Auftragsdatenverarbeitung – wenn die Rechtsgrundlage nicht das BDSG ist

So können Sie auch Auftragsdatenverarbeitung für Auftraggeber außerhalb des BDSG ausführen

Zusammenfassung: Ein Unternehmen führt Softwarewartung für ein Personalverwaltungssystem durch. Es handelt sich eindeutig um Auftragsdatenverarbeitung (ADV). Normalerweise sind die Auftraggeber Unternehmen aus dem nicht-öffentlichen Bereich. Hier gelten regelmäßig die Vorschriften aus § 11 Bundesdatenschutzgesetz (BDSG). Eine kirchliche Organisation, die mehrere Alten- und Pflegeheime betreibt, bittet um ein entsprechendes Angebot. Bestandteil des Ausschreibungstextes ist ein Passus, wonach der Auftragnehmer sicherstellen müsse, dass die einschlägigen Rechtsvorschriften des Datenschutzgesetzes der evangelischen Kirche in Deutschland (DSG-EKD) einzuhalten seien. Insbesondere müssten die technischen und organisatorischen Maßnahmen (ToMs) an die Formulierungen des DSG-EKD angepasst werden. Dies sei Voraussetzung für die Erteilung des Auftrags. Ansonsten passt der Auftrag genau in das Leistungsspektrum des Auftragnehmers. Ein Blick in das DSG-EKD zeigt etliche vom BDSG abweichende Formulierungen, die auf die Auftragsdatenverarbeitung Auswirkungen haben..

Alternative Situation: Der Auftraggeber ist eine kommunale Organisation und fordert, das jeweils einschlägige Landesdatenschutzgesetz einzuhalten.

Konsequenz: Denkt man diese Forderung zu Ende, muss ein Unternehmen, das als Auftragnehmer für alle potenziellen Auftraggeber seine Dienstleistungen im Rahmen der ADV anbieten möchte, eine Vielzahl von unterschiedlichen Vertragsvorlagen vorhalten. Zu Ende gedacht, wären das neben dem BDSG noch 18 weitere unterschiedliche Verträge (16 Bundesländer, das DSG-EKD für die evangelischen Landeskirchen und die Gliedkirchen, innerhalb der katholischen Kirche die Anordnung über den kirchlichen Datenschutz (KDO) für die Bistümer). Bleibt die Frage, wie dies mit einem überschaubaren organisatorischen Aufwand erfüllt werden kann und wie vor allem sichergestellt werden kann, dass die unterschiedlichen vertraglichen Verpflichtungen auch eingehalten werden können.

Risiko: Hier besteht das Risiko, dass das Unternehmen den Auftrag nicht erhält, weil die spezifischen vertraglichen Anforderungen nicht eingehalten werden. Dieses Risiko ist aus der bisherigen Praxis heraus zwar als eher gering einzustufen, allerdings hat sich in den letzten Jahren beim Datenschutz vor allem in den kirchlichen Organisationen einiges geändert. Hier wurde der Datenschutz neu geordnet. Datenschutzbeauftragte der Kirchen wurden neu bestellt. Es ist also davon auszugehen, dass die Kirchen, die mit der gesamten Vielfalt der sozialen Einrichtungen wie Kliniken, Alten- und Pflegeheimen, Schulen, Kindergärten usw. einen recht großen Nachfragemarkt bilden, verstärkt auf die Einhaltung einschlägiger Rechtsvorschriften achten werden.

Rechtslage: Bei der Auftragsdatenverarbeitung (ADV) liegt die Besonderheit vor, dass der Auftragnehmer nicht Dritter im Sinne der Datenschutzgesetze ist, sondern als „verlängerte Fachabteilung“ der beauftragenden Organisation gilt. Daher muss auch ein Auftragnehmer die Rechtsgrundlagen erfüllen können, die für die auftraggebende Stelle gelten. Somit muss das Unternehmen, das im Auftrag für eine Einrichtung der evangelischen Kirche tätig ist, deren datenschutzrechtliche Vorgaben erfüllen. Wer als Auftragnehmer für eine Kommune in Baden-Württemberg tätig wird, muss die einschlägigen datenschutzrechtlichen Vorschriften, hier vor allem das Landesdatenschutzgesetz des Landes Baden-Württemberg, erfüllen. Außerdem gelten noch weitere einschlägige Rechtsvorschriften, wie beispielsweise für den Sozialdatenschutz (vor allem im SGB X), die zumindest Auswirkungen auf die Zitate bei den Rechtsquellen in den Vertragsformulierungen haben.

Begründung: Die Bundesrepublik Deutschland ist eine föderalistische Republik, was zur Folge hat, dass der Bund keine Rechtsvorschriften für die Länderangelegenheiten erlassen darf. Für die Umsetzung der eigenen Belange (z.B. Datenschutz in den Landesbehörden oder den Kommunen) erlassen die Bundesländer eigene Gesetze. Allerdings dürfen diese nicht den Vorschriften der Rahmengesetzgebung des Bundes oder entsprechender Vorgaben beispielsweise des Bundesverfassungsgerichts widersprechen. Für die Kirchen gilt, dass durch die Trennung von Kirche und Staat die Kirchen nicht der Gesetzgebung des Staates unterliegen, sondern eigene Rechtsvorschriften zu erlassen haben, die jedoch den Vorgaben des Staates ebenfalls nicht widersprechen dürfen. Sie können jedoch, wie bei den Landesdatenschutzgesetzen auch, an die besonderen Be-

dingungen der Kirchen und kommunalen Einrichtungen angepasst werden.

Herausforderung: Man sollte eigentlich annehmen, dass der Föderalismus dafür sorgt, dass vor allem bei der Durchsetzung von Grundrechten (Datenschutz ist die direkte Auswirkung auf das Grundrecht auf informationelle Selbstbestimmung) keine Unterschiede für die Betroffenen entstehen. Dies ist grundsätzlich auch nicht der Fall. Jedoch können wichtige Details durchaus unterschiedlich formuliert werden. Dies ist beispielsweise bei der Formulierung der technischen und organisatorischen Maßnahmen (ToMs) auch geschehen. Da diese das Herzstück der Auftragsdatenverarbeitung (ADV) bilden, liegt die Herausforderung für Unternehmen, die hier Auftragnehmer sind, darin, die eigenen technischen und organisatorischen Maßnahmen so zu formulieren und einzurichten, dass die den teilweise abweichenden Anforderungen der unterschiedlichen einschlägigen Gesetze und Vorschriften dennoch entsprechen.

Für ein und dieselbe Dienstleistung unterschiedliche Anforderungen: Was für die anbietenden Unternehmen besonders ärgerlich ist, ist die Tatsache, dass für ein- und dieselbe Dienstleistung teilweise unterschiedliche Anforderungen gelten. Zumindest suggeriert dies ein Blick in die unterschiedlichen Formulierungen der technischen und organisatorischen in den einzelnen Landesdatenschutzgesetzen und den kirchlichen Datenschutzgesetzen. So enthält beispielsweise das Landesdatenschutzgesetz Baden-Württemberg elf technische und organisatorische Maßnahmen, das BDSG hingegen nur deren acht. Ein Unternehmen, das die Software für die Personalverwaltung wartet, muss demzufolge formal andere Vorschriften beachten als dies bei einem Auftraggeber aus der Privatwirtschaft der Fall ist.

Entwarnung: Allerdings unterscheiden sich die Vorgaben bei den technischen und organisatorischen Maßnahmen faktisch nicht so sehr, wie der erste Blick vermuten lässt. Im Beispiel Baden-Württembergs ist die allgemeine Organisationsverpflichtung des § 9 BDSG Bestandteil der technischen und organisatorischen Maßnahmen insgesamt und es gibt – anders als im BDSG – keine eigene Anlage für die ToMs. Betrachtet man die anderen Unterschiede im Detail, findet man rasch heraus, dass auch da die Unterschiede nicht so gravierend sind, als dass man diese nicht ohne allzu großen Zusatzaufwand in der Beschreibung der eigenen technischen und organisatorischen Maßnahmen wiederfinden kann. Es kommt eben auch hier auf die exakte Formulierung an. Diese vorzunehmen ist eine der Aufgaben der Datenschutzbeauftragten.

Handlungsempfehlung:

1. Datenschutzbeauftragte sollten eine Synopse der Vorschriften für die Auftragsdatenverarbeitung der in Frage kommenden Rechtsvorschriften (Bundesland, Kirchen) erstellen.
2. Gleiches gilt für die technischen und organisatorischen Maßnahmen, in der Regel das Herzstück der Datenverarbeitung im Auftrag. Dann sind im Bedarfsfall die spezifischen vertraglichen Regelungen rasch angepasst.
3. Im Laufe der Zeit entstehen so für die jeweilige Rechtsgrundlage eigene Vorlagen für die Formulierung in den Verträgen über Auftragsdatenverarbeitung und für die technischen und organisatorischen Maßnahmen.
4. In der Zukunft kann so schon in der Ausschreibungsphase bei entsprechender Anforderung gegenüber den Mitbewerbern ein augenfälliger Vorteil erzielt werden.

Hinweis: Der einfachste Weg wäre, einen Standardvertrag aufzusetzen und in der Präambel darauf hinzuweisen, dass die entsprechenden Vereinbarungen zwar für das BDSG formuliert wurden, jedoch ist dies in den einzelnen Rechtsvorschriften teilweise ausdrücklich ausgeschlossen. Dort wird vielmehr darauf verwiesen, dass die Auftragnehmer die Umsetzung des jeweils gültigen Rechtes (beispielsweise DSG-EKD) sicherzustellen haben. Somit reicht in der Praxis eine einfache Synopse der Rechtsgrundlagen, die Vertragsbestandteil wird, leider oft nicht aus.

Metatags: Auftragsdatenverarbeitung, Datenverarbeitung im Auftrag, ADV, DSG-EKD, Datenschutzgesetz der evangelischen Kirche, KDO, Kirchliche Datenschutzordnung, Landesdatenschutzgesetz, Auftraggeber, Auftragnehmer, technische und organisatorische Maßnahmen, TOMS, ToMs, Sozialdatenschutz

Zusätzliche Hinweise für andere Homepages:

EUWIS: Tagesseminar für „ADV mit anderen Rechtsgrundlagen als dem BDSG“

Tagesseminar: „Besonderheiten des DSG-EKD und der Rechtsverordnungen dazu“

Datenschutzberatung für ADV mit anderen Rechtsgrundlagen als dem BDSG

Datenschutzberatung in Gesundheitseinrichtungen der Kirchen und kommunalen Organisationen wie Kliniken

TDSSG: Datenschutzberatung für ADV mit anderen Rechtsgrundlagen als dem BDSG

Beratung: Anpassung der Unterlagen für die Auftragsdatenverarbeitung an andere Rechtsgrundlagen als das BDSG

Vertragsprüfung für die Auftragsdatenverarbeitung für Organisationen mit anderen Rechtsgrundlagen als dem BDSG

Team Datenschutz: Beratung: Anpassung der Unterlagen für die Auftragsdatenverarbeitung an andere Rechtsgrundlagen als das BDSG

Datenschutzberatung für ADV mit anderen Rechtsgrundlagen als dem BDSG

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