevanten Bereiche abdeckt** sind (Rechenzentren, Organisationseinheiten, Hard-/Software, Subunternehmer, etc.).