

Martin Conrads, Rechtsanwalt, Hamburg

Der US-Cloud-Act im Kontext nationaler Vergabeverfahren



Der Autor

ist Fachanwalt für Vergaberecht und Counsel im Hamburger Büro der Kanzlei Bird & Bird.

Unser Leben in der heutigen Zeit ist durch einen stetigen Wandel auf dem Gebiet der Digitalisierung gekennzeichnet. Die Nutzung technischer Errungenschaften ist aus unserem privaten und beruflichen Alltag nicht mehr hinwegzudenken. Schon längst stellen Schlagwörter wie Big Data bzw. neuerdings Smart Data oder Industrie 4.0 für viele keine leeren Worthülsen mehr dar.

Was jedoch auf der einen Seite eine Chance darstellt, bedeutet auf der anderen Seite auch Risiken. Nicht nur wegen der zunehmenden Anzahl an Cyber-Attacken ist das Bedürfnis nach mehr IT-Sicherheit groß geworden. Auch staatliche Zugriffsmöglichkeiten, wie nach dem US-amerikanischen Patriot-Act, haben das Sicherheitsbewusstsein der Öffentlichkeit verstärkt. Eine neue Herausforderung stellt in diesem Kontext der Umgang mit einem neuen US-amerikanischen Gesetz dar – dem US-Cloud Act.

Der Cloud-Act – Clarifying Lawful Overseas Use of Data – gestattet amerikanischen Behörden, ohne Rücksicht auf internationale Rechtshilfeabkommen und unabhängig vom europäischen Datenschutzrecht den unbeschränkten Zugriff auf – auch personenbezogene – Daten, die sich in der Obhut von US-Unternehmen oder deren ausländischen Tochtergesellschaften befinden. Betreffende Unternehmen unterliegen folglich der gesetzlichen Pflicht, Datenübermittlungsverlangen nachzukommen. Neu ist dabei, dass diese Zu-

griffsrechte auch dann gelten, wenn sich die Daten auf Servern außerhalb der US-Grenzen, z. B. in Irland befinden. Aus amerikanischer Sicht dient der Cloud-Act der Vereinfachung grenzüberschreitender behördlicher Ermittlungen unter Beachtung von Rechtsstaat und Bürgerrechten. Dies betrifft indes offensichtlich nur Bürgerrechte von US-Bürgern.

Vor diesem Hintergrund wird sich im Kontext von IT-Beschaffungsverfahren vermehrt die vergabe- und datenschutzrechtliche Frage stellen, wie anbietende Unternehmen und nationale Beschaffungsstellen rechtssicher mit dieser neuen amerikanischen Gesetzeslage umgehen sollen.

Im Vergaberecht hatte bereits die alte amerikanische Rechtslage dazu geführt, dass Auftraggeber bei sicherheitsrelevanten Aufträgen sog. „No-spy“-Klauseln als Ausführungsbedingungen und „technische no-spy-Klauseln“ in EVB-IT Verträgen gefordert haben. Der Auftragnehmer soll hierdurch den vertrauenswürdigen Umgang mit Daten zusichern und bestätigen, weder vertraglich noch gesetzlich zur Preisgabe vertraulicher Daten an Dritte verpflichtet zu sein. Kritiker befürchten hierdurch eine Diskriminierung von insbesondere US-amerikanischen Unternehmen und ihren deutschen Tochterunternehmen und zweifelten die Zulässigkeit entsprechender „No-spy“-Erklärungen an.

Die Wettbewerbsrelevanz solcher „No-spy“-Erklärungen ist auch zunächst nicht von der Hand zu weisen. Gleichwohl entschied das OLG Düsseldorf (Beschluss vom 21. 10. 2014 – VII-Verg 28/14), dass „No-spy“-Anforderungen zwar keine rechtlich zulässigen Eignungsvoraussetzungen der Bewerber oder Bieter sind, aber als Auftragsausführung im Sinne des § 97 Abs. 4 Satz 2 GWB a. F. (heute im Sinne des § 128 Abs. 2 GWB n. F.), sprich als Vertragsklausel statthaft sind.

Solche „No-spy“-Klauseln seien nach Einschätzung des OLG Düsseldorf nämlich dann nicht diskriminierend bzw. dessen Forderung gerechtfertigt, wenn der öffentliche Auftraggeber für die „Forderung der Datensicherheit einen aner kennenswerten und durch den Auftragsgegenstand gerechtfertigten sachlichen Grund, wie einen Schutz sensibler, für den Schutz des Staates relevanter Daten, namhaft machen kann“ und interessierte nationale Unternehmen „diskriminierungsfrei mit derselben Anforderung belegt werden“.

Außerdem gilt der allgemeine vergaberechtliche Grundsatz, dass ein Auftraggeber nicht gehalten ist, „Ausschreibungen so zuzuschneiden, dass sie – auch unter den Bedingungen, denen sie nach jeweils nationalem Recht unterliegen – zum Unternehmens- und Geschäftskonzept jedes potentiellen Bieters passen“.

US-Unternehmen mit Sitz in Europa befinden sich daher in einer nahezu ausgewogenen

Zwischen US-Cloud-Act und DatenschutzgrundVO: das Dilemma von Unternehmen und Vergabestellen.

Situation. Zum einen unterliegen sie der gesetzlichen Verpflichtung nach dem US-Cloud-Act, sodass sie sich bei einer erfolgreichen nationalen Ausschreibung mit Sicherheitsrelevanz vertragsbrüchig machen würden. Zum anderen unterliegen diese Firmen auch den europäischen Datenschutzbestimmungen. Eine unmittelbare Übermittlung von personenbezogenen Daten ist nach Art. 48 DSGVO nur unter der Voraussetzung des Vorliegens eines Rechtshilfeabkommens zwischen den USA und dem jeweiligen Land zulässig. Ein Verstoß löst nach Art. 83 DSGVO ein Bußgeld in Höhe von bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweiten Vorjahresumsatzes (je nachdem, was höher ist) aus. Eine Gesetzeskollision scheint wohl unumgänglich.

Ein möglicher Ausweg sollte weiterhin das sog. „Treuhändermodell“ sein. Hierbei erhält nur ein nicht dem US-Recht unterfallender Dritter als Datentreuhänder Zugriff über die im nationalen Raum gespeicherten Daten, sodass sie sich nicht mehr in der Obhut des US-Unternehmens befinden und sie als Adressat der Cloud-Act-Verpflichtung ausscheiden.

Letztendlich werden jedoch nur die Praxis und die Rechtsprechung zeigen, ob es adäquate Lösungen für die aufgeworfenen Probleme gibt. Den betroffenen Unternehmen und öffentlichen Auftraggebern bleibt damit zunächst nur die Option, bereits im Vergabeverfahren ganz genau zu prüfen, wo und von wem später Daten gespeichert werden sollen.