Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte in den katholischen Krankenhäusern Norddeutschlands

Nr. 05/2016

Problem: Aktenvernichtung im Krankenhaus

Der Bayerische Landesbeauftragte für den Datenschutz hat im Jahr 2015 eine flächendeckende Prüfung von Krankenhäusern hinsichtlich der Entsorgung von Patientenakten, Röntgenaufnahmen und anderen wichtigen Unterlagen vorgenommen. Die Ergebnisse dieser Prüfungstätigkeit hat er, gemeinsam mit dem Bayerischen Landesamt für Datenschutzaufsicht in einem 12-seitigen Leitfaden am 22.06.2016 veröffentlicht. Dabei geht es vor allem um die von den Kliniken meistens gewählte Auftragsdatenverarbeitung, bei der die Unterlagen einem Fremdunternehmen zur Vernichtung übergeben werden.

→ https://www.datenschutz-bayern.de/4/info_kh_leitfaden.pdf
→ Pressemitteilung des LfD Bayern und des BLA für Datenschutzaufsicht vom 29.06.2016

Wegen der Relevanz des Themas soll hier deshalb noch einmal auf die Anforderungen bei kirchlichen Krankenhäusern hingewiesen werden.

- Eine Auftragsdatenverarbeitung muss die Vorschriften des § 8 KDO erfüllen. Wesentlich hierbei sind ein schriftlicher Vertrag, die sorgfältige Auswahl des Auftragnehmers, eine dezidierte Beschreibung des Verfahrens und die Bereitschaft Kontrollen des Auftraggebers zu akzeptieren und zu unterstützen.
- Unter Anwendung der ärztlichen Verschwiegenheitspflicht nach § 203 StGB darf der Auftragnehmer keine Möglichkeit zur Einsichtnahme in die ihm zur Vernichtung übergebenen Unterlagen haben. Die Organisation der Sammlung, Übergabe und Vernichtung muss deshalb so gestaltet sein, dass ein unautorisierter Einblick nicht möglich ist. Hierzu kommt beispielsweise die Verwendung eines gesicherten Containers zur Sammlung der Altakten in Betracht.
- Die zu vernichten Unterlagen müssen, solange sie noch unverändert existieren, sich allein im Gewahrsam des Krankenhauses befinden. Nur dann ist der zu Gunsten des Patienten bestehende Beschlagnahmeschutz nach § 91 Abs. 2 StPO gewährleistet!
- Erfüllbar sind diese Voraussetzungen nur dann, wenn die Vernichtung unter Anwendung der DIN 66399 erfolgt. → Mustervertrag zur Vernichtung von Datenträgern nach DIN 66399 (Stand: 30.10.2014). Hierbei hat sich vor allem die unter § 2 Entsorgungsverfahren in den Absätzen 5 – 7 genannte Verfahrensweise bewährt. Das Zerreißen des Papiers wird mit Hilfe eines Spezialfahrzeugs und in Anwesenheit eines Mitarbeiters der Klinik vor Ort durchgeführt.

Der Bayerische Landesbeauftragte weist zudem noch auf folgendes hin:

- Dritte, im Sinne der Auftragsverarbeitung, sind auch Tochtergesellschaften von Krankenhäusern, da diese in der Regel geschaffen werden, „um nicht Teil des Krankenhauses zu sein und selbständig agieren zu können“.
- Das gleiche gilt für eine Dienstleistungs-GmbH des Krankenhauses.
- Krankenhäuser, die zu Klinikkonzernen gehören sind als eigenständige „Mandanten“ in der Datenverarbeitung zu behandeln. Wird die Aktenvernichtung zentral in einem der angeschlossenen Kliniken durchgeführt, muss auch hier ein Auftragsverhältnis nach § 8 KDO vorliegen.

Diese Grundsätze gelten in gleicher Weise auch für kirchliche Krankenhäuser.

Zur Vermeidung und Bekämpfung von Krypto-Trojanern gibt es jetzt ein Lagedossier des BSI

Schon mehrfach wurde an dieser Stelle vor Schadprogrammen gewarnt, die die Daten auf Ihrem Computer unautorisiert verschlüsseln und nur gegen Zahlung einer Geldsumme ein Passwort zur Entschlüsselung bereitstellen (meistens). Gegen diese Erpressungsmetzhoden war nur sehr schwer ein Schutz zu erzielen. Im Mai 2016 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) daher hierzu ein Lagedossier veröffentlicht, in dem die Bedrohungslage, Infektionswege und mögliche Präventionen hiergegen beschrieben werden.
→ BSI, Lagedossier Ransomware

Es wird daher allen betrieblichen Datenschutzbeauftragten, den IT-Technikern und Verwaltungsleitern empfohlen, sich diese Schrift kostenlos herunterzuladen und die eigene Sicherheit an den dort gegebenen Empfehlungen zu überprüfen.