Checkliste für Unternehmen im Gesundheitswesen

Für medizinische Einrichtungen stellt TÜV SÜD eine Checkliste zur Verfügung. Sie ist als Grundlage zur Selbstüberprüfung gedacht und erhebt keinen Anspruch auf Vollständigkeit. Zu beachten sind die jeweils gültigen Rechtsvorschriften unter Beachtung der Bundeslandspezifika.

Prüfung	Vorhanden	Fehlt	Nicht erforderlich
Ist die Benennung eines Datenschutzbeauftragten in meinem Unternehmen erforderlich? (> 9 Personen sind ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt).			
Werden Mitarbeiter hinsichtlich Datenschutz regelmäßig geschult? Steht den Mitarbeitern Informationsmaterial zum Datenschutz zur Verfügung?			
Werden Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, auf das Datengeheimnis nach § 5 BDSG verpflichtet?			
Sind die gesetzlichen Regeln zum Datenschutz bekannt und werden insbesondere die Anforderungen des BDSG eingehalten?			
Das BDSG verlangt in § 4, dass betriebliche und behördliche DSBs ein Verzeichnis führen müssen, das die eingesetzten automatisierten Verfahren erfasst, mit denen personenbezogene Daten verarbeitet werden. Ist dieses gesichert?			
Sind die Räumlichkeiten vor dem Zutritt Unbefugter ausreichend gesichert?			
Sind Regelungen zur Vertraulichkeit und Diskretion im Unternehmen getroffen und umgesetzt?			
Sind Patientenakten bzw. sonstige schriftliche Aufzeichnungen von Patientendaten vor dem Zugriff bzw. dem Einsehen durch Unbefugte geschützt?			
Ist der Zugang zu EDV-Anlagen vor Unbefugten gesichert (Benutzerauthentifizierung und Kennwort, Bildschirmschoner, etc.)?			
Gibt es Zugriffsregelungen zu personenbezogenen Daten in meinem Unternehmen und gibt es ein Zugriffskonzept?			
Sind Passwortregeln formuliert und kommuniziert?			
Werden Daten im Auftrag durch Fremdunternehmen verarbeitet und gibt es dazu die entsprechenden vertraglichen Vereinbarungen (§11 BDSG)?			
Ist der Bereich Fernwartung sicher und klar geregelt? (inkl. Passwort, Verschlüsselung; Zugriffsregelung, -Beschränkung, Dokumentation?)			
Gibt es ein IT-Sicherheitskonzept?			
Wird das Telemediengesetz beim Internetauftritt berücksichtigt?			
Werden Videoüberwachungsanlagen eingesetzt und gibt es hierzu klare Regelungen?			
Werden bei Entsorgung und Reparatur von IT-Systemen und Datenträgern Maßnahmen getroffen, welche eine vollständige Löschung von Datenträgern sicherstellen (inkl. Zusatzprogramme)?			
Wird die regelmäßige Datensicherung und die regelrechte Aufbewahrung der Datensicherung gewährleistet?			
Wird bei der Kommunikation über LAN, WLAN, VoiP der Datenschutz, insbesondere der besonders schützenswerten Patientendaten beachtet und sichergestellt?			

Die TÜV SÜD Akademie bietet 2012 das Seminar „Datenschutz in Einrichtungen des Gesundheitswesens (Patientendatensicherheit)“ an. Mehr dazu unter: www.tuev-sued.de/akademie/datenschutz.
Informationen zum Kurs erteilen Birgit Klusmeier, Tel.: 089 / 5791-3306, E-Mail: birgit.klusmeier@tuev-sued.de und Anita Lenzser, Tel.: 089 / 5791-3691, E-Mail: anita.lenzser@tuev-sued.de.