Prüfaufwand bei Auftragsdatenverarbeitung verringern

Zusammenfassung: Auftraggeber müssen ihre Auftragnehmer bei der Auftragsdatenverarbeitung aufgrund der einschlägigen gesetzlichen Vorgaben mehrfach und regelmäßig überprüfen. Dabei sind die vom Auftragnehmer verwendeten technischen und organisatorischen Maßnahmen der wesentliche Prüfgegenstand. Um den Prüfaufwand für Auftraggeber und Auftragnehmer deutlich zu verringern, bietet sich eine „§-11-Zertifizierung“ an, bei der ein unabhängiger Dritter die vertraglichen Vereinbarungen stellvertretend für die Auftraggeber prüft und testiert.

1 Outsourcing als ADV ist Alltag

Outsourcing ist für die meisten Unternehmen Alltag. Die Ausführenden des Outsourcings sind IT-Systemhäuser, Softwarehäuser, Callcenter und viele andere Unternehmen in etlichen Branchen. Ihr Geschäftsmodell basiert auf der Auftragsdatenverarbeitung (ADV). Gäbe es die ADV nicht, könnten sie nicht überleben (s.u.)

Allerdings ist der Aufwand, den Auftragnehmer laut Gesetz bei der ADV erfüllen müssen, erheblich. Schätzungsweise entsprechen erst 10 bis 15% aller ADV-Verhältnisse den gesetzlichen Vorgaben. Nachdem die Aufsichtsbehörden jetzt jedoch ernst machen und für unvollständige oder nicht vorhandene Vereinbarungen über Auftragsdatenverarbeitung Bußgelder erheben, dürfte sich das sehr bald ändern.

Immer mehr Auftraggeber werden dann aus Sorge vor Bußgeldern ihre Kontrollpflicht ernst nehmen und die erforderlichen Überprüfungen durchführen. Auftragnehmer müssen dann vermehrt damit rechnen, dass Auftraggeberkontrollen auch vor Ort durchgeführt werden.

2 Privileg ADV

Die Auftragsdatenverarbeitung gilt als Privileg für die Auftraggeber. Ohne ADV benötigt ein Unternehmen einen Ausnahmetatbestand, also eine Rechtsgrundlage, wenn personenbezogene Daten an Dritte übermittelt werden. Das Privileg liegt darin, dass Auftragnehmer bei der ADV nicht als Dritte gelten. Datenverarbeitungen, die durch Auftragnehmer erfolgen, gelten rechtlich als interne Verarbeitung. Der Auftragnehmer ist also eine Art Fachabteilung des Auftraggebers.

Allerdings gilt: Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften hinsichtlich Datenschutzes verantwortlich. Dieser hat ein Interesse daran, dass bei der ADV beim Auftragnehmer keine Fehler passieren.

3 Pflichten bei der ADV

Das spiegelt sich auch in den einschlägigen Datenschutzgesetzen wider. Der Auftragnehmer ist sorgfältig auszuwählen, wobei die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten des Auftragnehmers besonders zu beachten sind. Der Auftrag ist schriftlich zu erteilen. Es sind zehn Mindestinhalte, die in den Gesetzen zum Datenschutz aufgelistet sind, zu regeln. Der Auftraggeber muss vor der ersten Beauftragung eine Überprüfung der technischen und organisatorischen Maßnahmen beim Auftragnehmer durchführen. Diese muss sodann regelmäßig erfolgen. Überprüfungen sind zu dokumentieren.

4 Überprüfungen nehmen zu

Insbesondere für Unternehmen, deren Geschäftsmodell darauf basiert, als Auftragnehmer bei der Auftragsdatenverarbeitung tätig zu sein, kann diese Pflicht zur Überprüfung eine erhebliche wirtschaftliche Belastung werden.

Immer mehr Auftraggeber nehmen ihre Pflicht zur eigenen Überprüfung mangels Alternative wörtlich und führen diese vor Ort beim Auftragnehmer durch. Sie tragen das Risiko, wenn in Sachen Datenschutz Fehler begangen werden. Dabei muss die Überprüfung nicht unbedingt persönlich und vor Ort durch den Auftraggeber selbst erfolgen.

5 Prüfungen durch Dritte sind möglich

Alternativ gilt: Die Überprüfung kann auch durch einen neutralen Dritten erfolgen, beispielsweise in Form von Audits durch eine unabhängige Organisation oder zunächst auch durch die schriftliche Bestätigung durch den Datenschutzbeauftragten des Auftragnehmers, der ja per se unabhängig und nicht weisungsgebunden in Sachen Datenschutz ist. Sobald jedoch besonders schützenswerte Daten bei der Datenverarbeitung im Auftrag beteiligt sind, kann auf eine eigene oder unabhängige externe Überprüfung grundsätzlich nicht mehr verzichtet werden.

6 Aufwand für beide Seiten

Bei Vor-Ort-Audits durch Auftraggeber werden auf beiden Seiten erhebliche Ressourcen gebunden. Beim Auftraggeber muss ein fachkundiger Auditor anwesend sein. Dies ist in vielen Fällen ein externer Spezialist. Weiter müssen die Projektverantwortlichen anwesend sein, denn nur so kann eine fachkundige Begleitung des Auditors sichergestellt werden.

Aber auch wenn es sich nicht um einen externen sondern um einen internen Auditor handeln

sollte, kann nicht immer davon ausgegangen werden, dass dieser alle Projektdetails kennt.

Dann müssen der Datenschutzbeauftragte und auch der IT-Sicherheitsbeauftragte des Auftraggebers mir vor Ort sein. Beim Auftragnehmer entsteht ein vergleichbarer Aufwand, so dass schnell mehrere Manntage an Aufwand zusammenkommen. Dazu kommen Reise- und Unterbringungskosten. Rasch summiert sich der Aufwand auf mehrere Tausend Euro.

7 Lösung „§-11-Zertifizierung“

Immer dann, wenn eine Vielzahl von Auftraggebern vorhanden ist und damit potenziell viele Überprüfungen vor Ort „drohen“, kann mit einer speziellen Zertifizierung der Aufwand beträchtlich gesenkt werden. Die Idee dahinter ist, dass die Überprüfung speziell für die Auftragsdatenverarbeitung, also der vertraglichen Vereinbarungen und vor allem der vereinbarten technischen und organisatorischen Maßnahmen, durch einen unabhängigen Dritten erfolgt.

Dabei handelt es sich um eine spezielle Auditierung, die auf der genauen Analyse der vertraglichen Verpflichtungen basiert und quasi die Prüfpflichten der Auftraggeber übernimmt.

Das führt dazu, dass die Auftraggeber ihre Prüfpflicht an einen unabhängigen Dritten abgeben. Das funktioniert besonders gut, wenn die Verträge über Auftragsdatenverarbeitung zumindest ähnlich, wenn nicht sogar in weiten Teilen identisch sind, vor allem hinsichtlich der technischen und organisatorischen Maßnahmen,.

8 Vorteile auch für Auftraggeber

Wenn eine verlässliche Überprüfung der Auftragsdatenverarbeitung durch einen unabhängigen Dritten erfolgt, darf der Auftraggeber das Ergebnis als eigene Prüfdokumentation verwenden. Macht der unabhängige Dritte bei der Überprüfung Fehler, kann er unter Umständen haftbar gemacht werden.

9 Vertrieb wird unterstützt

Mit der Tatsache des verringerten Aufwands kann der Auftragnehmer bei den Vertriebsgesprächen gegenüber der Konkurrenz punkten. Verringerter Aufwand ist immer ein gutes Argument.

10 Lohnende Investition

Die Kosten für Vorbereitung und Durchführung der §-11- Zertifizierung sowie die erforderlichen Prüf- und Rezertifizierungsaudits sind im Vergleich zu den Aufwendungen durch Überprüfungen deutlich geringer. Dies gilt umso mehr, je einheitlicher die Aufträge und die vertraglichen Vereinbarungen sind. Eine §-11-Zertifizierung wird in der Regel schon nach drei erforderlichen Prüfungen durch Auftraggeber, die durch die Zertifizierung ersetzt werden, zu einer lohnenden Investition für den Auftragnehmer.

11 Handlungsempfehlungen

- **Aussagefähige TOMS erstellen:** Auftragnehmer bei der ADV sollten sich eine aussagefähige Dokumentation der (TOMs) bezüglich der Auftragsprojekte erstellen.
- **Bei Ausschreibungen verwenden**: Die TOMs sollten Bestandteil der Ausschreibungsunterlagen oder der Angebote sein.
- **Akzeptanz bei Auftraggebern** Erfahrungsgemäß sind Auftraggeber bereit, die TOMs des Auftragnehmers zu akzeptieren, vor allem dann, wenn diese spezifisch für die zu erteilenden Aufträge erstellt worden sind. Das reduziert den Bearbeitungsaufwand bei Auftraggeber und Auftragnehmer.
- **Partner für Zertifizierung:** Nun gilt es, einen geeigneten Anbieter für die „§-11-Zertifizierung“ zu suchen. Denkbar ist auch eine Zertifizierung nach DIN ISO 27001 (Informationssicherheit), nur ist diese deutlich aufwendiger.
- **Umsetzung:** Die §-11-Zertifizierung wird durchlaufen.
- **Vorlage der Ergebnisse:** Die Prüfkriterien und Prüfergebnisse werden den aktuellen und den künftigen Auftraggebern in kumulierter Form vorgelegt.
- **Eigene Prüfkriterien sind möglich:** Gegebenenfalls sollte man die Auftraggeber auch eigene Kriterien formulieren lassen, wenn diese in der vorliegenden §-11-Zertifizierung nicht enthalten sein sollten, diese dann dem Auditor übergeben und beim nächsten Audit bzw. bei der nächsten Zertifizierung mit prüfen lassen.

Eberhard Häcker, Ensdor

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. Das jüngste Projekt ist datenschutzkabarett.de