Auftragsdatenverarbeitung – Auftraggeber sollten sich bevorzugt Auftragnehmer mit Erfahrung bei der Auftragsdatenverarbeitung suchen

Zusammenfassung: Wer Auftragsdatenverarbeitung als Auftraggeber ausschreibt, sollte schon in der Ausschreibung auf Erfahrung mit dem Datenschutz setzen. Dies kann in der Folge Ressourcen im nennenswerten Umfang sparen. Vermeintlich günstigere Anbieter, bei denen in der Folge nicht unerheblicher Aufwand bei den dann erforderlichen Nacharbeiten im Zusammenhang mit Datenschutz entstehen kann, erweisen sich oftmals rasch als zunächst versteckte Kostenfalle. Frühzeitige Einbindung des Datenschutzes und der Nachweis der Erfahrung mit dem Datenschutz schon in der Ausschreibungsphase können zu erheblichen Kosteneinsparungen beitragen

Situation: Jedes Unternehmen ist heute Auftraggeber im Sinne der Datenverarbeitung im Auftrag (Auftragsdatenverarbeitung, ADV) gemäß § 11 BDSG (bzw. der jeweils gültigen Rechtsgrundlage, wenn Verträge mit kirchlichen oder kommunalen Organisationen geschlossen werden). Selbst wenn der Vertrag unstreitig als Vertrag über Datenverarbeitung im Auftrag gekennzeichnet ist und insoweit den Anforderungen der jeweils einschlägigen Rechtsgrundlage entspricht, ist die Umsetzung nicht immer ohne weiteres möglich. Auch etliche Jahre nach Inkrafttreten der Bestimmungen zur Auftragsdatenverarbeitung behaupten viele Auftragnehmer, sie hätten zahlreiche Aufträge auch mit Organisationen, die auf Datenschutz großen Wert legen müssten, aber dass sie ADV betreiben würden und dass man dafür besondere Rechtsbestimmungen beachten müsse, damit würden sie zum ersten Mal konfrontiert. Viele Datenschutzbeauftragte sind angesichts dieser rechtlichen Ignoranz mittlerweile einfach genervt. Hier bietet es sich an, bevorzugt Auftragnehmer zu beauftragen, die nachweislich über Erfahrung mit der Auftragsdatenverarbeitung verfügen.

Rechtslage: Handelt es sich bei derartigen Aufträgen um Datenverarbeitung im Auftrag gemäß § 11 BDSG bzw. entsprechend einer gegebenenfalls abweichenden einschlägigen Rechtsvorschrift (z.B. Landesdatenschutzgesetze, kirchlicher Datenschutz), sind die entsprechenden Rechtsvorschriften einzuhalten. Dies sind insbesondere sorgfältige Auswahl des potenziellen Auftragnehmers unter besonderer Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen sowie ein schriftlicher Vertrag mit den im jeweiligen Gesetz geforderten Mindestinhalten. Außerdem hat sich Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis der Überprüfungen ist zu dokumentieren.

Ignoranz: Leider sind immer noch viele potenzielle Auftragnehmer nicht bereit, die Vorgaben der einschlägigen Rechtsvorschriften anzuerkennen und behaupten, sie würden seit vielen Jahren ohne derartige vertragliche Regelungen auskommen, eine einfache Vertraulichkeitsvereinbarung reiche aus. Für Datenschutzbeauftragte beim Auftraggeber hat das regelmäßig einen unverhältnismäßigen Aufwand zur Folge. Die Erfahrung lehrt, dass die Auftragnehmer in der Folge eine Salamitaktik betreiben. Es braucht oft eine Extraportion Geduld, wenn die vertraglichen Vereinbarungen tatsächlich eingefordert werden. Das beginnt mit der Tatsache, dass kein Datenschutzbeauftragter bestellt ist oder dieser offenkundig nicht in der Lage ist, die Anforderungen der einschlägigen Gesetze richtig anzuwenden. Oft fehlen ernsthafte und belastbare Beschreibungen der technischen und organisatorischen Maßnahmen beim Auftragnehmer. Das geht weiter über fehlende Regelungen mit Subunternehmern sowie nicht vorhandener Dokumentation von Überprüfungen. Verpflichtungen auf das Datengeheimnis fehlen oder sind unvollständig oder veraltet, Schulungen wurden nicht oder nur unzureichend durchgeführt usw. Diese Mängelliste lässt sich beinahe beliebig fortsetzen. Für Datenschutzbeauftragte bei den Auftraggebern entsteht so ein oft unverhältnismäßiger Aufwand, und das, wo doch die zeitlichen Ressourcen ohnehin bei den meisten knapp bemessen sind.

Risiko: Die Bußgeldbestimmungen des BDSG sind eindeutig. Werden Verträge über Auftragsdatenverarbeitung gar nicht oder unvollständig entsprechend den gesetzlichen Anforderungen (Schriftform, Mindestinhalte) geschlossen, und erfolgt die gesetzlich zwingend geregelte Überprüfung des Auftragnehmers vor der ersten Beauftragung nicht, droht Bußgeld bis 50.000 Euro pro Einzelfall.

Weiteres Risiko: Ist das auftraggebende Unternehmen seinerseits Auftragnehmer bei der Auftragsdatenverarbeitung, so enthalten die entsprechenden Verträge Regelungen zur Auswahl und Kontrolle der Unterauftragnehmer (regelmäßig IT-Dienstleister, aber auch andere). Die Auftraggeber sind berechtigt, die Einhaltung datenschutzrechtlicher Bestimmungen in den Verträgen mit den Unterauftragnehmern zu prü-

fen. Entsprechen diese Verträge nicht den gesetzlichen Vorgaben, droht Entzug des Auftrags oder gar Konventionalstrafe.

Vermeintliche Kostenvorteile schmelzen rasch dahin: Werden Aufträge an solche Auftragnehmer vergeben, geschieht dies nicht selten, weil sie ein vermeintlich günstiges Angebot abgegeben haben. Sei es, weil sie in der Nähe sind und daher nur wenige oder gar keine Reisekosten zu berücksichtigen sind, sei es, weil das gesamte Angebot günstiger als bei den Mitbewerbern war. Letzteres wäre übrigens nicht verwunderlich, wenn die gesetzeskonforme Umsetzung des Datenschutzes nicht erfolgt – denn eine datenschutzkonforme Organisation ist nun mal nicht zum Nulltarif zu haben. Was keinesfalls geschehen darf, ist das Anbieter ohne nennenswerte Datenschutzorganisation leichter Aufträge erhaschen können als gesetzestreue Anbieter. Leider scheint das aber in der Praxis immer wieder der Fall zu sein. Verspricht sich jedoch ein Auftraggeber einen günstigeren Preis bei der Dienstleistung, kann dieser durch einen deutlich höheren Aufwand beim eigenen Datenschutzbeauftragten rasch dahin schmelzen. Zwar betrifft das dann in der Regel nicht das Budget des beauftragenden Geschäftsbereichs. Dort wird nämlich der Aufwand für den Datenschutz in der Regel nicht anfallen. Für das Unternehmen insgesamt jedoch wird ein vermeintlich günstigerer Anbieter rasch zur Kostenfalle, wenn durch die Datenschutzignoranz des Auftragnehmers ein erheblicher Aufwand beim Datenschutz des Auftraggebers entsteht.

Datenschutzbeauftragte sind rechtzeitig zu informieren: Gemäß den gesetzlichen Bestimmungen zu den Datenschutzbeauftragten sind diese rechtzeitig über neue Verfahren bei der Datenverarbeitung zu informieren. Geschieht dies, können Datenschutzbeauftragte frühzeitig auf derartige Risiken hinweisen. Dann kommt es nicht zu der unschönen und aufwendigen Folge, dass ein Vertrag geschlossen wurde und im Nachhinein Nachbesserungen erforderlich werden, weil die Regelungen zur Auftragsdatenverarbeitung nicht beachtet wurden.

Schon in der Ausschreibung auf Erfahrung mit Datenschutz bestehen: Die alles kann weitgehend vermieden werden, wenn schon in der Ausschreibung die Erfahrung mit der Umsetzung des Datenschutzes, insbesondere im Zusammenhang mit der Auftragsdatenverarbeitung, verbindlich gefordert wird, idealerweise als Voraussetzung für die Teilnahme an der Ausschreibung überhaupt. Dann wird rasch klar, wer als seriöser Partner in Frage kommt und wer nicht. Und wie oben gezeigt, relativieren sich vermeintliche Kostenvorteile rasch, wenn aufwendig beim Datenschutz nachgebessert werden muss. im schlimmsten Fall muss ein Vertrag bei fehlender Eignung des Vertragspartners ausgesetzt oder gekündigt werden, was stets mit einem erheblichen Aufwand für das auftraggebende Unternehmen verbunden ist.

Handlungsempfehlungen:

1. Ausschreibungsanforderungen bei Datenverarbeitung im Auftrag um die Anforderung „Erfahrung mit Datenschutz, insbesondere bei der Datenverarbeitung im Auftrag als Auftragnehmer“ als eine Voraussetzung für die Auftragserteilung aufnehmen.
2. Schon in der Ausschreibungsphase eine Beschreibung der vom Auftragnehmer leistbaren technischen und organisatorischen Maßnahmen verlangen. Diese müssen in der Folge vom Datenschutzbeauftragten des Auftraggebers einzeln geprüft werden.
3. Daher besser: Vorgabe der erwarteten technischen und organisatorischen Maßnahmen beim Auftragnehmer als Voraussetzung für die Teilnahme an der Ausschreibung beifügen.
4. Falls nicht anderweitig ersichtlich (beispielsweise auf der Homepage des potenziellen Auftragnehmers), Referenzen für die Umsetzung des Datenschutzes mit anderen Auftraggebern anfordern – das erspart später unangenehme Überraschungen
5. Der denkbar beste Fall: Potenzielle Auftragnehmer können eine gültige einschlägige Zertifizierung im Zusammenhang mit Datenschutz und IT-Sicherheit vorweisem. Muster hierfür ist die Zertifizierung nach DIN ISO/IOC 27001, bei deren Vorlage weitestgehend davon ausgegangen werden kann, dass einschlägige Datenschutzbeatimmungen eingehalten werden. Auch eine Zertifizierung eines freien Anbieters für die Auftragsdatenverarbeitung kann von großem Vorteil sein, wenn die Umstände der Zertifizierung bekannt sind. Beides spart vor allem in der weiteren Umsetzung im Zusammenhang mit der Auftragsdatenverarbeitung (ADV) weitere Ressourcen, vor allem bei den Vorab- und Regelüberprüfungen.

Metatags: Auftragsdatenverarbeitung, ADV, Auftraggeber, Auftragnehmer, Zertifizierung, Bußgeld, Ressourcen schonen, Vorabüberprüfung, Vorabüberprüfung bei der Auftragsdatenverarbeitung, Regelüberprüfung, Regelüberprüfung bei der Auftragsdatenverarbeitung, Dokumentation Datenschutz

Zusätzliche Hinweise für die Homepages:

EUWIS GmbH:

- Tagesseminar zur Auftragsdatenverarbeitung
- Beratung zum praktischen Umgang mit der Auftragsdatenverarbeitung

TDSSG:

- Beratung zum praktischen Umgang mit der Auftragsdatenverarbeitung
- Beratung: Vertragsprüfung von Verträgen zur Auftragsdatenverarbeitung

HäckerSoft:

- DATSIS als Tool für die Auftragsdatenverarbeitung

TeamDatenschutz:

- Beratung zum praktischen Umgang mit der Auftragsdatenverarbeitung
- Beratung: Vertragsprüfung von Verträgen zur Auftragsdatenverarbeitung

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de