

Blogartikel vom 17.08.2022

Datenschutz

Autorin: Rechtsanwältin Vera Franz

## Unzulässigkeit von Cloud- und IT-Dienstleistungen durch US-Tochterunternehmen?

Unter Datenschützern sorgte am 13.07.2022 ein Beschluss der Vergabekammer Baden-Württemberg (Az. 1 VK 23/22) für große Aufregung. In dem zu entscheidenden Fall ging es um die Beschaffung von Software durch die öffentliche Hand (daher die Zuständigkeit der Vergabekammer, die zumindest nicht vorrangig mit Datenschutz befasst ist). Ein Bieter erbrachte Server- und Hosting-Leistungen durch eine in der EU ansässige Tochtergesellschaft eines US-Mutterkonzerns.

Erläuternd zum Hintergrund: Datenübertragungen in die USA sind seit Wegfall des Privacy-Shields rechtlich problematisch und werden vorrangig auf sog. Standarddatenschutzklauseln gestützt. Die Frage ist nun, ob US-Anbieter digitaler Leistungen ihre Dienstleistungen über europäische Tochtergesellschaften erbringen können oder ob eine Zusammenarbeit mit US-Anbietern nach Wegfall des Privacy-Shields trotz der Verwendung von Standarddatenschutzklauseln unzulässig ist.

Die Vergabekammer ist der Ansicht, dass eine datenschutzrechtlich unzulässige Übermittlung vorliegt, wenn der entsprechende Server zwar von einer EU ansässigen Gesellschaft betrieben wird, diese aber Teil eines US-Konzerns ist, weil:

*„in dem Einsetzen (des Bieters, Anm. d. Verf.) als Hosting-Dienstleister ist eine Übermittlung im Sinne der Art. 44 ff. DSGVO zu sehen (...). Der Übermittlungsbegriff ist im Lichte des **weit gefassten Wortlauts des Art. 44 S. 1 DSGVO** sowie der in Art. 44 S. 2 DSGVO niedergelegten Anweisung in Bezug auf die Normanwendung auszulegen und damit **umfassend** zu verstehen: Übermittlung ist **jede Offenlegung personenbezogener Daten** gegenüber einem Empfänger in einem Drittland oder einer internationalen Organisation, wobei es weder auf die Art der Offenlegung, noch auf die Offenlegung gegenüber einem Dritten ankommt (...). Gemessen an diesen Maßstäben führt der beabsichtigte Einsatz (des Bieters), eine europäische Gesellschaft, deren Muttergesellschaft die in den USA ansässige Inc. ist, zu einer **unzulässigen Datenübermittlung in ein Drittland.**“*

Denn:

*„Die Beauftragung (des Bieters) basiert unter anderem auf dem „X. GDPR DATA PROCESSING ADDENDUM“. Diese Vereinbarung enthält unter Ziffer 3 eine Klausel, die die Vertraulichkeit von Kundendaten zum Gegenstand hat ("Confidentiality of Customer Data"). Nach dieser Klausel darf auf die Kundendaten seitens (des Bieters) weder zugegriffen noch dürfen diese verwendet oder an Dritte weitergegeben werden, es sei denn, dies ist zur Aufrechterhaltung oder Bereitstellung der Dienste oder zur Einhaltung von Gesetzen oder wirksamen und rechtskräftigen Anordnungen staatlicher Stellen erforderlich. (...)*

Ziffer 3 und 12.1 des „X. GDPR DATA PROCESSING ADDENDUM“ sind generalklauselartig gestaltet und **eröffnen sowohl staatlichen als auch privaten Stellen außerhalb der EU und insbesondere in den USA** im Rahmen der im konkreten Fall jeweils anwendbaren vertraglichen oder gesetzlichen Ermächtigungen eine Möglichkeit, **in bestimmten Situationen auf bei** (dem Bieter) **gespeicherte Daten zuzugreifen**. (...) Schließlich kann sich das **latente Risiko** jederzeit realisieren. (...) gibt durch die Eingehung der Vereinbarung mit (dem Bieter) die **Einflussmöglichkeiten im Hinblick auf die** (dem Bieter) **anvertrauten Daten jedenfalls partiell aus der Hand.**“

Die alleinige Möglichkeit, dass durch die US-Mutter auf personenbezogene Daten der EU-Tochter zugegriffen werden kann, führt also zu einer Weitergabe der Daten nach der DSGVO.

Gegen diese Entscheidung wurde Sofortige Beschwerde eingelegt. Der Rechtsstreit wird nun durch das OLG Karlsruhe entschieden werden.

Am 15.08.2022 nahm der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink Stellung und bewertete die Entscheidung der Vergabekammer als „*zwar fachlich qualifiziert und von über den (aus einem behördlichen Vergabeverfahren herrührenden) Ausgangsfall hinausweisender Bedeutung*“, kritisierte aber, dass zum einen das Verfahren Klauseln zum Prüfungsgegenstand hatte, die aus Sicht der Vergabekammer hinter den Anforderungen der aktuell einsetzbaren Standarddatenschutzklauseln zurückblieben sind und zum anderen, dass die von der Vergabekammer vorgenommene „Gleichsetzung von Zugriffsrisiko und Übermittlung (als Verarbeitungsform nach Art. 4 Nr. 2 DSGVO) rechtlich zweifelhaft“ ist.

Denn die Kammer stützt ihre Entscheidung darauf, dass ein „latentes Risiko“ eines Zugriffs der US-Konzernmutter besteht, was schon ausreichen soll um eine datenschutzrechtlich unzulässige Übermittlung zu bejahen. OB und WIE naheliegend der Eintritt der in den Klauseln niedergelegten Umstände, die für einen Zugriff im Einzelfall erforderlich ist, sei irrelevant, schließlich könne sich das „latente Risiko jederzeit realisieren.“

Brink bestreitet (unserer Ansicht nach zu Recht), dass ein Zugriffsrisiko „ohne weiteres“ einen Übermittlungstatbestand erfüllt und kritisiert weiter, dass gerade gegen solche Zugriffsrisiken wirksame Gegenmittel in Gestalt sog. „technisch-organisatorischer Maßnahmen existieren“, die jedes Risiko ausschließen können. Diese wurden aber vorliegend überhaupt nicht betrachtet, insbesondere wurde die vom Mitbieter eingesetzte Verschlüsselungstechnik aus vergabeverfahrensrechtlichen Gründen nicht weiter geprüft.

Die Entscheidung der Vergabekammer ist beachtlich, das Urteil des OLG ist daher mit Spannung zu erwarten. Der LfDI Baden-Württemberg hält bislang eigener Aussage nach an den Maßgaben seiner Orientierungshilfe zu Datentransfers (diese finden Sie unter <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf>) fest, wonach nach wie vor einzelfallbezogene Alternativprüfungen und nicht pauschale Transferverbote das Mittel der Wahl sind die Vorgaben der DSGVO bestmöglich umzusetzen. Wir gehen derzeit davon aus, dass sich andere Datenschutzaufsichtsbehörden und insbesondere Bayern dieser Ansicht anschließen.