Cloud als IT- und Datenschutz-Thema:

Datenschutzrechtliche Überlegung zur Cloud-Speicherung, zum Cloud-Computing.

Seit ein paar Jahren gehört die Cloud, also die „Daten-Wolke“, zum EDV-Vokabular. Viele sind noch skeptisch, aber immer mehr nutzen die Cloud. Die Spieler auf diesem Markt sind gute Bekannte. Google Drive, Dropbox, Microsoft Onedrive, Apple iCloud usw.
Doch was sagt die DSGVO dazu?

Hintergrund: Unter dem Begriff **Cloud-Speicherung** versteht man, dass die Daten nicht mehr auf einem lokalen Rechner gespeichert sind, sondern irgendwo in die Wolke, also die Weiten des Internets, ausgelagert werden. Dadurch ist es möglich, die Daten von überall abzurufen. Wo die Daten lagern, auf wie vielen Rechnern sie gespeichert sind, welche (Urheber-)Rechte man damit womöglich abgibt, damit hat sich wohl bis zur DSGVO kaum jemand näher beschäftigt.

Dazu kommt, dass Software-Hersteller auch **Cloud-Computing** anbieten. D.h. das gewünschte Programm – etwa Office 365 – ist nicht mehr lokal gespeichert, sondern ebenfalls in der Cloud. Auch hier bedenkt wohl kaum jemand, dass z.B. durch das Schreiben einer Bestellbestätigung über ein Online-Office-Paket personenbezogene Daten auf Server – womöglich in die USA - transferiert werden.

Da viele dieser **technischen Möglichkeiten** sukzessive die Privatsphäre der Menschen einschränken können, wird hier die DSGVO besonders greifen. Daher sollte man als vorsichtiger Unternehmer auf diesen Bereich genau hinschauen.

Welche Vorteile/Gefahren bestehen bei Cloud-Nutzung?

Die **Vorteile** einer Online-Speicherung liegen klar auf der Hand. Sollte ein Hochwasser oder Feuer Ihr Büro und die EDV-Infrastruktur zerstören, liegen die Daten auf Servern in der Wolke und helfen beim Wiederherstellen. Auch können Vielreisende von überall auf die Daten zugreifen. Die Vorteile von Online-Software – ständig die aktuellste Software – sind den meisten nicht wirklich greifbar und daher bietet Microsoft neben der monatlichen Miete im heurigen Jahr das Office-Paket auch wieder als normale PC-Version an.

Die **Gefahren** sind vielfältiger. Ein paar Ideen dazu.

Der Cloud-Anbieter verschwindet (Konkurs usw.).
Der Cloud-Anbieter lässt sich (Urheber-)Rechte an den Daten einräumen (Kleingedrucktes lesen).
Ihre Daten gehen verloren (technische Probleme usw.). Wer haftet wofür?
Hacker erhalten Zugriff auf Ihre Daten, was oftmals unbemerkt bleibt. Verändern sie, stehlen sie, usw.
Die Cloud oder der Softwaredienst sind wegen technischer Schwierigkeiten nicht erreichbar.

Für die DSGVO relevant: WO liegen die Daten?

Die Frage nach dem WO ist relevant für die Antwort, ob Sie z.B. personenbezogene Daten in Cloud-Systemen speichern dürfen oder E-Mail-Server/Newsletter-Server etc. nutzen dürfen.

Bekanntlich regelt die DSGVO, wann Sie welche Daten speichern dürfen und unter welchen Bedingungen Sie diese weitergeben dürfen, löschen müssen etc. Und bei all den oben geschilderten Punkten geben Sie Daten bewusst oder nicht bewusst an externe Server weiter.

Einfache Antwort: Bei europäischen Anbietern, etwa einer **Cloud:** Ja.
Bei **US-Cloud-Anbietern** ist Vorsicht geboten, denn dort gelten Datenschutz-Regeln, die mit den unseren nicht vergleichbar sind. Daher gilt für europäische Daten, die auf US-Servern liegen, **fast kein Datenschutz.** Folge: Amerikanische Server gelten aus Sicht der DSGVO grundsätzlich als nicht sicher.

Zwar hat die EU mit den USA ein **Privacy Shield-** Abkommen geschlossen (**EU-US-Datenschutzschild**). Das ist ein Abkommen, in dem die US-Regierung gewisse Zusicherungen hinsichtlich des Datenschutzrechts gemacht hat. Das war nötig, nachdem der Europäische Gerichtshof das davor bestehende **Safe Harbor-Abkommen** (nach der Klage des österreichischen Datenschützers Max Schrems gegen Facebook) aufgehoben hatte.

Es gibt nach wie vor heftige Kritik von Datenschützern am Privacy Shield-Abkommen, aber es scheint zumindest eine „Grundabsicherung" der Daten zu garantieren. Daher sollte man **nachsehen, ob sich der gewünschte Lieferant dem Privacy Shield unterwirft.** Falls nicht, müssen Sie die betreffenden Firmen anschreiben und einen schriftlichen Vertrag bezüglich DSGVO-konformen Handelns (auf Englisch: GDPR-compliant; GDPR steht für General Data Protection Regulation) anfordern. Kommt darauf keine Antwort, dann besser Hände weg!

Ob jemand das Privacy Shield akzeptiert hat, kann man hier prüfen:
https://www.privacyshield.gov/welcome

Was rät die Datenschutzbehörde?

Leider haben wir bei unserer Recherche weder auf der Homepage der österreichischen Datenschutzbehörde noch auf jenen einiger deutschen Bundesländer **einen Ratschlag betreffend Cloud-Nutzung gefunden.**

Aus den obigen Problematiken könnte man zur Risikovermeidung u.a. Folgendes versuchen:

- **Europäische Anbieter anstatt US-Anbieter** (auch wenn diese eventuell das Privacy Shield-Abkommen akzeptiert haben. Grund: Datenschützer hoffen darauf, dass der Europäische Gerichtshof auch das Privacy Shield-Abkommen aufheben wird und dann hätten wir wieder Probleme aufgrund DSGVO).

- Wenn doch ein US-Anbieter gewählt wird, dann die Bestätigung, dass Privacy Shield eingehalten wird, anfordern oder von der Homepage des Anbieters herunter laden.

- Mit dem Anbieter sind alle „Formvorschriften" vertraglich zu regeln, die die DSGVO vorsehen. Etwa einen **Auftragsverarbeitervertrag** abschließen (damit wird die DSGVO-konforme Behandlung der Daten und Geheimhaltung geregelt). Die **TOMs** (technischen und organisatorischen Maßnahmen) ebenso definieren wie **Dokumentations- und Informationspflichten** (etwa Meldung binnen 72 Stunden nach einem Hackerangriff an die Datenschutzbehörde nötig). Dabei sollte man sich die Lagerung in einer europäischen Cloud, auf europäischen Servern etc. bestätigen lassen. Ergänzen Sie Ihre **eigene Datenschutzerklärung** um diese Cloud-Nutzung usw.

- **Trotzdem: Kleingedrucktes genau lesen! Was bekomme ich, was nicht?**
Wer haftet, wer nicht? Wenn Sie etwa die Nutzungsbedingungen von Apple iCloud studieren (hier klicken…), so steht dort, **dass Apple für nichts garantiert oder haftet:**

Apple wird den Dienst mit angemessener Sorgfalt und Fachkenntnis erbringen, aber SOWEIT NACH DEN ANWENDBAREN GESETZEN ZULÄSSIG, GARANTIERT APPLE NACH MASSGABE DER BEDINGUNGEN DIESER VEREINBARUNG NICHT, DASS DIE INHALTE, DIE DU MÖGLICHERWEISE ÜBER DEN DIENST SPEICHERST ODER AUF DIE DU MÖGLICHERWEISE MITHILFE DES DIENSTES ZUGREIFST, NICHT VERSEHENTLICH BESCHÄDIGT ODER VERFÄLSCHT WERDEN, VERLOREN GEHEN ODER GELÖSCHT WERDEN. APPLE IST AUSSERDEM NICHT VERANTWORTLICH, SOLLTE ES ZU SOLCHEN SCHÄDEN, VERFÄLSCHUNGEN, VERLUSTEN ODER LÖSCHUNGEN KOMMEN.

Noch ein Hinweis zum „Kleingedruckten“:
Die dauernden Einwilligungserklärungen, die z.B. bei Google Chrome etc. aufpoppen, und die man vor der Nutzung des Browsers anklicken muss, sollte man wirklich genau lesen, weil man damit u.U. zu mehr zustimmt, als man zuvor schon erlaubt hat.
Leider hat kaum jemand so viel Zeit, um sich das genau durchzulesen. Daher klickt man oft auf „Akzeptieren“, um weiterarbeiten zu können. Was möglicherweise auch die Absicht ist.

- **Verschlüsselung, VPN-Tunnel**

Die Übertragung von und zur Cloud sollte immer verschlüsselt erfolgen, um die Sicherheit zu erhöhen. Andernfalls kann der Cloud-Anbieter Ihre Daten entschlüsseln, was gerade bei US-Unternehmen heikel ist. Bekanntlich hat Edward Snowden aufgedeckt, dass US-Behörden systematisch personenbezogene Daten absaugen. Auch die Nutzung eines VPN-Tunnels (eine Art abgesicherte Leitung) kann die Sicherheit erhöhen.

Resümee: Die technischen Möglichkeiten sind enorm und bieten sicherlich für zahlreiche Nutzer Vorteile. Doch aus (datenschutz-)rechtlicher Sicht ist hier nach wie vor Vorsicht geboten. Auch weil noch keine Empfehlung von Behördenseite oder Urteile zu diesem Bereich vorliegen. Möchten Sie auf Nummer sicher gehen, denken Sie an das Grundprinzip der DSGVO: So viele Daten wie unbedingt nötig, so wenige Daten wie möglich.

Quellen: Das österreichische Versicherungsvermittlerrecht, 10. Aktualisierung mit großem Update zur DSGVO-Umsetzung, Mag. Stephan Novotny (Rechtsanwalt mit Spezialgebiet Versicherungsrecht & DSGVO), Computerwoche.de, Cloudcomputing-insider.de, Heise.de, computerwelt.de