DATENSCHUTZ

Wenn die Prüfer kommen

VON THOMAS ALTHAMMER
Thomas Althammer ist Wirtschaftsinformatiker und berät Einrichtungen und Träger zu IT-Strategiefragen, im Bereich IT-Compliance und zu Fragen rund um Datenschutz und Datensicherheit. Er verfügt über langjährige Erfahrung bei der Gestaltung und Implementierung von EDV-Systemen in Verwaltung, Abrechnung und Pflege.
www.althammer-it.de

Die Aufsichtsbehörden für den Datenschutz kontrollieren die Ausführung der Gesetze und Vorschriften über den Datenschutz und beraten den betrieblichen Datenschutzbeauftragten. Die Aufsichtsbehörden verwalten das Register der meldepflichtigen »automatisierten Verarbeitungen« nach dem Bundesdatenschutzgesetz und führen »anlassbezogene« Kontrollen durch, meistens nach Beschwerden von Betroffenen.

Einrichtungen und Träger der Sozialwirtschaft sind heute abhängig von einem reibungslosen Betrieb ihrer Informationstechnologie (IT) und müssen gleichzeitig dafür Sorge tragen, dass die ihnen anvertrauten Daten sicher und vertraulich behandelt werden.

Der Datenschutz greift zwar auch bei papiergestützten Verfahren. Mit Einsatz von IT-Lösungen sind jedoch noch weitreichendere Aspekte zu berücksichtigen, da Daten von verschiedenen Stellen und ortsungebunden erhoben, eingesehen und verarbeitet werden können. Zur Einhaltung der einschlägigen Datenschutzvorschriften ist damit ein wesentlich höherer Aufwand erforderlich, um ein angemessenes Datenschutzniveau zu erreichen.

Grundsätzlich gilt das Verbotsprinzip mit Erlaubnisvorbehalt: Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn es hierfür eine gesetzliche Regelung gibt oder eine Einwilligung des betroffenen Bürgers oder Bürgerin vorliegt. Das Bundesdatenschutzgesetz beschreibt konkrete Anforderungen für die Sicherstellung des Datenschutzes in Unternehmen und öffentlichen Einrichtungen. Ob diese abstrakten Vorgaben ausreichend umgesetzt sind, ist jedoch häufig eine Frage der Interpretation. Datenschutz kann sowohl pragmatisch und lösungsorientiert, als auch überladen und nahezu geschäftshindernd angegangen werden. Die verarbeitende Stelle und die Umstände definieren die Angemessenheit des Datenschutzniveaus.

In einigen Teilbereichen und Branchen gibt es Präzisierungen und Empfehlungen, die deutlicher die genauen Anforderungen beschreiben. So hat im Jahr 2011 die Konferenz der Datenschutzbeauftragten des Bundes, der Länder und der beiden großen Kirchen in Deutschland eine Orientierungshilfe Krankenhausinformationssysteme (OH-KIS) vorgelegt, die sehr genau die technischen und organisatorischen Anforderungen an IT-Systeme in Kliniken aus Sicht der Datenschützer definieren.

Für Altenheime und andere soziale Einrichtungen gibt noch kein vergleichbares offizielles Dokument. Die Orientierungshilfe Krankenhausinformationssysteme kann jedoch als Grundlage und Orientierung verwendet werden, da die grundsätzlichen Datenarten und viele inhaltliche Forderungen in ähnlicher Form auch auf Einrichtungen in der Sozialwirtschaft angewandt werden können. Unsere Branche ist auch weiterhin im Fokus der Datenschützer.

Die Unsicherheit ist groß, wenn es um schriftliche Anfragen oder gar persönliche Kontrollen durch die Datenschutz-Aufsichtsbehörden geht. Anlassbezogene Prüfungen erfolgen

meist nach einer Anzeige. Immer häufiger werden Unternehmen aber auch stichprobenartig wie bei einer Steuerprüfung angeschrieben und um detaillierte Auskunft zur Umsetzung der Datenschutzgesetze gebeten.

Neben den einschlägigen gesetzlichen Bestimmungen werden aktuelle Themen und Entwicklungen, wie zum Beispiel der Umgang mit Videoüberwachung, E-Mail oder verschlüsselten Datenträgern gezielt untersucht. Einen Überblick über bekannte Aufforderungen zur Offenlegung des Umsetzungsgrades von Datenschutzmaßnahmen gibt dazu einen Eindruck (vgl. Tabelle).

Bei einem unzulässigen Umgang mit den anvertrauten personenbezogenen Daten können durch die Aufsichtsbehörden Bußgelder festgesetzt werden.

In der Praxis werden Bußgelder jedoch eher selten verhängt und der Bußgeldrahmen meist nicht ausgeschöpft. Bei Handlung gegen Entgelt oder anderen schwerwiegenden Verstößen können Freiheitsstrafen von bis zu zwei Jahren nach § 44 BDSG ausgesprochen werden. Problematisch ist hierbei, dass durch die Organ- oder Vertreterhaftung die Verantwortung Geschäftsführern, Vorständen oder anderen Leitungspositionen zugerechnet werden kann (vgl. § 14 StGB). Neben dem Datenschutz sind auch die gesetzlichen Regelungen zur Schweigepflicht zu beachten (siehe § 203 StGB).

Mit der Datenschutznovelle II im Jahr 2009 wurde die Meldepflicht von Datenschutzpannen eingeführt: Unternehmen müssen Kunden oder Mitarbeiter informieren, wenn deren Daten in falsche Hände gelangt sind oder die Kenntniserlangung durch Unbefugte nicht ausgeschlossen werden kann. Im Falle eines überschaubaren Kreises an Betroffenen können diese direkt informiert werden. Das ist jedoch nicht immer möglich oder praktikabel, beispielsweise wenn eine große Menge an Daten verloren gegangen ist oder wenn sich nicht klar bestimmen lässt, wer konkret betroffen sein könnte. Für diesen Fall sieht der Gesetzgeber vor, dass halbseitige Anzeigen in zwei bundesweit erscheinenden Tageszeitungen geschaltet werden müssen, um die Betroffenen zu informieren (§ 42a BDSG).

Neben der beschriebenen Möglichkeit der Anfrage oder Kontrolle durch Aufsichtsbehörden gibt es ein gesetzlich verankertes Recht Betroffener auf Auskunft zu den über sie gespeicherten Daten (vgl. § 34 BDSG). Im Zuge der öffentlichen Debatte um die Weiterentwicklung des Datenschutzes in Europa werden Betroffene von diesem Recht in Zukunft verstärkt Gebrauch machen. Ein geregelter Prozess zum Umgang mit Anfragen von Verbrauchern oder Aufsichtsbehörden sollte Teil des Datenschutzkonzepts in der Einrichtung sein. ■

Themenbereich	Gegenstand der Überprüfung

Allgemeines & Datenschutzbeauftragter	■ Rechtsgrundlagen für die Verarbeitung der verschiedenen Arten personenbezogener Daten (§28 BDSG)
	■ Bestellung des Datenschutzbeauftragten nach §4f BDSG, sofern dieser erforderlich ist, inklusive
	  ■ Nachweise über Fort- und Weiterbildungen
	  ■ Tätigkeitsnachweise wie Jahres- oder Quartalsberichte
	  ■ Datenschutzrichtlinien und Informationen an Mitarbeiter
	  ■ Nachweise über Mitarbeiterschulungen
	■ Richtlinien und Anweisungen zur Einbeziehung des Datenschutzbeauftragten
	■ Vorgesehener Zeitanteil für den Datenschutzbeauftragten sowie ggf. übertragene sonstige Aufgaben
	■ Vorgesehenes Budget für den Datenschutzbeauftragten und dessen Eingliederung in das Unternehmen
	■ Angaben zu Ansprechpartner für betroffene Personen, die ihre Datenschutzrechte wahrnehmen wollen (§ 35 BDSG)

Mitarbeiter & Prozesse	■ Offenlegung des Verfahrensverzeichnisses (§ 4g BDSG)
	■ Verpflichtung von Mitarbeitern auf das Datengeheimnis (§ 5 BDSG)
	  ■ Wann erfolgt die Verpflichtung?
	  ■ Wer hat verpflichtet?
	  ■ Vorlage Musterformular
	■ Auftragsdatenverarbeitung nach § 11 BDSG
	  ■ Offenlegung der externen Dienstleister
	  ■ Vorlage des Mustervertrages
	  ■ Offenlegung der Kriterien, nach denen Dienstleister ausgewählt werden
	  ■ Wie wird die Einhaltung der Auftragsbedingungen überwacht?

Konkrete und aktuelle Themen	■ Einsatz von Videoüberwachung
	  ■ Zu welchem Zweck wird Videoüberwachung eingesetzt
	  ■ Gibt es dazu schriftlichen Festlegungen nach § 6b BDSG?
	  ■ Dokumentation der Überwachungsmittel
	  ■ Details über Beobachtung und Aufzeichnung – wer hat Zugriff darauf?
	  ■ Angaben zu Speicherungszeiten und Löschfristen
	■ Private Nutzung von dienstlichen Kommunikationsmitteln
	  ■ Telefon und Handy, Smartphone, PC und Laptop, Internet, E-Mail
	  ■ Offenlegung der Regelungen
	■ Private Kommunikationsmittel mit dienstlicher Nutzung
	  ■ Smartphone, Laptop
	  ■ Offenlegung der Regelungen
	■ Festlegungen zur Sperrung und Löschung nicht mehr erforderlicher Daten

Technisch-organisatorische Maßnahmen	■ Übersicht über getroffenen technischen und organisatorischen Maßnahmen nach § 9 BDSG
	  ■ Vorlage Gesamtkonzept über die Sicherheitsmaßnahmen
	  ■ Angaben zu externer Auditierung oder Zertifizierung der getroffenen Maßnahmen
	  ■ Einsatz von Verschlüsselung bei mobilen Datenträgern
	  ■ Sichere Löschung von Altgeräten bzw. Altdatenträgern
	  ■ Datenschutzgerechte Entsorgung von Altpapier
	  ■ Versand von personenbezogenen Daten in E-Mails
	■ Vorbereitung zum Umgang mit einer Datenpanne nach § 42a BDSG
	■ Vorhandensein und Nutzung eines Notfallplans

Die Datenschutz-Aufsichtsbehörden verlangen bei Prüfungen umfangreiche Auskünfte von Unternehmen auch der Sozialwirtschaft.