**CHECKLISTE: Datenschutzaspekte bei Clouddiensten**

**Aspekt**

**Hintergrund**

**Geprüft und in Ordnung?**

Wie stellt sich der Ge- samtprozess der Daten- verarbeitung dar?

* Sie brauchen ein umfassendes Bild der Verarbeitung personenbezogener Daten. Lassen Sie sich die Sache im Detail erklären und fordern Sie Konzepte, Übersichten und Diagramme an.
* Klären Sie auch das Drumherum im Unternehmen, etwa Verantwortlichkeiten oder Ent- scheidungsträger bezüglich des Vorgehens. Manchmal ist es auch wichtig, den „Sponsor“ zu kennen, weil oftmals hier die letzte Entscheidungsinstanz zu finden ist.
* Prüfen Sie auch, inwieweit es tatsächlich um personenbezogene Daten geht.

q Ja q Nein

Was hat man mit den per- sonenbezogenen Daten bzw. mit der Verarbeitung vor?

* Hinterfragen Sie die Motivation, warum man etwas an einer Verarbeitung ändern möchte oder warum diese bei einem Dienstleister oder in der Cloud stattfinden soll.
* Orientieren Sie sich unter Datenschutzaspekten immer an dieser grundsätzlichen Frage: Wer will welche personenbezogenen Daten zu welchem Zweck wie und wo verarbeiten?
* Besprechen Sie auch das Thema Rechtsgrundlage. Hierzu müssen Sie wissen, was man konkret vorhat. Bei einer „normalen“ Auftragsverarbeitung bedarf es keiner weiteren Rechtsgrundlage. Die Sache kann anders aussehen, wenn der Auftragsverarbeiter auch eigene Zwecke verfolgt, etwa ein KI-Training mit Kundendaten.

q Ja q Nein

Wer ist heute daran be- teiligt und wer soll es zukünftig sein?

* Lassen Sie sich am besten alle beteiligten Stellen im Unternehmen nennen. Meist ist das eben nicht nur die IT-Abteilung.
* Durch eine Verlagerung zu einem Auftragsverarbeiter oder in die Cloud können sich die Beteiligten gegenüber der heutigen Situation ändern. Klären Sie, inwieweit das der Fall ist.

q Ja q Nein

Welche datenschutzrecht- liche Rolle haben die jeweiligen Beteiligten?

* Identifizieren Sie mit den Kollegen, wer welche Funktion oder Rolle bei einer Verarbeitung übernimmt.
* Bedenken Sie auch: Geht es um eine Verarbeitung im Konzern, ist das wegen dieses „Kons- trukts“ nicht automatisch zulässig. Auch hier müssen die jeweiligen Rollen geprüft und die sich daraus ergebenden Verantwortlichkeiten bewertet werden.

q Ja q Nein

Wo sind die Beteiligten ansässig und welchem Recht unterliegen sie?

* Lassen Sie sich genau nennen, mit wem Ihr Unternehmen zusammenarbeiten will.
* Der Sitz und das relevante Recht können von Bedeutung sein, wenn der Dienstleister bzw. Anbieter in einem Drittstaat ohne anerkanntes Datenschutzniveau ansässig ist. Ggf. muss hier aufwendig für ein angemessenes Datenschutzniveau gesorgt werden. Das kann man- chen Anbieter schnell weniger interessant werden lassen.

q Ja q Nein

**CHECKLISTE: Datenschutzaspekte bei Clouddiensten**

Wo findet die Verarbeitung der personenbezogenen Daten statt?

* Der Ort der Verarbeitung kann von erheblicher Bedeutung sein. Denn das muss nicht auto- matisch der Hauptsitz des Dienstleisters oder Anbieters sein. Eventuell findet die Verarbei- tung in der EU statt, obwohl der Anbieter außerhalb der EU ansässig ist.
* Hinterfragen Sie, ob tatsächlich die ganze Verarbeitung an einem Standort stattfindet. Ggf. kommen Subdienstleister zum Einsatz, die wiederum anderswo ansässig sein können. Das kann die Sache unter Datenschutzaspekten schwierig machen.

q Ja q Nein

Welche Dienstleister oder Anbieter kommen in Be- tracht?

* Gerade im Zusammenhang mit der Auftragsverarbeitung muss Ihr Unternehmen beachten: Der Billigste ist nicht immer der Beste.
* Klären Sie, welche Dienstleister in Betracht gezogen wurden.

q Ja q Nein

Warum ist der ausge- wählte Dienstleister bzw. Anbieter im Datenschutz als fähig und zuverlässig anzusehen?

* Das zielt darauf ab, dass Art. 28 DSGVO Ihrem Unternehmen auferlegt, nur mit qualifizierten Auftragsverarbeitern zu arbeiten. Die müssen hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO stattfindet.
* Fordern Sie entsprechende Bewertungen ein. Gibt es diese nicht, sollten diese erstellt wer- den. Schließlich ist aufgrund der bestehenden Rechenschaftspflicht eine Nachweisbarkeit unerlässlich.

q Ja q Nein

Wie steht es um die Si- cherheit der Verarbeitung bzw. der Daten?

* Lassen Sie sich die Maßnahmen des Dienstleisters bzw. des Anbieters erläutern.
* Fordern Sie Datenschutzkonzepte oder Zertifizierungen an. Prüfen Sie bei Zertifizierungen, was konkret zertifiziert wurde, wer zertifiziert hat und ob die Zertifizierung noch gültig ist.
* Denken Sie auch an den Schutz drum herum. So z. B. für die Frage, wie die Daten zum Dienstleister kommen und wie Daten abgesichert werden, etwa durch ein Back-up.

q Ja q Nein

Gibt es ein Datenschutz- niveau, das für unsere Verarbeitung angemessen ist?

* Die (Standard-)Schutzmaßnahmen des Dienstleisters bzw. des Anbieters können auf dem Papier super klingen. Doch sie müssen ganz konkret zur Schutzwürdigkeit und zum Schutz- bedarf Ihres Unternehmens und dessen Verarbeitung passen.
* Die Risikoanalyse Ihres Unternehmens muss Maßstab für die Bewertung sein. Aussagen aus „Hochglanzbroschüren“ helfen nicht. Ihr Unternehmen ist und bleibt für die Verarbei- tung verantwortlich.

q Ja q Nein

Sind kritische oder proble- matische Subdienstleister im Einsatz?

* Gibt es diese angeblich nicht, sollten Sie genauer hinschauen. Meist können Dienstleister oder Anbieter die angebotene Leistung nicht ohne weitere Dienstleister erbringen. Haken Sie bezüglich einer Liste nach. Intransparenz kann zum großen Problem werden.
* Gerade bei Subdienstleistern sollte auch unter dem Aspekt „Konkurrenz“ genau geprüft werden. Ein Konkurrent hätte ggf. Einblick in die Geschäftstätigkeit Ihres Unternehmens, selbst wenn Daten nicht vereinbarungswidrig verarbeitet werden.

q Ja q Nein

Wie wird der Datenschutz vertraglich geregelt?

* Klären Sie, inwieweit es eine Vereinbarung geben soll und ob etwas verhandelbar ist. Läuft die Sache nach dem Motto „Friss oder stirb“ und kann Ihr Unternehmen nicht mitreden, sollten die entsprechenden Risiken bewertet werden.
* Prüfen Sie, inwieweit die Vereinbarung zu den tatsächlichen Rollen der Beteiligten passt. Wird die falsche Vereinbarung geschlossen, kann Ärger vorprogrammiert sein, etwa auch mit der Datenschutzaufsicht.
* Achten Sie auch auf das vereinbarte Recht. Zwar wird die Anwendung der DSGVO meist kein Thema sein. Anders kann es für die sonstigen Rahmenbedingungen aussehen.

q Ja q Nein

Was passiert, wenn der Dienstleister oder die Cloud ausfällt?

* Hier sollten Sie das Thema „Business Continuity Management“ hinterfragen. Besprechen Sie, wie sichergestellt wird, dass man auch bei Problemen oder dem Ausfall des Dienstleis- ters bzw. Anbieters weiterarbeiten kann. Gibt es keine Überlegungen, kann das die Existenz des Unternehmens bedrohen.
* Klären Sie zudem, auf welche Zwischen- und Notfälle man sich vorbereitet. Auch eine ausgefallene Internetverbindung kann zum Problem werden, wenn der Dienstleister oder Anbieter nicht mehr erreichbar ist.

q Ja q Nein

Können wir schnell und unproblematisch Betroffe- nenrechte erfüllen?

* Ist Ihr Unternehmen Verantwortlicher, muss es den entsprechenden Verpflichtungen nachkommen können, und zwar grundsätzlich unverzüglich. Dabei muss ggf. auch der Dienstleister oder Anbieter unterstützen. Macht er das nicht, kann Ihr Unternehmen seine Pflichten nicht erfüllen. Ärger ist dann vorprogrammiert.
* Haben Sie auch ein Auge auf den Umfang und eventuelle Kosten einer Unterstützung durch den Dienstleister. Ggf. können hier im Vertrag erhebliche Risiken lauern.

q Ja q Nein

Wie soll die Einhaltung der Datenschutzstan- dards beim Dienstleister bzw. Anbieter überwacht werden?

* Wie detailliert man prüft, hängt insbesondere von der Schutzwürdigkeit der Daten ab. Ggf. reichen Zusicherungen aus. Unter Umständen ist jedoch eine Überprüfung der Schutzmaß- nahmen vor Ort unerlässlich.
* Lassen Sie sich die entsprechenden Planungen für Prüfungen vorlegen. Dabei muss den Risiken angemessen Rechnung getragen werden.

q Ja q Nein