POSITION STATEMENT

Aktuelle Entwicklungen im Vergaberecht

Stellungnahme des Telecommunications, Internet, and Media (TIM) Committee der American Chamber of Commerce in Germany e.V.

November 2014

1 Anlass

Das Bundesministerium des Innern (BMI) hat am 30. April 2014 einen Erlass veröffentlicht, in dem zwei Klauseln für öffentliche Ausschreibungen mit möglicher Sicherheitsrelevanz im Geschäftsbereich des BMI eingeführt werden:

— Eine Eignungserklärung, die bei Abgabe der Bieterunterlagen zu zeichnen ist. Über die üblichen Klauseln zur Vertraulichkeit hinausgehend soll der Bieter erklären, dass er rechtlich und tatsächlich in der Lage ist, vertrauliche Informationen vertraulich zu behandeln.

— Eine Vertragsklausel, die bei Vertragsabschluss zu zeichnen ist. Die Vertragsklausel sieht vor, dass im Falle der Nichteinhaltung der schon in der Eignungserklärung genannten Bedingungen ein besonderer Kündigungsgrund vorliegt. Der Auftragsnehmer wird darüber hinaus verpflichtet, nach Vertragsabschluss eintretende Offenbarungspflichten dem Auftraggeber zu melden.

Ziel dieser beiden Klauseln ist es, eine Beweiserleichterung zugunsten der öffentlichen Hand zu erwirken. Für die Ablehnung eines Bieters im Zuge der Zuverlässigkeitsprüfung bzw. für eine Vertragskündigung soll in Zukunft der Nachweis ausreichen, dass der Bieter einer rechtlichen Verpflichtung zur Datenweitergabe unterliegt.

2 Bewertung

Die American Chamber of Commerce in Germany e.V. (AmCham) setzt sich für ein hohes Sicherheitsniveau in der öffentlichen Verwaltung ein. Gleichzeitig sind wir der Meinung, dass grundsätzliche Diskussionen über so wichtige Themen wie die nationale Sicherheit und Datenschutz geführt werden müssen. Sie bilden eine wesentliche Grundlage für das Vertrauen der Anwender in die von ihr genutzten IT-Systeme. Die AmCham ist sich jedoch bewusst, dass es gegenwärtig ein Vertrauensdefizit in die Integrität der Informationstechnologie gibt. Dennoch sollten die notwendigen Diskussionen zwischen den zuständigen Regierungsstellen geführt werden und sich nicht negativ auf die Geschäftstätigkeit von Privatunternehmen auswirken. Aus unserer Sicht ist der vorliegende Erlass nicht dazu geeignet, in der gegenwärtigen Form für die Erhöhung des Vertrauens in die Integrität der IT beizutragen:

Erstens: Der Erlass verwendet unklare Rechtsbegriffe und schafft so Unsicherheiten sowohl für Vergabeämter als auch für Unternehmen. Gerade im Bereich der IT-Sicherheit sind klare Richtlinien und eindeutige Pflichten und Regeln wichtig. Der Erlass führt eine Reihe von Begriffen ein, die das Gegenteil erwirken:

— Begriff „Vertrauliche Informationen": Der Erlass bezieht sich auf „vertrauliche Informationen", die definiert werden als „Informationen, die ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden." Diese Definition führt dazu, dass Unternehmen verpflichtet werden, die Vertraulichkeit von Kundendaten selber bewerten zu müssen. Eine Erweiterung auf alle Daten, die „ein verständiger Dritter als schützenswert ansehen würde" schafft Grauzonen, Auslegungsbedarf und letztendlich Rechtsunsicherheit. Die Vertraulichkeit von Daten sollte ausschließlich vom Auftraggeber festgestellt werden und dementsprechend klar gekennzeichnet werden.

— Begriff „Mögliche Sicherheitsrelevanz": Der Erlass bezieht sich auf Vergabeverfahren mit „möglicher Sicherheitsrelevanz". Dies schafft erneut jede Menge Interpretationsspielräume und Unklarheiten. Diese Regel kann dazu führen, dass in Zukunft regelmäßig und pauschal eine Eigenerklärung abzugeben ist. Hier ist eine Konkretisierung hinsichtlich der als sicherheitsrelevant eingestuften Daten sowie der Bedrohungsszenarien notwendig. Dies sollte in enger Anlehnung an den bereits existierenden Rahmen der Vergabeordnung Verteidigung und Sicherheit (VSVgV) geschehen.

Zweitens: Die Klauseln stehen in einem unklaren Verhältnis zur Leistungsbeschreibung. Ein Grundsatz des Vergaberechts ist die eindeutige und abschließende Beschreibung der Leistung. Je klarer diese Beschreibung gefasst ist, desto geringer ist das Risiko von Missverständnissen, Fehlkalkulationen und letztendlich Budgetüberschreitungen. Der vorliegende Erlass relativiert die Leistungsbeschreibung und schafft Unklarheiten hinsichtlich der konkreten Anforderungen im Bereich der IT-Sicherheit. Letztere kann sinnvollerweise nur durch objektivierbare Kriterien definiert werden. Die Form des vorliegenden Erlasses ist hierzu nicht geeignet.

Drittens: Bei Berücksichtigung der vorliegenden Entscheidung der 2. Vergabekammer des Bundes, die sich mit dem aktuellen „No Spy"-Erlass befasst, wird unterstrichen, dass die Problematik einer Verpflichtung zur Datenweitergabe nicht durch die vom Erlass ins Zentrum gerückte Zuverlässigkeitsprüfung im Rahmen der Eignungsprüfung eines Anbieters gelöst werden kann. Danach kommt es auch mit Blick auf den europäischen Rechtsrahmen auf „persönliche" Merkmale an und nicht auf das Unterworfensein unter eine fremde Rechtsordnung. Es sollte daher genau bedacht werden, wie unter dieser Prämisse mit Blick auf die Folge eines de-facto Ausschlusses von öffentlichen Ausschreibungen die geltenden Rechtsnormen und damit die angestrebten Ziele überhaupt erreicht werden können.

Viertens: Der Erlass verschärft das Problem inkompatibler internationaler Rechtsnormen. Unternehmen sind weltweit verpflichtet, mit Sicherheitsbehörden zu kooperieren. In Deutschland wäre hier zum Beispiel das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses zu nennen (Artikel-10-Gesetz). Eine Klausel, die von Unternehmen verlangt, diese Kooperationspflichten vertraglich auszuschließen, schafft ein unauflösliches Dilemma für die Unternehmen. Sie können den gesetzlichen Verpflichtungen aus dem öffentlichen Auftrag nicht gerecht werden, ohne Vorschriften in einem anderen Land zu verletzen und umge-

kehrt. Ein solches Szenario gilt deswegen nicht nur für ausländische Konzerne, die über eine Tochtergesellschaft in Deutschland anbieten, sondern auch für deutsche Konzerne, die im Ausland aktiv sind. Der Erlass verschärft somit das Problem internationaler, nicht kompatibler Rechtsnormen und überantwortet die Lösung dieses Dilemmas den Unternehmen.

Fünftens: Die Beweislasterschwerung für den Bieter ist unfair, weil allein ein abstraktes rechtliches oder technisches Verdachtsmoment als Beweis ausreicht; d.h. das Verdachtsmoment ist der Pflichtverletzung gleichgestellt und begründet den Ausschluss vom Verfahren bzw. berechtigt zur Vertragskündigung. Somit hat der Bieter keine Chance zu beweisen, dass es nicht zu einem Vertraulichkeitsbruch gekommen ist.

Empfehlungen

- **Vergaberechtlich:** Klarere Definition der eingeführten Begriffe und Orientierung an den geltenden Grundsätzen des Vergaberechts. Dies gilt insbesondere für die Vollständigkeit der Leistungsbeschreibung.
- **IT-Sicherheitspolitisch:** Fokussierung auf objektivierbare Kriterien bei der Definition von IT-Sicherheitsstandards, die tatsächlichen Einfluss auf das Sicherheitsniveau haben und Risiken minimieren.
- **International:** Verständigung über den Umgang mit inkompatiblen Rechtsnormen, unter anderem im Rahmen der TTIP-Verhandlungen.

Kontakt AmCham Germany
Telecommunications, Internet, and Media (TIM) Committee

Chair
Dr. Nikolaus Lindner, LL.M.
Leiter Government Relations Deutschland, eBay GmbH

Co-Chair
Mike Cosse
Vice President Government Relations Middle & Eastern Europe, SAP SE

Co-Chair
Dr. Gunnar Bender
Leiter Unternehmenskommunikation, Marketing & Politik, Arvato AG

Staff Contact
Constanze Krüger
Assistant, Government Relations
American Chamber of Commerce in Germany e.V.
Charlottenstrasse 42, 10117 Berlin
T +49 30 288789-24
F +49 30 288789-29
E ckrueger@amcham.de