Eignung von Auftragnehmern bei der Auftragsdatenverarbeitung

Teil 1: Auswahl des geeigneten Auftragnehmers

Zusammenfassung: Für die Frage, welche Auftragnehmer für die Durchführung der Datenverarbeitung im Auftrag in Frage kommen, gilt: „Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen“. Zwei Komplexe sind demzufolge miteinander abzugleichen: Das auftraggebende Unternehmen muss seine Anforderungen an die technischen und organisatorischen Maßnahmen (ToMs) des Auftragnehmers kennen und diese Anforderungen müssen mit den vom Auftragnehmer eingereichten ToMs abgeglichen werden. Potenzielle Auftragnehmer, die keine Unterlagen über ToMs einreichen können oder wollen, oder bei denen die eingereichten ToMs nicht ausreichen, kommen als Auftragnehmer grundsätzlich nicht in Frage. Beauftragt das auftraggebende Unternehmen wider besseres Wissen einen nicht geeigneten Auftragnehmer, können die Folgen Bußgeld bis 300.000 Euro pro Vertrag oder (bei Vorsatz oder dem Willen der Bereicherung) auch Freiheitsstrafe sein.

Situation: Eine Aufgabe des Unternehmens soll ausgelagert werden. Verantwortliche und Datenschutzbeauftragter haben das Vorliegen einer Auftragsdatenverarbeitung identifiziert. Nun soll der geeignete Auftragnehmer gefunden werden. Dabei steht eine Ausschreibung an – oder die Anfrage bei in Frage kommenden Unternehmen mit der Aufforderung, ein Angebot abzugeben. Oft haben die Verantwortlichen schon einen Anbieter im Auge. Nun gilt es die datenschutzrechtlichen Anforderungen zu erfüllen. Dies ist unter anderem Aufgabe des Datenschutzbeauftragten

Rechtslage: Wenn das BDSG einschlägig ist, gilt für die Durchführung der Auftragsdatenverarbeitung § 11 BDSG, wenn ein LDSG oder kirchlicher Datenschutz einschlägig ist, gilt die in den jeweils einschlägigen Gesetzen vorhandene Rechtsgrundlage. Diese weichen vom BDSG gar nicht oder nur geringfügig ab. Im BDSG heißt es: „Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen“ (§ 11 Abs. 2 Satz 1 BDSG). Die Formulierung „ist … auszuwählen“ lässt keine alternative Vorgehensweise zu.

Zu erfüllende Anforderungen: Um die Eignung der vom potenziellen Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (ToMs) beurteilen zu können, müssen beim Auftraggeber die Anforderungen an diese ToMs zunächst einmal definiert sein. Dann muss der potenzielle Auftragnehmer seine ToMs einreichen. Die eigenen Anforderungen sind mit den eingereichten ToMs abzugleichen.

ToMs sind projektbezogen vorzugeben: Die ToMs des Auftraggebers sind nicht unbedingt die für das gesamte Unternehmen dokumentierten technischen und organisatorischen Maßnahmen. Vielmehr sind diese auf den konkreten Fall bezogen. Bespiel: Es soll die Zeiterfassung eines Klinikums in einer Software vorgenommen werden und für die Lieferung, Implementierung und Wartung der Software wird ein Auftragnehmer gesucht. Dann genügt es, wenn das auftraggebende Unternehmen (Klinik) die ToMs für die Beschäftigtendaten als Kriterium anlegt. Die ToMs, die gegebenenfalls davon abweichend für die Erhebung, Verarbeitung und Nutzung der Patientendaten vorhanden sind, haben bei diesem Vorgang nichts zu suchen.

ToMs müssen für die Laufzeit des Projekts aktuell sein: Außerdem ist sicherzustellen, dass der Auftraggeber seine vom Auftragnehmer geforderten ToMs auf dem aktuellen Stand der Technik hat. Beispiel. Die ToMs des Auftraggebers sind zuletzt vor drei Jahren aktualisiert worden. Seither wurden beim Auftraggeber auch Smartphones und Tablets erstmals verwendet. Es ist geplant, dass sich Beschäftigte auch über diese Geräte in die Zeiterfassung einloggen können, um gegebenenfalls erforderliche Korrekturbuchungen selbst vornehmen zu können. Dann müssen die ToMs, die der Auftraggeber von seinem Auftragnehmer fordert, sich auch auf den Einsatz dieser mobilen Endgeräte beziehen. Hier ist unter anderem zu klären, wie die Daten vor dem Abfluss an Betreiber von Apps geschützt werden können.

Abgleich der geforderten und der eingereichten ToMs: In der Folge werden die in Frage kommenden Auftragnehmer ihre ToMs einreichen. Diese sind nun zu prüfen, denn die Vorgabe des BDSG ist eindeutig. Die Eignung der vom Auftragnehmer getroffenen ToMs ist besonders zu berücksichtigen. Gehen die ToMs des potenziellen Auftragnehmers über die Anforderungen des Auftraggebers hinaus, umso besser. Kritischer ist es, wenn die eingereichten ToMs von den geforderten „nach unten“ abweichen oder bestimmte Bereiche überhaupt nicht abdecken. Hier ist sorgfältig zu prüfen, ob auf die georderten Kriterien verzichtet werden kann oder ob es gleichwertige Alternativen gibt, die

vom Auftraggeber auch akzeptiert werden können.

Bei gravierenden Abweichungen kein Auftrag: Die im Gesetz geforderte „besondere Berücksichtigung“ der Eignung der Auftragnehmer-ToMs lässt keinen Spielraum. Weichen die ToMs des Auftragnehmers zu sehr von den Forderungen des Auftraggebers ab, so darf kein Auftrag erteilt werden, wenn es alternative Angebote gibt. Der Preis ist hier nicht ausschlaggebend, Datenschutz darf kein Ramschartikel sein, der bei möglicher Kostenersparnis einfach übersehen werden darf. Zwar hat der Datenschutzbeauftragte keine Durchgriffsmöglichkeit, er wirkt ja nur auf die Einhaltung des Datenschutzes hin. Für die Verantwortlichen im Unternehmen gilt jedoch, dass bei entsprechenden Warnungen des DSB davon ausgegangen werden muss, dass – werden dessen Warnungen in den Wind geschlagen – nunmehr von vorsätzlichem Handeln der Verantwortlichen ausgegangen werden muss.

Bei fehlenden ToMs kein Auftrag: Reichen die potenziellen Auftragnehmer gar keine oder offenkundig völlig unzureichende ToMs ein, ist von einer Beauftragung ebenfalls abzusehen. Gleiches gilt, wenn sich der Verdacht aufdrängt, dass die datenschutzrechtlichen Aktivitäten des potenziellen Auftragnehmers nur auf falschen Angaben beruhen. Beispiel: Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt, der keinen Fachkundenachweis aufweisen kann, sondern nur ein „Grundlagenseminar Datenschutz und IT-Sicherheit“ besucht hat. In diesem Fall ist auch bei weiteren Dokumenten zum Datenschutz Vorsicht geboten, denn ohne Fachkunde kann nicht von einem sachgerechten Datenschutz ausgegangen werden.

Mögliche Rechtsfolgen: Beauftragt das auftraggebende Unternehmen wider besseres Wissen einen nicht geeigneten Auftragnehmer, können gemäß § 43 Abs. 2 sowie § 44 Abs. 1 BDSG die Folgen Bußgeld bis 300.000 Euro pro Vertrag oder (bei Vorsatz gegen Entgelt oder dem Willen der Bereicherung) auch Freiheitsstrafe sein.

Handlungsempfehlung: Sollen Aufgaben des Unternehmens im Rahmen einer Auftragsdatenverarbeitung ausgelagert werden, sollten ToMs definiert werden, die passgenau auf das auszulagernde Projekt ausgerichtet sind. Werden potenzielle Auftragnehmer zur Abgabe eines Angebots aufgefordert, sind deren ToMs anzufordern. Denkbar ist auch, die eigenen ToMs mitzuschicken und die potenziellen Auftragnehmer aufzufordern, eine verbindliche Erklärung darüber abzugeben, dass diese faktisch umgesetzt werden können. Die Überprüfung durch den Auftraggeber muss ja sowieso im übernächsten Schritt erfolgen (nach der Ausfertigung des schriftlichen Vertrags erfolgt die Überprüfung des Auftragnehmers vor der ersten Beauftragung). Werden keine ToMs eingereicht, muss nachgehakt werden, liegen diese jedoch gar nicht vor, ist das anbietende Unternehmen in der Regel auch nicht als Auftragnehmer geeignet. Werden die ToMs eingereicht, sind sie sorgfältig zu prüfen. Abweichungen müssen geklärt werden. Die nächsten Schritte (schriftlicher Vertrag und Überprüfungen des Auftragnehmers mit Dokumentation der Prüfungen) können nur eingeleitet werden, wenn das Prüfergebnis positiv ausfällt.

Hinweis: Da es sich beim Datenschutz um die Umsetzung eines Grundrechts handelt, darf der möglicherweise günstigere Preis eines Anbieters ohne hinreichenden Datenschutz gegenüber einem Anbieter mit Datenschutz nicht das ausschlaggebende Kriterium sein.

Eberhard Häcker, Ensdorf