Datenverarbeitung im Auftrag entdeckt – was ist zu tun?

Zusammenfassung: Zunächst ist zu prüfen, ob es sich um Auftragsdatenverarbeitung (ADV) oder um Funktionsübertragung (FÜ) handelt. Die nächste Prüfung gilt der Suche nach einer schriftlichen Vereinbarung. Wurde ein schriftlicher Vertrag geschlossen? Gibt es bei der FÜ eine Vertraulichkeitsvereinbarung? Gibt es bei der ADV Vereinbarungen über technische und organisatorische Maßnahmen? Wie kann die Auftragskontrolle erfolgen? Gibt es Unterstützung durch den Fachbereich, der den Vertrag eingefädelt hat? In jedem Fall ist sicherzustellen, dass den gesetzlichen Anforderungen an die Datenverarbeitung im Auftrag Genüge getan wird.

1 DSB sind Kummer gewohnt

Datenschutzbeauftragte sind Kummer gewohnt. Immer wieder stoßen sie bei ihrer Arbeit auf Datenverarbeitung im Auftrag, von der sie erstens noch nichts wissen und wo zweitens die näheren Umstände nicht geklärt sind.

Beispiel: Ein Geschäftsbereich arbeitet mit einer eigenen Software, bei deren Beschaffung vor einigen Jahren die IT nicht beteiligt war. Bei der IT erfährt der DSB nichts über die Software und die Umstände zum Vertrag und zur Wartung. Hier muss der Geschäftsbereich befragt werden.

Aufgabe des Datenschutzbeauftragten ist es nun, die genauen Umstände zu erfahren und gegebenenfalls dafür zu sorgen, dass für die vertraglichen Verhältnisse Rechtskonformität hergestellt wird.

2 ADV oder FÜ?

Zunächst ist zu prüfen, ob es sich um einen Vertrag über Auftragsdatenverarbeitung oder um Funktionsübertragung handelt.

Wenn es sich um Auftragsdatenverarbeitung handelt, hat der Gesetzgeber einige Formalien für die Umsetzung vorgegeben. Der Auftragnehmer ist unter besonderer Berücksichtigung der von ihm eingesetzten technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Es ist ein Vertrag über Auftragsdatenverarbeitung abzuschließen, der schriftlich abgefasst sein muss und der die in der jeweiligen einschlägigen gesetzlichen Grundlage genannten Mindestbestandteile enthalten muss. In der Regel dürfte es sich hier um § 11 BDSG handeln.

Ist für den Auftraggeber ein anderes Datenschutzgesetz, beispielsweise ein Landesdatenschutzgesetz oder ein kirchliches Datenschutzgesetz einschlägig, so sind dessen rechtliche Vorgaben für die ADV zu beachten.

Sodann ist der Auftragnehmer vor der ersten Beauftragung zu prüfen, ob die vertraglich zugesagten technischen und organisatorischen Maßnahmen auch erfüllt werden. Diese Prüfung ist zu dokumentieren und in der Folge regelmäßig erneut durchzuführen. Auch die Folgeprüfungen sind zu dokumentieren. Bei Nichterfüllen eines Teils dieser Anforderungen droht, zumindest wenn das BDSG gilt, ein Bußgeldverfahren durch die zuständige Aufsichtsbehörde.

3 Empfohlene Prüfschritte

Wenn Datenschutzbeauftragte bei ihrer Arbeit auf eine Datenverarbeitung im Auftrag stoßen, von der sie bislang noch nichts wussten, sollten sie den Vorgang einer genaueren Prüfung unterziehen. Dazu bietet sich ein strukturiertes Vorgehen in mehreren Prüfschritten an, an die sich gegebenenfalls konkrete Handlungen anschließen.

- **ADV oder FÜ?** In einem ersten Schritt ist zu prüfen, ob es sich bei der vorgefundenen Datenverarbeitung im Auftrag um ADV oder FÜ handelt.
- **Schriftliche (Vertrags-)Unterlagen vorhanden?** Wie die Erfahrung lehrt, liegt vor allem bei Verträgen, die schon seit mehreren Jahren in Kraft sind, nur selten ein Vertrag über Auftragsdatenverarbeitung vor. Und wenn einer vorhanden ist, entspricht dieser Vertrag nur in seltenen Fällen den aktuellen gesetzlichen Anforderungen. Zumeist sind nur Regelungen zum Vertragsgegenstand vorhanden.
- **Vertragspartner bekannt**? Eventuell gibt es mit dem Auftragnehmer gegebenenfalls weitere Verträge, auf die zurückgegriffen werden kann und für die es gegebenenfalls schon Verträge über ADV oder FÜ gibt. Wenn dies der Fall ist, macht das die ganze Sache etwas leichter. Dann bestehen schon Vereinbarungen, auf die man gegebenenfalls aufbauen kann.
- **DSB vorhanden?** Falls es beim Auftragnehmer einen Datenschutzbeauftragten gibt, macht es das Ganze auch noch einmal etwas leichter. Aber wie die Erfahrung ebenfalls lehrt, ist das sehr oft nicht der Fall oder es handelt sich um einen DSB, der nur wenig Erfahrung und nur wenig Zeit hat, weil er als Lückenfüller bestellt wurde.
- **Auftragskontrolle:** Wie die Auftragskontrolle erfolgen kann, ist eine nicht zu unterschätzende Frage. Papier ist geduldig, wenn eine

Vertragsergänzung nachgereicht wird, um den Anforderungen an die ADV gerecht zu werden, wird vieles unterschrieben. Die Auftragskontrolle beim Auftragnehmer gestaltet sich oft alles andere als einfach.

- **Unterstützung anbieten:** Gegebenenfalls kann man den Kollegen / die Kollegin vor Ort unterstützen, indem man verwendbare Vorlagen hinsendet oder Tipps zur Umsetzung der vertraglichen Anforderungen gibt. Wie auch immer, die Auftragskontrolle ist unverzichtbar.
- **Auftragskontrolle vor Ort erforderlich?** Ob sie vor Ort erfolgen muss, ergibt sich in der Regel erst in den Einzelfragen, die im Laufe des Verfahrens aufkommen. In jedem Fall gilt: Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
- **Dokumentationspflicht erfüllen:** Das Ergebnis der Auftragskontrolle ist zu dokumentieren.

4 Vorsicht – Bußgeld droht

Erst vor kurzem hat das Bayerische Landesamt für Datenschutz in Ansbach ein Bußgeld in fünfstelliger Höhe wegen fehlerhafter ADV erlassen.

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt.

Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden. Dies gilt für jeden einzelnen Fall. Bestehen beispielsweise mit fünf Unternehmen Vereinbarungen über Auftragsdatenverarbeitung, die je-doch einen oder mehrere der hier genannten Mängel vorweisen, kann das Bußgeld auch mehrfach, hier fünffach, verhängt werden.

5 Handlungsempfehlungen

- **Prüfen ADV oder FÜ** – handelt es sich bei der neu entdeckten Datenverarbeitung im Auftrag um ADV oder um Funktionsübertragung (FÜ)?
- **Verantwortlichkeiten ermitteln**: Feststellen, wer im Haus die Vertragsverantwortlichen sind und mit diesen die Rechtslage besprechen
- **Schriftliches vorhanden?** • Prüfen, ob eine schriftliche Vereinbarung / ein Vertrag vorhanden ist und prüfen, ob dort eventuell schon Vereinbarungen zur Auftragsdatenverarbeitung getroffen sind
- **Vollständigkeit gegeben?** • Prüfen, ob eventuell vorhandene Unterlagen vollständig sind
- **Vertragsergänzung:** Bei Bedarf anfertigen und nachreichen einer Vertragsergänzung mit Regelungen zur ADV (oder FÜ)
- **TOMs einfordern:** Einfordern der technischen und organisatorischen Maßnahmen (TOMs) des Auftragnehmers oder Vorgabe der TOMs, die beim Auftragnehmer zu erfüllen sind
- **Auftragskontrolle:** diese muss in geeigneter Weise vorgenommen werden
- **Weitere unentdeckte ADV vorhanden?** Prüfen, ob im betreffenden Geschäftsbereich weitere unentdeckte Datenverarbeitungen im Auftrag vorliegen, bei Bedarf Schulung der Verantwortlichen vornehmen

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