Datenschutz - Technisch und organisatorische Maßnahmen gemäß § 9 BDSG

Bruno Schierbaum

Mit der verstärkten Einführung und Anwendung von DV-Systemen in den Krankenhäusern werden zunehmend sowohl personenbezogene Daten der Patienten als auch personenbezogene Daten der Beschäftigten erhoben, verarbeitet und genutzt. Vor diesem Hintergrund sind die Krankenhäuser verpflichtet die Datenschutzgesetze umzusetzen und einzuhalten, um den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Krankenhäuser müssen je nach Trägerschaft und geographischer Lage jeweils unterschiedliche Datenschutzgesetze anwenden. Dabei handelt es sich insbesondere um das Bundesdatenschutzgesetz, die Länderdatenschutzgesetze und die Datenschutzgesetze der Amtskirchen (vgl. hierzu Management & Krankenhaus 11/95, S. 12). Da in bezug auf die wichtigsten Vorgaben bei den einzelnen Datenschutzgesetzen keine wesentlichen Unterschiede bestehen, wird im folgenden auf das BDSG Bezug genommen. Um den Schutz der Persönlichkeitsrechte zu gewährleisten, müssen Krankenhäuser vor der Verarbeitung personenbezogener Daten eine Zulässigkeitsprüfung gemäß § 4 BDSG für jedes einzelne Datum vornehmen. Die Verarbeitung ist nur dann zulässig, wenn der Betroffene eingewilligt hat, eine andere Rechtsvorschrift dieses vorschreibt oder erlaubt, oder das BDSG dieses erlaubt. Zudem sind die Rechte der Betroffenen auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung (§§ 33 - 35 BDSG) zu gewährleisten. Als weitere Aufgaben müssen nicht-öffentliche Stellen (Privatbetriebe) und öffentliche Stellen, die personenbezogene Daten verarbeiten technisch und organisatorische Maßnahmen zum Datenschutz gemäß § 9 BDSG treffen. Da das BDSG ein Schutzgesetz darstellt, ergibt sich u.a. die Konsequenz, daß ein Verstoß gegen die aufgeführten Pflichten ein Schadensersatzanspruch nach § 823 Abs. 2 BGB begründen kann.

Datenschutzmaßnahmen nach § 9 BDSG

In § 9 BDSG werden die Anforderungen folgendermaßen festgelegt:

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organsatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemesssenen Verhältnis zu dem angestrebten Schutzzweck steht."

Personenbezogene Daten

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Alle Daten, die einer Person zugeordnet werden können, sei es durch die Aussagekraft der Daten selbst oder beispielsweise durch das Zusatzwissen eines Sachbearbeiters, sind personenbezogene Daten im Sinne des BDSG. Der Begriff „personenbezogene Daten" geht in bezug auf die Beschäftigen über die sogenannten Personalstammdaten hinaus und umfaßt u.a. auch Leistungs- und Verhaltensdaten (z. B. am Patienten erbrachte Leistungen), Werturteile und Qualifikationsdaten im weitesten Sinne. Bei den Daten der Patienten sind die zu schützenden Daten nicht nur die persönlichen Grunddaten wie Name, Vorname, Wohnort, Geburtsdatum etc. sondern auch alle Daten über die am Patienten erbrachten Leistungen. D. h., daß bei der DV-gestützten Verarbeitung dieser Daten die technischen und organisatorischen Maßnahmen nach § 9 BDSG zu treffen sind.

Datenschutz und Datensicherung

Im Zusammenhang mit dem § 9 BDSG tauchen in der einschlägigen Literatur die Begriffe „Datenschutz" und „Datensicherung" auf, wobei die Vorschrift häufig als „Datensicherungsvorschrift" be-

zeichnet wird, obwohl der Begriff selbst in § 9 BDSG nicht vorkommt. Dieses hat seine Ursache darin, daß bereits vor Inkrafttreten des BDSG im Jahre 1977 die Betriebe Datensicherungsmaßnahmen, wie den Schutz von Dateien, Datenträgern, Programmen und DV-Anlagen ergriffen haben. Auch wenn viele Maßnahmen, die zur Datensicherung ergriffen werden, sich auch zur Ausführung der Datenschutzvorschriften eignen, bestehen jedoch in bezug auf die Ziele grundlegende Unterschiede, die nicht verwischt werden sollten. Unter Datensicherung versteht man die Summe von Maßnahmen zur Sicherung des ordnungsgemäßen Ablaufs der Datenverarbeitung durch Sicherung der Hard- und Software und der Daten vor Verlust, Beschädigung und Mißbrauch. Im Rahmen von Datenschutzmaßnahmen geht es insbesondere um die Verhinderung unzulässiger Verarbeitung und Nutzung personenbezogener Daten. Der Unterschied zwischen Datenschutz und Datensicherung ist am besten auf der Ebene des Schutzzweckes zu erkennen: Die Datensicherung dient dem Interesse der datenverarbeitenden Stelle; der Datenschutz dient unmittelbar oder mittelbar dem Interesse des Betroffenen. Da das BDSG gemäß § 1 den Zweck hat, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, handelt es sich bei §-9 BDSG nicht um eine Datensicherungs- sondern um eine Datenschutzvorschrift, auch wenn es bei konkreten Maßnahmen zu Überschneidungen kommt. Vor diesem Hintergrund schreibt das BDSG auch nur solche Maßnahmen vor, die dem Schutzanspruch des Betroffenen dienen.

Verhältnismäßigkeitsprinzip

Die gebotenen technischen und organisatorischen Maßnahmen, die in der Anlage zu § 9 BDSG als Zielvorgaben formuliert sind, sind ausdrücklich dem Verhältnismäßigkeitsprinzip unterstellt: Sie sind nur „erforderlich", d. h. von Gesetzes wegen vorgeschrieben, „wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht" Hierdurch wird klargestellt, daß nicht mit „Kanonen auf Spatzen geschossen werden soll". Die Datenschutzmaßnahmen sind somit nicht Selbstzweck, sondern sind nach dem jeweiligen Schutzzweck auszurichten. Das Verhältnismäßigkeitsprinzip richtet sich jedoch niemals danach, ob die vom Gesetz ausgesprochenen Ge- und Verbote zu beachten sind, sondern einzig und allein um Art und Umfang der Maßnahmen. Bezugspunkte der Maßnahmen sind in jedem Fall die Belange der Betroffenen. Die eigenen Interessen der datenverarbeitenden Stelle müssen bei der Abwägung der Erforderlichkeit im Hintergrund treten.

Bei der Auswahl der technisch und organisatorischen Maßnahmen wird in der Datenschutzliteratur vorgeschlagen, die Daten in Schutzklassen einzuteilen (vgl. hierzu z. B. Der Hamburgische Datenschutzbeauftragte (Hg.): Datenschutzkonzept für PC, Einzelplatzsysteme, Lokale Netze, PC-Host-Kopplung, S. 10 ff.). So sollten die Daten nach ihrer Sensibilität gewichtet und in folgende Stufen eingeteilt werden:

- Stufe A: personenbezogene Daten, deren Mißbrauch keine besondere Beeinträchtigung erwarten läßt;
- Stufe B: personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann;
- Stufe C: personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann, bzw. die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, insbesondere die Daten, die in § 28 Abs. 2 Nr. 1 BDSG aufgeführt sind, die sich auf
  - gesundheitliche Verhältnisse,
  - strafbare Handlungen,
  - Ordnungswidrigkeiten,
  - religiöse oder politische Anschauungen,
  - arbeitrechtliche Rechtsverhältnisse beziehen;
- Stufe D: personenbezogene Daten, deren Mißbrauch für den Betroffenen Gefahren für Leib und Leben bedeuten.

Auch wenn dieses Stufenprinzip in der Praxis als Orientierungshilfe dienen kann, ist eine Einteilung der Daten in Schutzklassen problematisch. So hat das Bundesverfassungsgericht (BVerfG Urteil v. 5.12.1983 NJW 1984 H. 8, S. 419 ff.) im sogenannten Volkszählungsurteil festgestellt, daß es unter den Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr gibt. Dem ist nachdrücklich zuzustimmen, da vermeintlich belanglose Daten durch die Verknüpfung mit anderen Daten eine neue Qualität bzw. andere „Sprengkraft" erhalten. Darüber hinaus handelt es sich bei den Daten, die im Krankenhaus verarbeitet werden, fast ausnahmslos um sehr sensible Daten, die den obersten Schutzklassen zuzuordnen sind. Dieses gilt sowohl für die Gesundheitsdaten der Patienten, aber auch bei den Beschäftigendaten.

Technische und organisatorische Maßnahmen

Die Begriffe „technisch" und „organisatorisch" sind weit auszulegen. So gehören zu den technischen Maßnahmen nicht nur diejenigen, die sich direkt auf die Hard- und Software beziehen, sondern auch das gesamte baulich-räumliche Umfeld. Organisatorische Maßnahmen gehen in der Regel auch mit personellen Regelungen (Vorkehrungen) einher, wie z. B. Verteilung von Aufgaben, Befugnissen und Verantwortung, die Gestaltung des Arbeitsablaufs, die Zugangs- und Zugriffsregelungen oder die Vornahme von stichprobenartigen Erfolgskontrollen.

Wegen der unterschiedlichen Verhältnisse bei den datenverarbeitenden Stellen, ist es nicht möglich, ein allgemeingültiges Datenschutzkonzept zu entwickeln, das als Vorgabe für die Praxis dienen kann. Vielmehr liegt es in der Verantwortung jeder einzelnen Stelle, ein entsprechendes Datenschutzkonzept mit angemessenen technischen und organsatorischen Maßnahmen zu erstellen. So werden nachfolgend Maßnahmenbeispiele aufgelistet. Beim Einsatz von Großrechnern in Rechenzentrum und auch beim Einsatz von Netzwerken (Client-Server) lassen sich die in der Anlage zu § 9 BDSG aufgestellten Anforderungen umsetzen, was aber beim Einsatz von Personal-Computern oder gar Laptops bei einigen Zielvorgaben nicht möglich ist. Vor diesem Hintergrund muß sich die Frage gestellt werden, ob vor diesem Hintergrund die Verarbeitung von sensiblen Daten auf PC oder Laptop nicht ganz unterbleiben muß. Die nachfolgende Aufstellung kann als Checkliste genutzt werden, wobei zum einen geprüft werden muß, welche Maßnahmen im Einzelfall ergriffen werden müssen und zum andern u.U. noch Maßnahmen je nach betrieblichen Gegebenheiten ergänzt werden müssen. Die nachfolgenden Maßnahmen sind angelehnt an den Prüfungskriterien der Aufsichsichtbehörden zum Datenschutz (vgl. § 38 BDSG; vgl. hierzu „Aus der Kontrollpraxis der Aufsichtsbehörden", in: RDV 3/91, S. 158 ff.).

Maßnahmenbeispiele

1. Zugangskontrolle

Anforderung: Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Nr. 1 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Schaffung von Sicherheitsbereichen
- Festlegung befugter Personen
- Berechtigungsausweise, Schlüsselregelung, Codekarten, Besucherausweise
- Anwesenheitsaufzeichnungen
- Regelung des Zugangs betriebsfremder Personen
- Closed-Shop-Betrieb.

2. Datenträgerkontrolle

Anforderung: Es ist zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Nr. 2 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Festlegung befugter Personen
- Absicherung der Bereiche, in denen Datenträger aufbewahrt werden
- Kennzeichnung der Datenträger auch in bezug auf eigene und fremde Datenträger
- Maßnahmen gegen unbefugtes Entfernen
- Ausgabe von Datenträgern nur an authorisierte Personen
- Bestandskontrollen
- Lagerung der Datenträger in einem Sicherheitsbereich (Datenarchiv, Sicherheitsschränke, Tresor)
- Kontrollierte Vernichtung von Datenträgern mit Protokollierung
- Regelung der Anfertigung von Kopien
- Kontrolle der Disketten und mobilen Festplatten sowie der Druckausgaben und deren sichere Verwahrung (PC-Einsatz)
- Einsatz diskettenloser Arbeitsplatzrechner im Netzwerk (PC-Einsatz)
- Sperrung des Copy-Befehls (PC-Einsatz)
- Physisches Löschen nicht mehr benötigter Daten und Dateien, wobei dafür geeignete Dienstprogramme einzusetzen sind.

3. Speicherkontrolle

Anforderung: Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten ist zu verhindern (Nr. 3 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Einsatz von Benutzercodes (Passworte) für Dateien und Progamme
- Regelung über Vergabe, Verwendung und Veränderung von Passwörtern
- Einsatz von Verschlüsselungsroutinen für Dateien, Sicherungssoftware
- Differenzierte Zugriffsregelungen für Prozeduren, Steuerkarten, Verfahren zur Ablaufsteuerung, Befugnis zum Katalogisieren von Programmen
- Richtlinien zur Dateiorganisation
- Protokollierung der Dateibenutzung
- Schriftliche Anweisungen für Wiederanlaufverfahren
- Automatisches Abschalten der Datenstationen (log off) nach längerer Zeit der Nichtbenutzung
- Einsatz von Sicherungssoftware (PC-Einsatz).

4. Benutzerkontrolle

Anforderung: Es ist zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Nr. 4 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Abschließbarkeit von Datenstationen und dezentralen Datenverarbeitungssystemen
- Identifizierung der Terminals/Nutzer gegenüber dem DV-System
- Automatisches Abschalten der Datenstationen bei fehlerhafter Passworteingabe (log off)
- Sperrung der Benutzerberechtigung
- Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals
- Auswertung von Protokollen
- Einsatz von geeigneter Sicherheitssoftware (PC-Einsatz)
- Einsatz von geprüften Verschlüsslungsverfahren (PC-Einsatz).

5. Zugriffskontrolle

Anforderung: Es ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Nr. 5 der Analge zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Anlegen von revisionsfähigen Benutzerprofilen
- Regelung der Zugriffsberechtigungen
- Funktionelle und zeitlich beschränkte Nutzung von Terminals
- Maschinelle Überprüfung der Berechtigung (Identifizierungsschlüssel)
- Auswertung von Protokollen
- Sperren der Betriebssystemebene (PC-Einsatz).

6. Übermittlungskontrolle

Anforderung: Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Nr. 6 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Dokumentation der Abruf- und Übermittlungsprogramme
- Festlegung der Übermittlungswege und der Datenempfänger
- Protokollierung der Datenübermittlung
- Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können.

7. Eingabekontrolle

Anforderung: Es ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Nr. 7 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Datenerfassungsanweisungen
- Plausibilitätskontrollen
- Protokollierung der Eingaben
- Speicherung des Erfassens bei den Eingaben
- Vorgangsprotokollierung für jeden Einzelfall.

8. Auftragskontrolle

Anforderung: Es ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können (Nr. 8 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Sorgfältige Auswahl der Auftragnehmer
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und -geber (Datensicherungsmaßnahmen, Transportregelungen, Aufbewahrungsvorschriften, Vertragsverletzungen, Versicherung).

9. Transportkontrolle

Anforderung: Es ist zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden (Nr. 9 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Verpackungs- und Versandvorschriften (geschlossene Behältnisse)
- Verschlüsselung
- Direktabholung, Kurierdienst, Transportbegleitung
- Sorgfältige Auswahl des Transportpersonals
- Vollständigkeits- und Richtigkeitsüberprüfung.

10. Organisationskontrolle

Anforderung: Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Nr. 9 der Anlage zu § 9 BDSG). Beispiele für Maßnahmen sind:

- Funktionstrennung in räumlicher, organisatorischer und personeller Hinsicht (z. B. Closed-Shop-Betrieb, Stellenbeschreibung)
- Vier-Augen-Prinzip (kein Operateur oder Programmierer mit Zugriff auf personenbezogenen Daten allein im Betrieb)
- Bestellung eines betrieblichen Datenschutzbeauftragten (§ 36 BDSG) bzw. eines behördlichen Datenschutzbeauftragten nach bestimmten Landesdatenschutzgesetzen
- Richtlinien, Arbeitsanweisungen, Verfahrensbeschreibungen
- Regelung von Programmierung, Test und Freigabe
- Regelung zur System- und Programmprüfung
- Datensicherungskonzept, -plan, -katalog
- Katastrophenplanung
- Auflagen zur sicheren Behandlung, Aufbewahrung und Vernichtung von Eingabelisten und Ausdrucken.

Für die Gewährleistung des Datenschutzes und damit auch für die Umsetzung der technischen und organisatorischen Maßnahmen ist die speichernde Stelle (das einzelne Krankenhaus) verantwortlich. Besteht die Verpflichtung gemäß § 36 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen, gehört es zu dessen Aufgaben, auf der Basis der betrieblichen Gegebenheiten ein angemessenes Datenschutzkonzept für einzelne DV-Anwendungen zu entwicklen. Der betriebliche Datenschutzbeauftragte sollte in enger Zusammenarbeit mit den Beschäftigten im EDV-Bereich (Leiter der EDV etc.) mit Unterstützung der Softwarehersteller bzw. -anbieter den Datenschutz umsetzen und dokumentieren. Der Betriebsrat

hat gemäß § 80 Abs. Nr. 1 BetrVG die Aufgabe die Einhaltung des Datenschutzgesetzes zu überwachen. Dieses gilt in gleicher Weise für den Personalrat z. B. nach § 68 Abs. 1 BPersVG. Darüber hinaus haben Betriebs- und Personalräte Mitbestimmungsrechte bei der Einführung und Anwendung von EDV-Technologien (z. B. § 87 Abs. 1 Nr. 6 BetrVG oder § 75 Abs. 3 Nr. 17 BPersVG). Als externe Kontrollinstanzen kommen die Aufsichtsbehörden bzw. je nach Anwendung des entsprechenden Datenschutzgesetzes der Landesdatenschutzbeauftragte oder Bundsdatenschutzbeauftragte in Betracht.

erschienen in: Management & Krankenhaus
Nr. 5/96, Seite 18 - 20

Bruno Schierbaum
BTQ Niedersachsen
(Beratungsstelle für Technologiefolgen und Qualifizierung)
Donnerschweerstr. 84
26123 Oldenburg
Tel: 0441/82068
Fax: 0441/83824