

Positionspapier

LA Public Sector
AK Öffentliche Aufträge
AK Öffentliche Sicherheit
AK E-Government

Erlass des Bundesministeriums des Innern zum Schutz vor nicht offengelegten Informationsabflüssen an ausländische Sicherheitsbehörden bei öffentlichen Aufträgen

15. Juli 2014
Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 2.100 Unternehmen, davon über 1.300 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der Bitkom setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Inhalt

| | | |
|-----|---|----|
| 1 | Zusammenfassung..... | 2 |
| 2 | Inhalt des Erlasses..... | 3 |
| 3 | Relevante Zielkonflikte | 4 |
| 4 | Unbestimmtheit | 5 |
| 4.1 | Begriff „vertrauliche Informationen“ | 5 |
| 4.2 | Anwendungsbereich „mögliche Sicherheitsrelevanz“ | 5 |
| 4.3 | Anwendbarkeit auf verbundene Unternehmen und multinationale Konzerne | 6 |
| 4.4 | Anwendbarkeit in Lieferketten..... | 7 |
| 4.5 | Begriff der Verpflichtung zur Offenbarung | 7 |
| 4.6 | Eigenerklärung darf nur für künftige Vergabeverfahren gelten | 8 |
| 4.7 | Rechtliche Gewährleistung der Vertraulichkeit | 8 |
| 4.8 | Tatsächliche Gewährleistung der Vertraulichkeit | 9 |
| 4.9 | Organisatorische Sicherheitsmaßnahmen müssen berücksichtigt werden | 9 |
| 5 | Sicherheitsanforderungen gehören in die Leistungsbeschreibung..... | 9 |
| 6 | Unangemessene Beweiserschwerung gefährdet effektiven Rechtsschutz des Bieters | 10 |
| 7 | Transparenz | 11 |

Ansprechpartner

Dr. Pablo Mentzini
Bereichsleiter Public Sector
Tel. +49.30.27576-130
Fax: +49.30.27576-51-130
p.mentzini@bitkom.org

Felix Zimmermann
Bereichsleiter Öffentliches
Auftragswesen und Verga-
berecht
Tel.: +49.30.27576-526
Fax: +49.30.27576-51-526
f.zimmermann@bitkom.org

Präsident

Prof. Dieter Kempf

Hauptgeschäftsführer

Dr. Bernhard Rohleder

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 2

1 Zusammenfassung

Das Bundesministerium des Innern (BMI) bittet das Bundesamt für Beschaffung (BeschA), bei Vergabeverfahren mit möglicher Sicherheitsrelevanz von Bietern künftig eine Eigenerklärung anzufordern sowie die Vertragsbedingungen in geeigneten Fällen durch eine Klausel zu erweitern. Die Eigenerklärung und die Vertragsklausel bezwecken eine Beweiserleichterung zugunsten der Bundesrepublik Deutschland. Für die Ablehnung eines Bieters bei der Zuverlässigkeitsprüfung bzw. für eine Kündigung des Vertrages soll es künftig ausreichen, dass nachgewiesen wird, dass der Bieter einer rechtlichen Verpflichtung zur Datenweitergabe unterliegt. Die neuen Bedingungen gelten im Geschäftsbereich des BMI für Vergabeverfahren mit möglicher Sicherheitsrelevanz. Ob die Verwendung der Eigenerklärung und der Klausel erforderlich ist, soll der Beschaffer mit dem jeweiligen Bedarfsträger abstimmen.

Über die üblichen Klauseln zur Vertraulichkeit hinausgehend sollen die bietenden Unternehmen zukünftig erklären, dass sie rechtlich und tatsächlich dazu in der Lage sind, vertrauliche Informationen vertraulich zu behandeln und vor Einblicken Dritter zu schützen.

Bitkom unterstützt nachdrücklich, dass die Bundesregierung Maßnahmen ergreift, um ein Höchstmaß an Sicherheit für ihre IT- und Kommunikationssysteme herzustellen. Dabei sind neben technischen und wissenschaftlichen auch organisatorische, kommunikative und rechtliche Maßnahmen einzubeziehen. Insofern begrüßen wir, dass die Bundesregierung auch ihre Beschaffungsbedingungen hinsichtlich sicherheitsrelevanter Kriterien überprüft. Dabei muss eine Beschränkung des Wettbewerbs die Ausnahme bleiben und sollte nicht pauschal und formelhaft erfolgen. Die Bundesregierung wird daher um ganz besondere Sorgfalt bei der Entwicklung einer ausbalancierten Regelung gebeten.

Die bisher bekannt gewordenen Vorschläge zur Eigenerklärung des Bieters bedürfen noch einer Konkretisierung, damit Unternehmen in vollem Umfang abschätzen können, ob sie die Eigenerklärung unterschreiben können oder nicht.

Bitkom geht zudem davon aus, dass technische Sicherungsmaßnahmen wie z.B. starke Kryptographie oder organisatorische Sicherheitsmaßnahmen wie *Chinese Walls* in den meisten Fällen grundsätzlich zur Herstellung der Vertraulichkeit von Daten ausreichen. Der Einsatz solcher technologischen Sicherheitsmaßnahmen wird von Bitkom ausdrücklich empfohlen und unterstützt. Eine Eigenerklärung sollte dem Einsatz solcher Technologien Rechnung tragen können und als Maßnahme verstanden werden, die Auftragnehmer rechtlich und tatsächlich in die Lage versetzt, vertrauliche Informationen vertraulich zu behandeln.

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 3

2 Inhalt des Erlasses

Der Anfang Mai 2014 bekannt gewordene Erlass zum Schutz vor nicht offengelegten Informationsabflüssen an ausländische Sicherheitsbehörden bei öffentlichen Aufträgen verpflichtet die Vergabestellen im Geschäftsbereich des Bundesministeriums des Innern. Darunter befindet sich etwa das Beschaffungswesen des Bundes mit einem der größten jährlichen Beschaffungsvolumina in Deutschland.

Der Erlass gilt für alle Aufträge mit *möglicher Sicherheitsrelevanz*. Ob dies jeweils zutrifft, können die Beschaffer für jeden Auftrag selbst entscheiden. Wird eine mögliche Sicherheitsrelevanz angenommen, so muss die mit dem Erlass vorgegebene Eigenerklärung angefordert werden.

Die Eigenerklärung ist eine vorformulierte Erklärung, die von den Bietern im Vergabeverfahren zu unterschreiben ist. Üblicherweise werden derartige Erklärungen zusammen mit dem Angebot beim öffentlichen Auftraggeber eingereicht. Nach der Erteilung des Zuschlags kann die Erklärung nicht mehr ohne Zustimmung des gewinnenden Bieters eingefordert werden. Die Eigenerklärung ist daher ausschließlich im Vorfeld einer Beauftragung zulässig und kann nicht einseitig in ein bestehendes Auftragsverhältnis implementiert werden.

Die Erklärung besteht aus zwei aufeinander aufbauenden Teilen. Der erste Teil betrifft die Zuverlässigkeit des Bieters im Rahmen der Eignungsprüfung. Der Bieter muss der Vergabestelle bestätigen, dass er

rechtlich und tatsächlich in der Lage ist, [...] alle erlangten vertraulichen Informationen [...] vertraulich zu behandeln, insbesondere nicht an Dritte weiterzugeben [...]. Insbesondere bestehen zum Zeitpunkt der Angebotsabgabe keine Verpflichtungen, Dritten solche Informationen zu offenbaren [...]. Dies gilt nicht, soweit hierfür gesetzliche Offenlegungspflichten bestehen [...], es sei denn, solche Offenlegungspflichten bestehen gegenüber ausländischen Sicherheitsbehörden. [...]

Ohne die Unterzeichnung der Erklärung wird der Bieter vom Verfahren ausgeschlossen. Er hat dann keine Chance mehr, den Auftrag zu erhalten.

Der zweite Teil der Eigenerklärung besteht aus einer vertraglichen Regelung. Mit ihr verspricht der Bieter, die gleiche Verpflichtung auch für den Fall des Vertragsschlusses einzuhalten. Damit soll ein besonderer Kündigungsgrund geschaffen werden, mit dem sich der Auftraggeber im Falle der Nichteinhaltung der Klausel vom Vertrag lösen kann. Zudem wird der Auftragnehmer verpflichtet, etwaige später eintretende Offenbarungspflichten dem Auftraggeber auch während der Dauer des Vertragsverhältnisses proaktiv zu melden.

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 4

3 Relevante Zielkonflikte

Bitkom unterstützt ausdrücklich das Anliegen der öffentlichen Auftraggeber, die Vertraulichkeit der Daten zu verlangen und sicherzustellen. Nur so kann das Vertrauen der Bevölkerung in einen effektiven und nachhaltigen Schutz der Vertraulichkeit von Daten durch die Behörden und sonstigen Einrichtungen der Verwaltung aufrechterhalten werden. Deutsche Behörden haben einen guten Ruf, was den Schutz der Vertraulichkeit von Daten betrifft und das soll und muss so bleiben. Somit ist klar, dass die Bundesregierung alle geeigneten und erforderlichen Maßnahmen ergreifen muss, um ein Höchstmaß an Sicherheit für ihre IT- und Kommunikationssysteme herzustellen. Dies schließt neben technischen auch organisatorische und rechtliche Maßnahmen ein. Insofern begrüßt Bitkom, dass die Bundesregierung auch das Vergaberecht hinsichtlich sicherheitsrelevanter Kriterien überprüft. Gleichzeitig müssen Wettbewerbseingriffe so gering wie irgend möglich bleiben. Die Regelung sollte daher vor allem dem konkreten Sicherheitsbedürfnis gerecht werden und nicht pauschal und formelhaft erfolgen.

In vielen Ländern bestehen gesetzliche Verpflichtungen für Unternehmen, bestimmte sicherheitsrelevante Informationen weiterzuleiten. Unabhängig davon, ob diese Unternehmen tatsächlich Informationen weiterleiten, gelangen diese Unternehmen allein aufgrund der rechtlichen Verpflichtung in ein nicht auflösbares Dilemma. Sie können ihren gesetzlichen Verpflichtungen aus dem öffentlichen Auftrag nicht gerecht werden, ohne die Vorschriften des Heimatlandes zu verletzen und umgekehrt.

Zusätzliche Herausforderungen entstehen durch die besonders tiefe und breite Vernetzung der Wertschöpfung im globalisierten Markt der ITK-Produkte und Dienstleistungen. Idealbild des Vergabeverfahrens ist ein offener, effektiver und nichtdiskriminierender Wettbewerb mit möglichst vielen Bietern. Auf nationaler, europäischer und internationaler Ebene gibt es daher fast gleichlautende Regelungen, die allen Unternehmen der unterzeichnenden Staaten einen Anspruch auf diskriminierungsfreie Teilnahme an Ausschreibungen zusichern. Unabhängig von der Herkunft der Anbieter und der Produkte soll also die beste und wirtschaftlichste Lösung gewinnen. Schließlich erwartet der Steuerzahler, dass seine Steuergelder wirtschaftlich und sparsam eingesetzt werden. An öffentlichen ITK-Ausschreibungen beteiligen sich häufig neben nationalen IT-Unternehmen auch rechtlich selbständige nationale Tochterunternehmen von internationalen Unternehmen.

Umgekehrt greifen auch Unternehmen, die ihren Hauptsitz in Deutschland haben, auf Produkte und Lösungen zurück, die von Unternehmen im Ausland oder von nationalen Tochtergesellschaften angeboten werden.

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 5

4 Unbestimmtheit

Bitkom hat Sorge, dass die Regelung in der vorliegenden Fassung wichtige Fragen offen lässt und dadurch Unsicherheit auf Seiten der Unternehmen entstehen.

4.1 Begriff „vertrauliche Informationen“

Der in der Eigenerklärung verwendete Begriff „vertrauliche Informationen“ wird erläutert 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. Vertrauliche Informationen dürfen ausschließlich zum Zweck der Erfüllung der Verpflichtungen aus dem Vertrag eingesetzt werden. Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die bereits rechtmäßig bekannt sind oder außerhalb des Vertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden.“

Vertrauliche Informationen sollten aus Sicht von Bitkom ausdrücklich als vertraulich gekennzeichnet werden. Nur so lässt sich bei Auftraggeber und Auftragnehmer ein gemeinsames Verständnis über den Umfang der Vertraulichkeit erreichen. Die Erweiterung auf alle Informationen, die ein verständiger Dritter als schützenswert ansehen würde, geht demgegenüber sehr weit.

4.2 Anwendungsbereich „mögliche Sicherheitsrelevanz“

Die Eigenerklärung soll künftig den Erläuterungen des Erlasses zufolge bei Vergabeverfahren „mit möglicher Sicherheitsrelevanz“ angefordert werden. Ob die Eigenerklärung erforderlich ist, soll vom Beschaffer mit dem jeweiligen Bedarfsträger abgestimmt werden.

Bereits eine Beschränkung auf „Vergabeverfahren *mit Sicherheitsrelevanz*“ wäre sehr weit. Eine Ausdehnung auf Vergabeverfahren mit *möglicher* Sicherheitsrelevanz dehnt den Anwendungsbereich weiter aus. Selbst bei Ausschreibungen, die auf den ersten Blick keine Sicherheitsrelevanz haben, würde somit die Verpflichtung auf eine Eigenerklärung erstreckt.

Die gewählte Formel ist als Instrument zur Entscheidungsfindung wenig geeignet. Im Interesse des Wettbewerbs sollte vermieden werden, dass künftig pauschal und formelhaft bei den meisten Ausschreibungen eine Eigenerklärung abzugeben ist. Zwar ist es grundsätzlich richtig, der Verwaltung durch unbestimmte Rechtsbegriffe Spielräume zu eröffnen, um konkrete Einzelfälle individuell zu regeln. Durch eine zu weite und offene Formulierung kann jedoch die Gleichförmigkeit und Nachvollziehbarkeit von Entscheidungen der beschaffenden Stelle gefährdet werden.

Bitkom bittet daher zu konkretisieren, welche Art von Daten als sicherheitsrelevant angesehen werden, welcher Herkunft sicherheitsrelevante Daten sind, welche Bedrohungsszenarien gemeint sind oder welche Funktionsbereiche der

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 6

Verwaltung geschützt werden sollen. Mit der Vergabeverordnung für die Bereiche Verteidigung und Sicherheit (VSVgV) gibt es im Vergaberecht bereits einen in Praxis und Rechtsprechung eingespielten Rechtsrahmen. Hieran kann der Erlass anknüpfen und die mögliche Sicherheitsrelevanz in diesem Sinne konkretisieren.

4.3 Anwendbarkeit auf verbundene Unternehmen und multinationale Konzerne

Multinationale und globale Konzerne sind in aller Regel so organisiert, dass neben dem Mutterhaus rechtlich selbständige Tochtergesellschaften bestehen. Bieter und Auftragnehmer ist bei deutschen Ausschreibungen die nationale Tochter, zumeist in der Rechtsform der GmbH. Als nationale Tochtergesellschaften unterliegen diese dem deutschen Recht. Verbundene Unternehmen und multinationale Konzerne sind in aller Regel so organisiert, dass sie arbeitsteilig zusammenarbeiten, d.h. ein Konzernunternehmen (z.B. Holding) bestimmte Aufgaben (z.B. Buchhaltung/ Rechnungsstellung, Rechtsberatung, HR Services etc.) zentral für mehrere verbundene Unternehmen wahrnimmt (sog. Shared Services). Dabei handelt es sich in der Regel um Hilfsleistungen und nicht um unmittelbare Leistungen im Rahmen eines Auftrages, so dass dieses Unternehmen in der Regel kein Nachunternehmer ist.

Offen bleibt, inwieweit die Zugehörigkeit zu einem ausländischen Mutterkonzern, die Unterhaltung eigener Niederlassungen im Ausland oder die Beauftragung von ausländischen Subunternehmern der Eigenerklärung unterliegen sollen. Kommt es auf die Pflicht der Mutter an, mit ausländischen Geheimdiensten zusammenzuarbeiten oder auf die ausdrückliche Pflicht der Tochterunternehmen? Bitkom rät zur Klarstellung, dass es bei der Eigenerklärung nur darauf ankommen kann, ob und inwieweit der tatsächliche Bieter, also die nationale Tochtergesellschaft von rechtlichen Verpflichtungen betroffen ist. Dies sollte gemeinsames Verständnis von Auftraggeber und Auftragnehmer sein.

Auch die umgekehrte Konstellation ist betroffen. Für Abhöraktionen durch ausländische Geheimdienste kann es auch ausreichen, dass sich ein Tochterunternehmen im betreffenden Staat befindet. Auch von einem Dienstleister der seinen Sitz in dem betreffenden Staat hat und Kunden in Deutschland betreut, kann erzwungen werden, Daten herauszugeben. Dabei kommt es auch nicht darauf an, wo sich die Server befinden. Die Mehrheit der mittleren und größeren Unternehmen verfügen über Tochtergesellschaften in aller Welt. Alle Tochterunternehmen und verbundene Gesellschaften haben grundsätzlich eine enge Verknüpfung zu ihrem Mutterkonzern. Viele dieser Unternehmen beauftragen externe ebenfalls global auftretende Dienstleister, z.B. mit Wartung und Betrieb ihrer Netzinfrastruktur.

Potentiell erfasst die Regelung damit auch deutsche Unternehmen, die wegen der Unterhaltung ausländischer Tochtergesellschaften oder Niederlassungen, der Notierung an einer ausländischen Börse oder kontinuierlicher Geschäftsaktivitäten im Ausland der dortigen Jurisdiktion unterfallen und dementsprechend ebenso wie originär ausländische Gesellschaften den dortigen gesetzlichen Offenlegungspflichten unterliegen. Das gilt insbesondere auch für die seit einiger Zeit in der Öffentlichkeit diskutierten Pflichten unter dem U.S.-„Patriot Act“ und

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 7

anderen U.S.-amerikanischen Gesetzesregelungen. Anknüpfungspunkte für eine Erstreckung von Eingriffsbefugnissen U.S.-amerikanischer Gerichte und Ermittlungsbehörden auf deutsche Unternehmen können sich insbesondere dann ergeben, wenn das Unternehmen in den U.S.A. kontinuierlich und systematisch bedeutsame Geschäftsaktivitäten entfaltet, wofür bereits eine Niederlassung ausreichen kann, oder in den U.S.A. ein Tochterunternehmen unterhält, das als „verlängerter Arm“ der deutschen Muttergesellschaft angesehen werden kann. Offen bleibt zudem, inwieweit Shared Services verbundener Unternehmen im Inland oder im Ausland der Eigenerklärung unterliegen sollen. Daher sollte klargestellt sein, dass es bei der Eigenerklärung nur darauf ankommen kann, dass die verbundenen Unternehmen die vertraulichen Informationen zur Durchführung ihrer Tätigkeit in Bezug auf den Auftrag benötigen und nicht anders als zu vertraglichen Zwecken verwenden, solange sie entsprechend zur Vertraulichkeit verpflichtet werden. Dies muss gemeinsames Verständnis von Auftraggeber und Auftragnehmer sein.

4.4 Anwendbarkeit in Lieferketten

Vertraulichkeit hängt nicht allein vom Auftragnehmer ab, sondern etwa in mehrstufigen Lieferketten auch von der Zuverlässigkeit der Subunternehmer und der eingesetzten Hardware und Software ab.

- In welchem Umfang muss ein Bieter als Generalunternehmer entsprechende Eigenerklärungen auch für Subunternehmen abgeben?
- Muss er entsprechende Zusagen im vertraglichen Innenverhältnis einfordern oder müssen Subunternehmer eigene Erklärungen abgeben?
- Welche Aussagen muss ein Unternehmen mit Blick auf die Sicherheit und Zuverlässigkeit der eingesetzten oder geplanten Hardwarekomponenten und der Software zusagen?

Um den vorstehenden Anforderungen gerecht zu werden, müsste ein Unternehmen grundsätzlich von allen verbundenen Unternehmen und Vertragspartnern ebenfalls eine entsprechende Erklärung erhalten. Der Kreis der lieferfähigen Unternehmen könnte in diesem Fall sehr stark eingeschränkt werden.

4.5 Begriff der Verpflichtung zur Offenbarung

Offen bleibt, wie konkret eine Verpflichtung zur Offenbarung ausgestaltet sein muss, mit der Folge, dass ein Unternehmen eine Eigenerklärung nicht mehr abgeben kann. Somit stellt sich die Frage, ab welchem Zeitpunkt ein Unternehmen nicht mehr in der Lage ist, die Vertraulichkeit zu gewährleisten.

- Ist dies bereits mit Inkrafttreten eines Gesetzes, das zur Weitergabe von Informationen verpflichtet, der Fall?
- Bei einer konkreten Anordnung auf Grundlage des Gesetzes?
- Wenn eine Vollstreckung auf Grundlage des Gesetzes angedroht oder wenn die Vollstreckung ausgeführt wird?
- Wie wird es bewertet, wenn das Unternehmen gegen eine Anordnung Rechtsschutz ergreift?

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 8

Bitkom empfiehlt klarzustellen,

- ob die jeweilige Offenlegungspflicht auf einer durch ein Gericht oder eine Ermittlungsbehörde angeordneten Beschlagnahme beruht (etwa gemäß den 94 ff. StPO, insbesondere § 95 StPO, bzw. vergleichbaren straf- und ermittlungsprozessualen Vorschriften anderer Länder)
- oder ob lediglich Offenlegungspflichten aufgrund anderweitiger, z.B. bloß verwaltungsbehördlicher Anforderung erfasst sind
- oder sogar nur Offenlegungspflichten, die der Auftragnehmer allgemein
- oder ob in bestimmten Fällen von sich aus, d.h. ohne behördliche Anforderung im Einzelfall erfüllen muss.

4.6 Eigenerklärung darf nur für künftige Vergabeverfahren gelten

Die Eigenerklärung und die vertragliche Ergänzung sind für künftige Vergabeverfahren gedacht. Dennoch sind bereits Vergabeverfahren bekannt geworden, in denen *nachträglich* die Abgabe einer entsprechenden Eigenerklärung gefordert wird. In dem Erlass muss klargestellt werden, dass die allein in künftigen Vergabeverfahren angewendet werden kann. Soweit im Nachhinein entsprechende Eigenerklärungen verlangt werden, entstehen insbesondere in mehrstufigen Vertragsverhältnissen für den Auftragnehmer als Generalunternehmer hohe Prüfungsaufwände und zudem kaum kalkulierbare Risiken.

4.7 Rechtliche Gewährleistung der Vertraulichkeit

Es ist unklar, in welchen Fällen der Bieter *rechtlich nicht in der Lage ist*, vertrauliche Daten als vertraulich zu behandeln. Dies ist auch aufgrund der proaktiven Mitteilungspflicht des Auftragnehmers von erheblicher Bedeutung. Denn dieser kann erst dann etwas mitteilen, wenn er genau weiß, was überhaupt mitzuteilen ist.

Für Bitkom ist es selbstverständlich, dass der Bieter keine *vertragliche Spionageverpflichtung über die konkreten Daten des Auftraggebers* mit Dritten abschließen darf. Auch Subunternehmer dürfen keine derartigen vertraglichen Pflichten eingehen. Dies gilt zumindest dann, wenn sie bestimmungsgemäß mit vertraulichen Daten des öffentlichen Auftraggebers in Berührung kommen sollen. Diese Fälle sind allerdings bereits ohne die vorgelegte Eigenerklärung nach geltendem Vertragsrecht unzulässig.

Bitkom sieht es aber als kritisch an, wenn dies ohne weitere Konkretisierung auch *gesetzliche Verpflichtungen* umfassend betreffen soll. Gesetzliche Herausgabepflichten beruhen auf abstrakten Rechtssätzen und enthalten keine konkreten Herausgabepflichten. Hierbei bleibt insbesondere unberücksichtigt, dass sich Unternehmen gegen entsprechende Anordnungen auf dem Rechtsweg wehren können.

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 9

4.8 Tatsächliche Gewährleistung der Vertraulichkeit

Bei Ausschreibungen wird das Sicherheitsniveau von Produkten und Services im Wesentlichen durch die Leistungsbeschreibung bestimmt. Hier muss festgelegt werden, welche Anforderungen an die Sicherheit gestellt werden. Eine pauschale Eigenerklärung des Bieters in der dieser zusagt, sein Produkt oder seine Dienstleistung sei tatsächlich in der Lage, alle vertraulichen Informationen vertraulich zu behandeln, schafft keinen realen Zugewinn an Vertraulichkeit.

Unklar bleibt zudem, wann ein Bieter *tatsächlich nicht mehr in der Lage* ist, vertrauliche Daten als vertraulich zu behandeln. Der Anspruch ist sehr weitreichend und auch für Unternehmen, die keiner rechtlichen Verpflichtung zur Weitergabe von Informationen unterliegen, kann es schwer werden, eine derart weitreichende Zusicherung zu geben. Dies gilt insbesondere bei konsequent strategischem Vorgehen von Geheimdiensten, die mit hohen Budgets ausgestattet sind. Gesetzeskonformes oder deliktisches Verhalten von Dritten kann nicht ausgeschlossen werden. Es stellt sich daher die Frage, welche Fälle von der Eigenerklärung ein- und welche ausgeschlossen sein sollen.

4.9 Organisatorische Sicherheitsmaßnahmen müssen berücksichtigt werden

Bitkom geht insoweit davon aus, dass technische Sicherungsmaßnahmen wie z.B. starke Kryptographie oder organisatorische Sicherheitsmaßnahmen wie *Chinese Walls* bzw. andere organisatorisch und technische Maßnahmen grundsätzlich zur Herstellung der Vertraulichkeit von Daten ausreichen. Dies lässt die Eigenerklärung jedoch nicht erkennen. So kann ein hoher Verschlüsselungsstandard dazu führen, dass ein Staat sich nicht an einen IT-Dienstleister wendet, um Zugriff auf dessen Kundendaten zu erhalten, sondern direkt an den betroffenen Kunden.

5 Sicherheitsanforderungen gehören in die Leistungsbeschreibung

Nach geltendem Vergaberecht ist der Auftraggeber verpflichtet, die Leistung eindeutig und abschließend zu beschreiben. Anders ist eine Kalkulation für die Bieter nicht möglich. Bei unklaren Vorgaben besteht die Gefahr, dass unterschiedliche Auffassungen von der Leistung erst im Laufe des Vertragsverhältnisses auffallen.

Für die Bieter stellt sich daher die Frage, inwieweit sich die versprochenen Erklärungsinhalte der Klausel auf das konkrete Angebot auswirken. Wichtig ist insoweit, dass der öffentliche Auftraggeber in der Leistungsbeschreibung genau spezifiziert, welches Schutzniveau er zur Sicherung der Vertraulichkeit der Daten fordert.

Der Erlass lässt offen, ob gleichzeitig auch gesteigerte inhaltliche Anforderungen an die Leistungsbeschreibung gestellt werden müssen. Dies ist nach Ansicht des Bitkom jedoch unverzichtbar. Andernfalls besteht die Gefahr, dass die Eigenerklärung schlicht die Pflicht des öffentlichen Auftraggebers zur Vorgabe klarer Standards in der Leistungsbeschreibung in eine weite Formulierung von Ver-

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 10

tragsbedingungen verlagert. Das Schutzniveau von Daten muss künftig stärker in der Leistungsbeschreibung der öffentlichen Aufträge berücksichtigt werden. Die Vertragsbedingungen sollten dann die Rechtsfolgen regeln, die greifen, falls die Leistungsbeschreibung nicht eingehalten wird.

6 Unangemessene Beweiserschwerung gefährdet effektiven Rechtsschutz des Bieters

Die Eigenerklärung und die Vertragsklausel bezwecken eine Beweiserleichterung zugunsten des Auftraggebers. Für die Ablehnung eines Bieters bei der Zuverlässigkeitsprüfung bzw. für eine Kündigung des Vertrages soll es künftig ausreichen, dass nachgewiesen wird, dass der Bieter einer rechtlichen Verpflichtung zur Datenweitergabe unterliegt.

Im Regelfall muss der öffentliche Auftraggeber eine Pflichtverletzung des Auftragnehmers nachweisen, wie etwa die Offenbarung vertraulicher Informationen. Das Verschulden des Auftragnehmers wird dann vermutet und muss nicht gesondert bewiesen werden. Es besteht insoweit bereits im Vertragsrecht von Gesetzes wegen eine erleichterte Beweisführung für den öffentlichen Auftraggeber.

Mit der neuen Eigenerklärung muss der öffentliche Auftraggeber hingegen nur noch nachweisen, dass den Auftragnehmer entweder eine *rechtliche* Verpflichtung zur Weitergabe vertraulicher Daten trifft oder für den Auftragnehmer ein Schutz der Vertraulichkeit *tatsächlich* nicht möglich ist.

Bereits im Hinblick auf die Beweislastverteilung entfernt sich die Regelung von einem ausgewogenen vertraglichen Risikoverhältnis und benachteiligt den Auftragnehmer unangemessen. Denn es ist vollkommen unerheblich, ob die Vertraulichkeit von Daten tatsächlich gebrochen worden ist, ob dies überhaupt bevorstand oder ob ein Dritter deliktisch dazwischengetreten ist. Es reicht allein ein abstraktes *rechtliches* oder *technisches* Verdachtsmoment als Beweis aus. Dieses Verdachtsmoment wird einer Pflichtverletzung gleichgestellt und begründet den Ausschluss vom Verfahren bzw. berechtigt zur Kündigung des Vertrags.

Der Auftragnehmer hat keine Möglichkeit nachzuweisen, dass es nicht zu einem Vertraulichkeitsbruch gekommen ist. Das Nichtbestehen einer Tatsache kann grundsätzlich nie bewiesen werden. Unklar ist auch, welche weiteren Rechtsfolgen an diese Kündigung zu knüpfen sind. Denn wenn der Auftraggeber unter bestimmten Voraussetzungen (auf die der Auftragnehmer keinerlei Einfluss hat) das Recht haben soll, einen Auftrag zu kündigen, sollte zumindest der Anspruch auf Vergütung oder jedenfalls auf Entschädigung für bereits erbrachte Leistungen gegeben und auch der Höhe nach der Klausel hinreichend bestimmt zu entnehmen sein. Denn die Entstehung von ausländischen gesetzlichen Offenlegungspflichten entzieht sich dem Einflussbereich des Bieters, weswegen ihm das diesbezügliche kaufmännische Risiko nicht einseitig aufgebürdet werden darf.

Bitkom bezweifelt, ob diese Konsequenzen tatsächlich von öffentlichen Auftraggebern gewünscht sein können. Das Recht des Auftragnehmers auf effektiven Rechtsschutz darf nicht derart verkürzt werden.

Positionspapier

Erlass des BMI zur Vertraulichkeit von Daten bei öffentlichen Aufträgen

Seite 11

7 Transparenz

Zu Recht weist der Erlass darauf hin, dass gegebenenfalls entsprechende Verpflichtungen zur Weitergabe von vertraulichen Daten im Vergabeverfahren offengelegt werden müssen. Gerade die mangelnde Transparenz über Inhalt und Umfang bestehender Verpflichtungen zur Weitergabe beeinträchtigen das Vertrauen zwischen Auftraggeber und Auftragnehmer. Daher ist die Forderung nach mehr Transparenz nachvollziehbar.