2 Grundlagen und Begriffe

Grundsätzlich ist für den Datenschutz in Apotheken das Bundesdatenschutzgesetz anwendbar.

Das Bundesdatenschutzgesetz (BDSG) formuliert seinen Zweck im ersten Artikel so: „*Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.*"

Das bedeutet, dass der Schutzbereich des Bundesdatenschutzgesetzes immer dann eröffnet ist, wenn personenbezogene Daten durch nicht-öffentliche Stellen (in diesem Fall durch Apotheken) erhoben, verarbeitet und genutzt werden dies unter Einsatz von Datenverarbeitungsanlagen oder aus nicht automatisierten Dateien erfolgt.

Im Kontext des Datenschutzes gibt es also reichlich zu klärende Begriffe und Definitionen, um festzustellen ob das Bundesdatenschutzgesetz anzuwenden ist. Die Begriffe sind im folgenden Kapitel definiert.

2.1 Personenbezogene Daten

Der Gesetzgeber formuliert im § 3 Abs. 1 BDSG den Begriff „Personenbezogene Daten" als „*Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person*".

Hinter dieser juristischen Formulierung verbergen sich einige Begriff, die für die Praxis von nicht unerheblicher Bedeutung sind.

2.1.1 Natürliche Person

Eine natürliche Person ist der Mensch in seiner Rolle als Rechtssubjekt. Rechtssubjekte haben die Fähigkeit, Träger von Rechten und Pflichten zu sein; sie besitzen Rechtsfähigkeit. Die Rechtsfähigkeit eines Menschen beginnt mit der Vollendung der Geburt und endet mit seinem Tod.

In Abgrenzung und zur Unterscheidung zur natürlichen Person kennt die Rechtsordnung den Begriff der juristischen Person. Grundform der juristischen Personen des Privatrechts ist der Verein. Daneben gehören zu den juristische Personen:

- Stiftungen
- Kapitalgesellschaften (Aktiengesellschaften, Gesellschaften mit beschränkter Haftung)
- Genossenschaften (e. G.)

Aus der Definition zum Begriff der „personenbezogenen Daten“ wird deutlich, dass der Schutzbereich des Datenschutzes nur für Menschen gilt.

2.1.2 Bestimmt oder bestimmbar

Die Artikel-29-Datenschutzgruppe hat in einem Arbeitspapier definiert, dass eine natürliche Person als „bestimmte Person“ anzusehen ist, wenn sie sich in einer Personengruppe von allen anderen Mitgliedern der Gruppe unterscheidet (vgl. Art. 29 Datenschutzgruppe, WP 136, Abschnitt 3 Nr. 3).

ARTIKEL-29-DATENSCHUTZGRUPPE Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes. Die Artikel-29-Datenschutzgruppe hat vornehmlich beratende Funktion. Sie kann aber auch von sich aus zu allen Fragen Empfehlungen abgeben und Stellung beziehen, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Gemeinschaft betreffen.

Bestimmbar ist eine Person, wenn die Daten direkt mit dem Namen der Person in Verbindung stehen oder der Bezug sich unmittelbar herstellen lässt (vgl. Gola/Schomerus, BDSG § 3 Rn. 10). Werden Daten über eine anwesende Person erhoben oder verarbeitet, so ergibt sich deren Bestimmtheit bereits allein aus ihrer Gegenwart; dabei ist es unerheblich, ob ihr Name oder andere Identifikationsmerkmale bekannt oder feststellbar sind (vgl. Dammann in: Simitis (Hrsg.), BDSG § 3 Rn. 22). Für die Praxis bedeutet dies, dass es sich bei einem Kunden, der ein Medikament bzw. ein Produkt kauft, um eine bestimmte natürliche Person handelt.

Beispiele für bestimmte natürliche Personen

Der Herr Müller aus der Arbeitsgemeinschaft hat ...
Die Frau Meier aus der Zentrale ist ...
Der Kunde da möchte ...

Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der Stelle an, die die Daten speichert. Die speichernde Stelle muss den Bezug mit den ihr zur Verfügung stehenden Mitteln und ohne unverhältnismäßigen Aufwand herstellen können (vgl. Gola/Schomerus, BDSG § 3 Rn. 10).

Das macht auch die Europäische Datenschutzrichtlinie 95/46/EG deutlich. Im Erwägungsgrund 26 heißt es dort: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.“

Die rein hypothetische Möglichkeit zur Bestimmung der Person reicht nicht aus, um die Person als „bestimmbar“ anzusehen.

Wenn „alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten“ diese Möglichkeit aber nicht besteht oder vernachlässigbar ist, ist die Person nicht als „bestimmbar“ anzusehen, und die Informationen würden nicht als „personenbezogene Daten“ betrachtet werden (vgl. Art. 29 Datenschutzgruppe, WP 136, Abschnitt 3 Nr. 3).

Tab. 3.1 Beispiel Checkliste

Sind die Mitarbeiter verpflichtet die Fenster und Türen zum Ende der Arbeitszeit zu verschließen?	☐ Ja Augenschein: ☐	☐ Nein	
	Bemerkung:		Bemerkung:
			Korrekturmaßnahme erforderlich:
			☐ Ja ☐ Nein
			Maßnahme:

bestätigt haben, kann dies in der Checkliste zusätzlich unter Augenschein vermerkt werden.

Unter der Überschrift „Abweichung" können bereits im Audit Informationen festgehalten werden, die für die Erstellung eines Berichtes berücksichtigt werden können. Ist z. B. in der Apotheke geregelt, dass ein Passwort grundsätzlich mit der Mindestlänge von acht Zeichen für Anwendungen und Systeme zu verwenden ist, im Audit hingegen eine maximale Passwortlänge von sechs Zeichen festgestellt ist, kann dies als Abweichung im Auditplan notiert werden.

Werden Korrekturmaßnahmen zur Behebung der Abweichung festgelegt, können diese auch im Auditplan festgehalten werden. Sinnvoll kann es eventuell sein, im Audit noch keine konkreten Maßnahmen zu definieren, sondern das Ergebnis von weiteren Audits abzuwarten, um gegebenenfalls die Maßnahmen zu konsolidieren und gemeinsam umzusetzen zu können. Die hier genannten Punkte sind als Beispiele zu verstehen und können an die Anforderungen der jeweiligen Apotheke angepasst werden.

Im Kern der Auditierung sollten die Verfahren automatisierter Verarbeitung (▸Kap. 3.5) stehen. Durch die Verbindung der Anwendungen, mit denen personenbezogene Daten verarbeitet werden, über die Verfahren automatisierter Verarbeitung erhält man eine ideale Ausgangslage für die Prüfung. Die Verfahren automatisierter Verarbeitung enthalten alle wesentlichen Informationen, um eine Bewertung der oben genannten Anforderungen vornehmen zu können.

Die Datenschutzaudits können gegebenenfalls auch Bestandteil der regelmäßigen Überprüfungen im Rahmen des Qualitätsmanagementsystems nach § 2a der Apothekenbetriebsordnung sein. So wird die Anzahl der internen Kontrollen bzw. Inspektionen reduziert und die Störung der Betriebsabläufe minimiert.

3.4.2 Schulung der Mitarbeiter

Den Datenschutzbeauftragten fällt die gesetzliche Aufgabe zu, die Personen, die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, mit den Vorschriften des Bundesdatenschutzgesetzes und anderen Vorschriften über den Datenschutz vertraut zu machen. Dazu hat der Datenschutzbeauftragte geeignete Maßnahme auszuwählen. Im Rahmen seiner Weisungsfreiheit ist er berechtigt, unter Berücksichtigung der Erfordernisse und Möglichkeiten der Apotheke selbst zu bestimmen, welches die geeigneten Maß-

nahmen zur Schulung der Mitarbeiter sind. Der Datenschutzbeauftragte wird auf der Grundlage seiner Fachkunde und Kenntnisse der Prozesse und Verfahren in der Apotheke selbst Inhalt und Verlauf der Schulung festlegen. Auch bei der Auswahl der Teilnehmerinnen und Teilnehmer wirkt er mit.

Die Möglichkeiten zur Information und Schulung der Mitarbeiter sind vielfältig. Sie reichen von Veranstaltungen, Seminaren bis hin zum persönlichen Gespräch, von der Herausgabe allgemeiner Lehr- und Schulungsunterlagen bis hin zu aktuellen arbeitsplatzbezogenen Informationen und Verfahrensrichtlinien.

Der Datenschutzbeauftragte soll entscheiden, inwieweit es hilfreich ist, bestimmte Mitarbeiter oder Mitarbeitergruppen mit aktuellen Informationen zu gesetzlichen Neuerungen (z. B. durch einen E-Mail Newsletter) zu versorgen.

Grundsätzlich muss es sich bei den verwendeten Unterlagen und Inhalten nicht zwingend um solche handeln, die der Beauftragte selbst erstellt hat. Er kann sich auch auf Schulungsunterlagen oder Präsentationen stützen, die von Dritten stammen. Entscheidend ist, dass die Auswahl durch ihn erfolgt, um sicherzustellen, dass die Inhalte für die Mitarbeiter geeignet sind und alle relevanten Vorschriften in die Schulung einfließen. Die Beauftragten müssen die Schulung grundsätzlich selbst durchführen. Das Hinzuziehen von Experten oder Dozenten kann jedoch angebracht und somit zulässig sein. Die Dozenten erfüllen eine reine Hilfsfunktion und sind verpflichtet sich an die Vorgaben des Datenschutzbeauftragten zu halten. Somit ist eine Delegation der Schulungsaufgabe des Datenschutzbeauftragten damit nicht verbunden.

Es gibt keine Vorgaben zur Häufigkeit von Schulungen. Es ist allerdings empfehlenswert einen Rhythmus im Rahmen eines Schulungsplanes festzulegen, der sicherstellt, dass alle Mitarbeiter in der Apotheke mit den besonderen Anforderungen des Datenschutzes und der Sensibilität der Datenverarbeitung von Gesundheitsdaten vertraut ist. Mindestens alle drei Jahre sollten alle Mitarbeiter durch den Datenschutzbeauftragten persönlich vertraut gemacht werden. In der Zwischenzeit kann der Datenschutzbeauftragte andere, geeignete Maßnahmen wählen.

Grundsätzlich können alle neuen Mitarbeiter in Rahmen eines Einführungs- oder Begrüßungsschreibens mit den allgemeinen Anforderungen und Fragen des Datenschutzes sowie mit der Rolle der Person als Datenschutzbeauftragten vertraut gemacht werden. Als Informationsgrundlage kann das Merkblatt zum Bundesdatenschutzgesetz herangezogen werden.

Merkblatt über wichtige Regelungen des Bundesdatenschutzgesetzes (BDSG)

1. Gegenstand des Datenschutzes

Zweck des Bundesdatenschutzgesetzes ist es, den Einzelnen davor zu schützen, dass er durch Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Dazu gehören bereits Name und Anschrift.

Daneben kennt das Bundesdatenschutzgesetz noch die besonderen Arten von personenbezogenen Daten. Dazu gehören: Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Sexualleben und insbesondere Angaben über die Gesundheit.

Diese Daten sind noch vertraulicher zu behandeln, da die Auswirkungen auf den Betroffenen bei Missbrauch, Verrat oder Diebstahl deutlich höher ausfallen können.

6 Technische und organisatorische Maßnahmen

Das Bundesdatenschutzgesetz fordert von der verantwortlichen Stelle, dass sie Maßnahmen zum Schutz der personenbezogenen Daten, die sie erhebt, verarbeitet oder nutzt, zu treffen hat.

Der Apotheker ist verpflichtet die Organisation seiner Apotheke so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Begriff der Organisation wird hier als Aufbau- und Ablauforganisation zu verstehen sein.

Die **Aufbauorganisation** gliedert die Aufgaben der Apotheke in Aufgabenbereiche und bestimmt die Stellen und Personen, die diese bearbeiten sollen. Als Ergebnis zeigt sich eine Struktur als Verknüpfung dieser organisatorischen Grundelemente, die sich als Organigramm darstellen lässt (Abb. 6.1).

Ablauforganisation baut auf den Ergebnissen der Aufbauorganisation auf, indem sie die einzelnen Aufgaben und die zu ihrer Erfüllung notwendigen Verrichtungen verbindet (Abb. 6.2). Die Arbeitsvorgänge müssen in der Apotheke geordnet ablaufen. Als Definition für eine Ablauforganisation kann gelten: „Das zeitliche und örtliche Hinter- und Nebeneinander der zur Erreichung eines bestimmten Arbeitsergebnisses auszuführenden Arbeiten". Heute wird der Begriff der Ablauforganisation zunehmend abgelöst durch Begriffe wie „Prozessmanagement" oder „Workflow-Management".

Daneben sind insbesondere Maßnahmen zu treffen, die geeignet sind personenbezogene Daten zu schützen. Wobei die „Eignung" der technischen und organisatorischen Maßnahmen von der Art der Daten oder Datenkategorien abhängt. Grundsätzlich gilt, dass Maßnahmen nur erforderlich sind, wenn ihr Aufwand in einem angemessenen Ver-

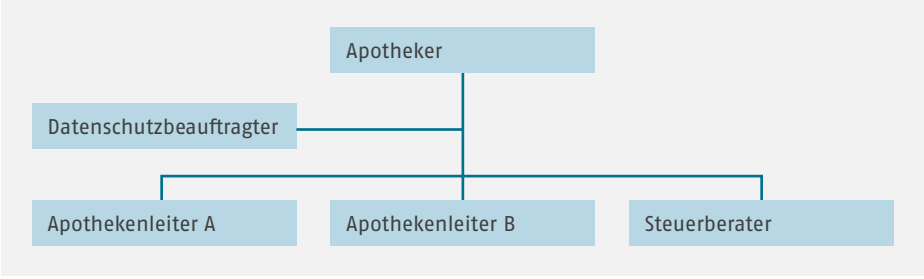

Abb. 6.1 Aufbauorganisation

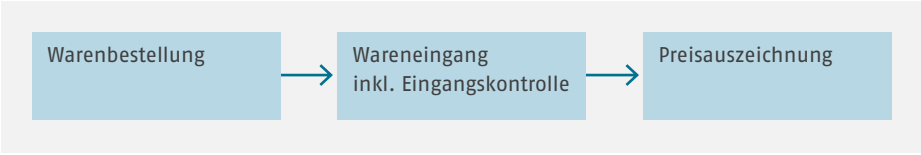

Abb. 6.2 Ablauforganisation

hältnis zum angestrebten Schutzzweck steht. Es soll nicht mit „Kanonen auf Spatzen geschossen" werden. Das kann allerdings nicht bedeuten, dass aufgrund des hohen zeitlichen oder finanziellen Aufwandes auf Maßnahmen verzichtet werden kann, die grundsätzlich erforderlich sind um den Datenschutz zu gewährleisten. Für die Bewertung der Angemessenheit und Erforderlichkeit für technische und organisatorische Maßnahmen kann die Betrachtung von Gefährdungen und daraus resultierenden Risiken im Rahmen der Vorabkontrolle herangezogen werden (▸Kap. 3.4.3).

Die technischen und organisatorischen Maßnahmen werden in acht Kontrollbereiche aufgegliedert. In der Praxis wird dafür auch der Begriff der „8 Gebote" verwendet.

6.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Unter Zutritt ist die räumliche Annäherung einer Person zu verstehen. Im Allgemeinen ist es ausreichend, dass Unbefugte den Raum, in dem Datenverarbeitungsanlagen aufgestellt sind, nicht betreten können. Je früher ein Unbefugter von den Datenverarbeitungsanlagen ferngehalten wird, desto besser.

Als Maßnahmen in einer Apotheke kommen z. B. folgende in Betracht:

- **Einteilung in Sicherheitszonen/Sperrbereiche:** Datenverarbeitungsanlagen sollten in Räumen mit einer eigenen Schließanlage/Schließung aufgestellt sein. Der Kreis der berechtigten Personen ist auf das notwendige Maß zu beschränken. Fenster und Türen zu den Räumen, in denen die zentralen Systeme (Server, Datensicherung, etc.) aufgestellt sind, sollten gegen unbefugtes Eindringen besonders geschützt sein. Dazu gibt es eine Norm für die Widerstandsklassen von Fenstern und Türen, die EN1627:2011 (□Tab. 6.1).
- **Schlüsselregelung:** Der Zutritt zu den Räumen der Apotheke sowie den zentralen Räumen, in denen die Datenverarbeitungsanlagen aufgestellt sind, ist zu regeln. Es sollten Schlüssel für die einzelnen Bereiche vorhanden sein und die Herausgabe sowie die Rückgabe der Schlüssel sind in einer Liste zu dokumentieren.
- **Automatische Zutrittskontrolle:** Vielfach werden die „klassischen" Schlösser durch elektronische Zutrittskontroll-Einrichtungen ersetzt. Dazu zählen Schlösser mit biometrischen Verfahren (z. B. Finger- oder Handabdruck) sowie Schlösser, die sich mit Transpondern, Chips oder Karten öffnen lassen. Die Anschaffungskosten über die Schlösser sind häufig höher als für „klassische" Sicherheitsschlösser, der Aufwand für die Verwaltung und Pflege der Berechtigungen wird jedoch reduziert. So kann z. B. eine Chipkarte aus dem Register der zugelassenen Karten bei Verlust entfernt werden. Es reicht also aus eine Einstellung in der Verwaltungssoftware vorzunehmen. Das Schloss muss nicht ersetzt werden. Dies ist gerade bei zentralen Schließanlagen ein