von Rechtsanwalt **Phil Salewski**

Teil 2: Datenschutzrechtliche Pflichten der Cloudhosting-Anbieter in Europa und den USA

Mit unterschiedlichen rechtlichen Datenschutzstandards in Europa und in den USA sehen sich Cloud-Hosting-Anbieter bei transatlantischen Bezügen auch mit inhaltlich stark divergierenden Datenschutz- und Datensicherheitspflichten konfrontiert. Gegenüber stehen sich die europäische Datenschutzgrundverordnung (DSGVO) und der amerikanische CLOUD Act. Lesen Sie nachfolgend, welche grundsätzlichen Pflichten Anbieter in Europa einerseits und in den USA andererseits zu erfüllen haben und welches Konfliktpotenzial dies mit sich bringt.

I.Rechtliche Pflichten von Cloudhosting-Anbietern in Europa

Speisen Nutzer von Cloudhosting-Diensten personenbezogene Daten in die Cloud ein, sind sie nach der DSGVO weiterhin originär für den Schutz dieser Daten verantwortlich und so grundsätzlich selbst gehalten, alle notwendigen Datenschutz- und Datensicherheitsmaßnahmen zu garantieren.

Cloudanbieter werden in Europa hinsichtlich der eingespeisten Daten nur als sogenannte Auftragsverarbeiter tätig, die bestimmte Datenverarbeitungen (etwa das Speichern, Kategorisieren und Bereithalten der Daten) weisungsgebunden für ihre Kunden übernehmen.

Weil Datenverantwortliche gemäß Art. 28 DSGVO nur mit solchen Auftragsverarbeitern zusammenarbeiten dürfen, welche geeignete technische und organisatorische Maßnahmen für die Datensicherheit bereithalten, sind Cloud-Anbieter stets verpflichtet, den typischen Risiken von cloudbasierten Datenverarbeitungen wirksam zu begegnen.

Dies erfordert die Einrichtung wirksamer Maßnahmen zur Verhinderung von

- Datenverlust und Datenmanipulation
- Identitätsdiebstählen
- Unberechtigten Drittzugriffen
- Schutzlücken wegen vorübergehender Nichtverfügbarkeit

Auf technischer Seite müssen Cloudanbieter dafür insbesondere hinreichende Verschlüsselungs- und Anonymisierungsoptionen sowie Back-Up-Lösungen anbieten.

Gleichzeitig müssen Cloudanbieter sicherstellen, dass Kunden Ihre Kontrollrechte als Datenverantwortliche wahrnehmen können. Da eine Vor-Ort-Kontrolle oftmals nicht möglich ist, sind hier einsehbare Protokolle zum Datenmonitoring vorzuhalten, über welche Kunden Zugriff auf ihre Datenbestände erhalten und diese gegebenenfalls verändern können.

Zusätzlich ist über technische Wege zu gewährleisten, dass Kunden auf Antrag von Datensubjekten

(Betroffenen) deren Betroffenenrechte umsetzen können. Hierzu gehören vordefinierte Abläufe zur Erteilung notwendiger Datenauskünfte, zur Umsetzung von Datenlöschungen, zur Durchführung von Datenberichtigungen und schließlich auch zur Datenübertragung im Falle eines Anbieterwechsels.

Beachtet werden muss auch, dass es Cloudanbietern gemäß Art. 28 Abs. 2 DSGVO gesetzlich untersagt ist, ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung mit weiteren Sub-Dienstleistern zusammen zu arbeiten, die mit eingespeisten Daten in Berührung kommen könnten.

Schließlich müssen Kunden nach Beendigung des Vertrages mit dem Cloudanbieter die Möglichkeit erhalten, eingebrachte Datensätze unwiederbringlich entfernen zu lassen und insbesondere eine Weiterverfügbarkeit sowie Zugriffsmöglichkeiten des Anbieters zu verhindern. Hier sind dem Kunden technische Maßnahmen zur Verfügung zu stellen, mit denen alle von ihm eingespeisten Daten nach seiner Wahl entweder gelöscht oder ihm zurückgegeben werden und vorhandene Kopien unwiederbringlich vernichtet werden.

In rechtlicher Hinsicht sind all diese Umstände abschließend spätestens im Zeitpunkt der erstmaligen Beanspruchung des Cloudhostings in einem spezifischen „Vertrag über die Auftragsdatenverarbeitung“ zu regeln, der zwischen dem Cloud-Anbieter und jedem einzelnen Kunden verpflichtend abzuschließen ist.

Eine Besonderheit ist abschließend zu beachten, wenn Daten aus der Cloud außerhalb des Europäischen Wirtschaftsraums gespeichert oder dorthin vom Anbieter übermittelt werden. Dies ist nicht ohne Weiteres möglich, sondern bedarf einer ausdrücklichen Rechtsgrundlage für jedes Drittland. Für Datenübermittlungen in die USA ist etwa eine Zertifizierung des Anbieters im US-EU-Privacy Shield erforderlich, welche das Einhalten des europäischen Datenschutzniveaus in den USA gewährleistet.

Daneben bestehen für manche Drittländer sogenannte Angemessenheitsbeschlüsse der EU-Kommission. Schließlich können Datentransfers ins außereuropäische Ausland auch über die Unterzeichnung von Standardvertragsklauseln gerechtfertigt werden. Diese werden von der EU-Kommission bereitgestellt.

II. Konfliktpotenzial: Rechtliche Pflichten von Cloudhosting-Anbietern in den USA

In den USA existieren keine einheitlichen gesetzlichen Datenschutzstandards für Cloudanbieter. Vielmehr können Unternehmen im Bereich des Cloud-Hostings weitgehend selbst festlegen, inwieweit sie datenschutzrechtlichen Bedenken ihrer Kunden begegnen wollen (sog. Compliance). Dies hat vor allem Auswirkungen auf die Übermittlung von cloudbasierten Daten von Europa aus in die USA, weil hier gemäß der DSGVO zu gewährleisten ist, dass das europäische Datenschutzrecht mit all seinen Facetten (etwa der Abschluss eines Auftragsverarbeitungsvertrages mit dem amerikanischen Cloud-Anbieter) eingehalten wird.

Im März 2018 ist mit einem neuen US-amerikanischen Rechtsakt ein weiteres Problem für US-amerikanische Cloudanbieter hinzugekommen. Unter der Regierung von Donald Trump wurde der sog. „CLOUD Act“ erlassen, der unter anderem Cloud-Anbieter zur weitgehenden Offenlegung von Daten

(personenbezogene Daten sowie Wirtschaftsinformationen und Telemetriedaten) gegenüber US-Behörden verpflichtet. Nach dem Gesetz sind US-Unternehmen, die Daten im Ausland verarbeiten, immer dem US-Recht unterworfen und infolgedessen dazu verpflichtet, die in ihrer Obhut befindlichen Daten den US-Behörden auf Anfrage offenzulegen. Die Notwendigkeit eines Gerichtsbeschlusses besteht hier nicht.

Diese Rechtspflicht von Cloudanbietern steht seitdem in einem unlösbaren Widerspruch zur DSGVO. Deren Art. 48 verbietet nämlich die Übermittlung von personenbezogenen Daten an Behörden eines Drittlandes, solange kein Rechtshilfeabkommen mit dem Drittland besteht. Ein solches ist mit den USA nie abgeschlossen worden und wird bislang auch nicht verhandelt.

US-Cloudanbieter, die auch Europäer zu ihren Kunden zählen, stehen damit vor einem Dilemma: Entweder sie verstoßen mit den Nachkommen der Übermittlungsaufforderung einer US-Behörde gegen die DSGVO und setzen sich damit der Gefahr empfindlicher Bußgelder aus, oder Sie widersetzen sich der behördlichen Aufforderungen und akzeptieren die Konsequenzen nach US-Recht.

Um diesem Dilemma zu entgehen, wird zwar teilweise eine maximale Datenverschlüsselung von personenbezogenen Daten bei der Übermittlung an US-Behörden vorgeschlagen. US-Behörden sind allerdings nach dem CLOUD Act befugt, Datensätze auch in unverschlüsselter Form anzufordern oder diese selbst zu entschlüsseln.

III. Fazit

Die datenschutzrechtlichen Pflichten, die US- und EU-Anbietern von Cloudhosting-Lösungen im jeweiligen Land auferlegt werden, sind grundsätzlich nicht vergleichbar. Während EU-Anbieter umfangreiche Datensicherungsanforderungen, Weitergabeverbote, Mitwirkungsobliegenheiten und vertragliche Bindungspflichten umsetzen müssen, legen US-Anbieter ihre Datenschutzanforderungen in Form von Compliance-Richtlinien grundsätzlich selbst fest. Für unüberwindbare Probleme sorgt allerdings bei transatlantischen Bezügen der US-CLOUD Act, der US-Anbietern die Offenlegung von Daten gegenüber Behörden auferlegt. Das Folgeleisten derartiger Forderungen verstößt nämlich automatisch gegen die DSGVO, sofern hiervon EU-Kunden betroffen werden.

Autor:
RA Phil Salewski
Rechtsanwalt