(adjuga Information April 2017)

4. Datenschutz und Cloud Computing

Cloud Computing findet in Deutschland immer weitere Verbreitung. Es ist allerdings nicht so, dass die Herausforderungen für rechtssichere Lösungen bereits allgemein bewältigt wären. Der Datenschutz bleibt eine zentrale Aufgabe für alle Cloud-Anbieter und Cloud-Nutzer. Zusätzlicher Informations- und gegebenenfalls Anpassungsbedarf entsteht durch die kommenden Änderungen des Datenschutzrechts: die neue europäische Datenschutz-Grundverordnung (DS-GVO).

Die DS-GVO ist ab dem 25.05.2018 als unmittelbar geltendes Recht in Deutschland anzuwenden. Bis dahin gelten das Bundesdatenschutzgesetz (BDSG) und andere Datenschutzgesetze unverändert fort. Die Datenschutz-Grundverordnung enthält viele bereits aus dem BDSG bekannte Vorgaben: dazu gehören Prinzipien wie das Gebot der Datenvermeidung und Datensparsamkeit, das grundsätzliche „Verbot mit Erlaubnisvorbehalt“ sowie die Zweckbindung und Transparenz der Verarbeitung personenbezogener Daten.

Eine Verarbeitung personenbezogener Daten in der Cloud kann datenschutzkonform regelmäßig nur als Auftragsdatenverarbeitung im Sinne des § 11 BDSG realisiert werden, da eine ansonsten erforderliche Einwilligung aller Betroffenen praktisch meist nicht einzuholen ist. Rechtlich bleibt der Cloud-Nutzer als Auftraggeber dann verantwortlich für die Einhaltung des Datenschutzes, der Cloud-Anbieter wird nur in seinem Auftrag zur Datenverarbeitung tätig. Das Auftragsverhältnis muss in schriftlicher Form abgefasst werden und die detaillierten Vorgaben von § 11 Abs. 2 BDSG einhalten. Gerade die danach dem Cloud-Nutzer als verantwortlicher Stelle obligatorisch einzuräumenden Kontrollpflichten machen in der praktischen Umsetzung große Schwierigkeiten. Hier kann die DS-GVO vor allem durch die neuen Instrumente der genehmigten Verhaltensregeln („Codes of Conduct“) und der Zertifizierung der Einhaltung der technisch organisatorischen Maßnahmen des Cloud-Anbieters Erleichterungen bringen.

Häufig stellt sich die Frage nach der Übermittlung von personenbezogenen Daten in ein Drittland, weil der Cloud-Anbieter dort seine Server betreibt. Nach europäischem Recht ist dafür Voraussetzung, dass ein angemessenes Schutzniveau in dem betreffenden Land besteht oder dass personenbezogene Daten in ein Drittland nur dann übermittelt werden, wenn der Auftragsdatenverarbeiter dazu geeignete Garantien abgegeben hat und dem Auftraggeber durchsetzbare Rechte zur Verfügung stehen, wie unternehmensinterne Datenschutzvorschriften (sog. „Binding Corporate Rules“) oder Standarddatenschutzklauseln, die von der EU-Kommission oder der zuständigen Aufsichtsbehörde akzeptiert wurden.

Die angesprochenen Aspekte machen deutlich, dass das Thema Datenschutz beim Cloud Computing für die Nutzer eine hohe Aktualität hat um das BDSG (weiterhin) einzuhalten und sich bereits auf die Neuerungen der DS-GVO einzustellen. Zukünftig dürfte es beispielsweise für Cloud-Nutzer wichtig werden, von bestehenden oder potenziellen Anbietern Zertifizierungen nach der DS-GVO zu erhalten. Bei Anbietern von außerhalb der EU sollten potenzielle Nutzer prüfen, wie sie die Vorgaben der DSGVO einhalten können, zum Beispiel auf welcher rechtlichen Grundlage eine Datenübermittlung in die Cloud durchgeführt wird.

Die datenschutzrechtliche Überprüfung der Cloudnutzung auf Konformität mit dem BDSG sowie eine Überprüfung und gegebenenfalls Anpassung bestehender Lösungen im Hinblick auf die kommende DS-GVO sollte mit hoher Priorität angegangen werden.

Dr. Tilo Jung +49 6221 4340230 tilo.jung@adjuga.com