

bestimmungen vor, sodass im gegebenen Zusammenhang nicht uneingeschränkt darauf zurückgegriffen werden kann. Wenn darin der Begriff des risikoorientierten Prüfungsansatzes ausgeführt wird, muss dem entgegengehalten werden, dass dieser im Angebot nicht unbedingt der Kalkulation zugrunde gelegt wird, sondern aufgrund der Formulierung nur eine „Annahme“ darstellt. Wesen einer Annahme ist, dass sich diese als falsch erweisen kann und daher eine andere Methode gewählt werden muss. Insofern trägt das vorgelegte Rechtsgutachten nicht zur Lösung der vergaberechtlichen Frage bei.

3.3.3.7 Wie oben ausgeführt steht das Angebot der Antragstellerin wegen nach seiner Formulierung verbleibenden Unsicherheit bei der Kalkulationsannahme in Widerspruch zur

Ausschreibung, da insbesondere die Kalkulation nicht unbedingt ist und daher zu Nachforderungen Raum bieten kann. Es ist daher auch aus diesem Grund gemäß § 141 Abs 1 Z 7 BVergG auszuschneiden.

3.3.4 Zusammenfassung

3.3.4.1 Die Antragstellerin hat einerseits die Strafregisterauskünfte nicht in der geforderten Aktualität vorgelegt und andererseits die Grundlage für ihre Preiskalkulation nur bedingt formuliert, sodass sie einerseits ihre Zuverlässigkeit nicht in der geforderten Form nachgewiesen hat und andererseits das Angebot in Widerspruch zur Ausschreibung steht.

[...]

NEWSFLASH

Schrems II: EuGH kippt „EU-US-Datenschutzschild“ (Privacy Shield)

Auf Betreiben des Datenschutzaktivisten Max Schrems kippte der EuGH das Datenschutzabkommen „Privacy Shield“ bzw die Nachfolgeregelung des bereits 2015 für rechtswidrig erklärten „Safe Harbor“-Abkommens zwischen der EU und den USA (EuGH 16.7.2020, C-311/18). Die Übertragung personenbezogener Daten in die USA ist somit in vielen Fällen rechtswidrig.

Zum Hintergrund: Personenbezogene Daten dürfen entsprechend den Bestimmungen der DSGVO insbesondere nur dann ins Ausland übermittelt bzw dort verarbeitet werden, wenn in diesem Land ein gleiches bzw ähnlich hohes Schutzniveau wie jenes der DSGVO herrscht. Das „EU-US-Datenschutzschild“ setzte genau da an und ermöglichte im Wesentlichen, dass Unternehmen personenbezogene Daten unter bestimmten Schutzvorkehrungen von einem EU-Land in die USA übermitteln können. Gemäß dem Abkommen konnten Unternehmen durch bloße Unterzeichnung einer Selbstverpflichtung erklären, dass eine der wichtigsten Bedingungen der DSGVO – eben die Gleichwertigkeit der Datenschutzvorkehrungen in einem bestimmten Nicht-EU-Land – erfüllt sei. Die datenschutzrechtlichen Stolpersteine des „EU-US-Datenschutzschildes“ waren – wie bereits bei Safe Harbor – die Zugriffsmöglichkeiten der US-Behörden auf Daten und der unzureichende Rechtsschutz für Betroffene. Die nicht richterlich zu bewilligenden Überwachungsbefugnisse der amerikanischen Geheimdienste und Sicherheitsbehörden waren dem EUGH dabei ein besonderer Dorn im Auge: *„In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid“*. Eine klare Botschaft Richtung USA und vor allem ein Arbeitsauftrag an die europäischen Unternehmen.

Die USA haben durch das Urteil ihren besonderen Zugang zum EU-Markt verloren und wurden in Bezug auf Datenübermittlungen aus der EU in die „normale“ Situation von Drittländern versetzt. Absolut notwendige Datenströme gemäß Art 49 DSGVO oder Datenübermittlungen unter ausdrücklicher Einwilligung des Nutzers können daher trotzdem weiterhin stattfinden.

Die EU-Datenschutzbehörde begrüßt in ihrer aktuellen Stellungnahme das „Schrems II-EuGH-Urteil“: *„It is more than a ‚European‘ fundamental right – it is a fundamental right widely recognised around the globe.“* Richtung USA werde darauf vertraut, dass diese *„alle erdenklichen Anstrengungen unternahme, um zu einem umfassenden Schutz der Privatsphäre und Daten zu gelangen.“* Europäische Unternehmer können jedenfalls nicht (nur) vertrauen, sondern müssen jetzt handeln: Im Falle einer Datenübermittlung in die USA – zB aufgrund der Verwendung von Cloud-Diensten (wie Google Cloud, Microsoft Azure etc) – ist die DSGVO-Konformität zu prüfen und rasch sicherzustellen. Es sind somit alle Datentransfers in die USA zu kontrollieren, allenfalls „aufzuspüren“ (zB WhatsApp am Firmenhandy, Youtube/Facebook auf Firmenhomepage etc) und DSGVO-konform zu regeln. Neben der bereits erwähnten ausdrücklichen Einwilligung könnte dies durch „Binding Corporate Rules“ oder die bewährten EU-Standardvertragsklauseln erfolgen. Bei letztgenannten Verträgen erklären die beteiligten Parteien, dass die Daten von EU-Bürgern auch im Ausland angemessen geschützt werden. Die tatsächliche Angemessenheit des Schutzniveaus kann jedoch auch bei der Verwendung von Standardvertragsklauseln (nur) von den zuständigen Datenschutzbehörden überprüft werden.