Vergabekammer BaWü: Unzulässige Drittlandübermittlung durch den Einsatz des EU-Tochterunternehmens eines US-Dienstleisters

Selten hat die Entscheidung einer Vergabekammer bereits in kurzer Zeit für so viel Aufsehen gesorgt wie der Beschluss der VK Baden-Württemberg vom 13. Juli 2022 (Az. 1 VK 23/22). Der noch nicht rechtskräftige Beschluss ist dabei nicht allein für Vergabeverfahren relevant. Die Ausführungen der Vergabekammer können sich ebenso auf die Auswahl von IT-Dienstleistern im privatrechtlichen Bereich auswirken.

Im zu Grunde liegenden Verfahren ging es um die Beschaffung von Software durch einen öffentlichen Auftraggeber. Das Lastenheft des Auftraggebers enthielt in den Anforderungen an IT-Sicherheit und Datenschutz insbesondere folgende Voraussetzungen:

> „[…]
>
> – Erfüllung der Anforderungen aus der DS-GVO und dem BDSG […]
>
> – Daten werden ausschließlich in einem EU-EWR Rechenzentrum verarbeitet bei dem keine Subdienstleister/ Konzernunternehmen in Drittstaaten ansässig sind
>
> […]“

Der Zuschlag wurde einem Bieter erteilt, welcher sich zur Erbringung der Server- und Hosting-Leistungen eines Unterauftragnehmers mit Sitz in der EU bediente. Allerdings handelte es sich hierbei um eine Tochtergesellschaft eines US-Konzerns. Der zweitplatzierte Bieter hat hiergegen einen Nachprüfungsantrag gestellt. Unter anderem berief sich der Antragsteller dabei darauf, dass der Einsatz des Rechenzentrumsbetreibers mit US-Muttergesellschaft einen Verstoß gegen Artikel 44 ff. der DSGVO darstelle und damit die Anforderungen der Vergabeunterlagen nicht erfüllt seien.

Einsatz europäischer Tochterunternehmen von US-Dienstleistern als Drittlandübermittlung

Die Vergabekammer folgte der Ansicht des Antragstellers und stellte fest:

> „In dem Einsetzen von X. als Hosting-Dienstleister ist eine Übermittlung im Sinne der Art. 44 ff. DS-GVO zu sehen. […].
>
> Der Übermittlungsbegriff ist im Lichte des weil [sic!] gefassten Wortlauts des Art. 44 S. 1 DS-GVO sowie der in Art. 44 S. 2 DS-GVO 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 […].

Eine Zugriffsmöglichkeit – etwa durch Einräumung von Zugriffsrechten konstituiert ein latentes Risiko, dass eine unzulässige Übermittlung personenbezogener Daten stattfinden kann, ohne dass hierfür die in der DS-GVO normierten rechtlichen Grundlagen gegeben sind […].

Gemessen an diesen Maßstäben führt der von der Beigeladenen beabsichtigte Einsatz der X., eine europäische Gesellschaft, deren Muttergesellschaft die in den USA ansässige X. Inc. ist, zu einer unzulässigen Datenübermittlung in ein Drittland."

Keine ausreichenden Ausgleichsmaßnahmen zur Einhaltung eines angemessenen Datenschutzniveaus

Weiterhin erachtete die Kammer die zwischen dem erfolgreichen Bieter und dem Rechenzentrumsbetreiber geschlossenen Datenschutzverträge sowie die darin vorgesehenen Maßnahmen als nicht ausreichend, um ein angemessenes Datenschutzniveau zu gewährleisten:

„Die Beauftragung der X. durch die Beigeladene 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 Costumer Data"). Nach dieser Klausel darf auf die Kundendaten seitens X. 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 der X. gespeicherte Daten zuzugreifen. […]

Schließlich kann sich das latente Risiko jederzeit realisieren. Die Beigeladene gibt durch die Eingehung der Vereinbarung mit X. die Einflussmöglichkeiten im Hinblick auf die der X. anvertrauten Daten jedenfalls partiell aus der Hand. […]

Die Übernahme einer Verpflichtung durch X., zu weit gehende oder unangemessene Anfragen staatlicher Stellen einschließlich solcher Anfragen, die im Widerspruch zum Recht der EU oder zum geltenden Recht der Mitgliedsstaaten stehen, anzufechten, beseitigt das latente Risiko eines Zugriffs durch ebendiese Stellen nicht."

Unzulässigkeit des Einsatzes von EU-Tochterunternehmen eines US-Dienstleisters

Dementsprechend kam die Kammer zu dem Ergebnis, dass die festgestellte Datenübermittlung in die USA

rechtswidrig erfolgt:

> „Hier liegt kein besonderer Erlaubnisgrund nach Art. 44 ff. DS-GVO vor. So fehlt es hier an einem Angemessenheitsbeschluss im Sinne des Art. 45 Abs. 1 DS-GVO. Auch Art. 46 Abs. 2 c), d) DS-GVO greift hier nicht ein. Standarddatenschutzklauseln im Sinne dieser Vorschrift sind nicht geeignet, Übermittlungen per se zu legitimieren; vielmehr bedarf es insofern einer Einzelfallprüfung […]. Diese führt – wie dargelegt – zur Annahme der datenschutzrechtlichen Unzulässigkeit. Ein Ausnahmetatbestand nach Art. 49 DS-GVO ist hier ebenfalls nicht gegeben."

Die Argumentation der Vergabekammer, eine unzulässige Datenübermittlung in ein Drittland bereits durch den Einsatz eines europäischen Tochterunternehmens einer US-Gesellschaft auf Grund des Vorliegens einer „latenten Gefahr" anzunehmen, ist nicht unumstritten. Darüber hinaus hat die Vergabekammer aus verfahrensrechtlichen Gründen den Vortrag zu einer vom Rechenzentrumsbetreiber eingesetzten Verschlüsselungstechnik nicht berücksichtigt. Nichtsdestotrotz ist die Entscheidung bemerkenswert. Sie verdeutlicht, dass bereits Zweifel an der datenschutzrechtlichen Compliance sich als echter Wettbewerbsnachteil darstellen können. Auch der enge zeitliche Zusammenhang mit dem kontroversen Einsatz eines US-Cloud-Anbieters im Rahmen des Online-Portals zur Durchführung des Zensus 2022, welcher noch durch den BfDI untersucht wird, macht deutlich, dass das Thema der Drittlandübermittlung – auch im öffentlichen Sektor – zunehmend an Aufmerksamkeit gewinnt. Die Entscheidungen, die eine Rechtswidrigkeit auf Grund mangelnder vertraglicher, technischer und organisatorischer Ausgleichsmaßnahmen annehmen, beginnen sich zu häufen.

Ansprechpartner:

Sebastian Hoegl, LL.M. (Wellington)
Tel: +49 761 769999-20
shoegl@kpmg-law.com

Francois Heynike, LL.M. (Stellenbosch)
Tel: +49-69-951195770
fheynike@kpmg-law.com