Datenschutz in der Apotheke – Neuerungen durch die DSGVO

Stand Mai 2018

Version 1.0
Apothekerverband Westfalen-Lippe (AVWL)

Vorab

„Wenn Daten das neue Öl sind, ist Datenschutz der neue Umweltschutz."
(aus dem Dokumentarfilm „Democracy – im Rausch der Daten" von David Bernet)

Mit der Datenschutz-Grundverordnung (DSGVO) treten am 25.05.2018 europaweite Standards für den Datenschutz in Kraft. Die DSGVO wirkt unmittelbar und zwingend sowohl für private als auch für öffentliche Stellen und wird ergänzt durch das neue Bundesdatenschutzgesetz (BDSG-neu).

Öffentliche Apotheken gehen mit besonders sensiblen Daten um: den Gesundheitsdaten der Patienten bzw. Kunden sowie den Daten Minderjähriger. Umso wichtiger ist es, sich mit der damit einhergehenden Verantwortung und den durch das Datenschutzrecht formulierten Anforderungen auseinanderzusetzen.

Beachten Sie, dass die Anforderungen zwar grundsätzlich bereits bis zum 25.05.2018 umgesetzt sein müssen. Allerdings kann von Ihnen zum Stichtag eine punktgenaue und jedes Detail umfassende Umsetzung kaum erwartet werden. Dafür ist die Komplexität der DSGVO zu groß. Sie stellt selbst die Datenschutzbehörden vor eine enorme Herausforderung und Kraftanstrengung. So hat bspw. die für Sie zuständige Landesdatenschutzbehörde in Nordrhein-Westfalen (LDI NRW) bereits verkündet, dass die Mitteilung der Kontaktdaten des Datenschutzbeauftragten – an sich sind diese meldepflichtig bis zum 25.05.2018 – zunächst nicht möglich sein wird, denn die beabsichtigte Zurverfügungstellung eines entsprechenden Online-Tools über die Homepage des LDI scheint nicht fristgerecht zu gelingen. Mitteilungen, die vor der Fertigstellung eingingen, könnten laut LDI nicht berücksichtigt werden. Weitere Informationen seien in den kommenden Monaten auf der LDI-Homepage nachzulesen. Zudem beabsichtige man, unterlassene Meldungen der Kontaktdaten der/des Datenschutzbeauftragten während einer Übergangszeit bis zum 31.12.2018 nicht als Datenschutzverstöße zu verfolgen oder zu ahnden.

Erwartet wird von Ihnen zum 25.05.2018 – das haben Vertreter der Landesdatenschutzbehörde zurückliegend auf verschiedenen Veranstaltungen stets betont – eine generelle Sensibilität für die Thematik sowie ein nachhaltiges Bemühen. Beides setzt eine vertiefte Auseinandersetzung mit der Materie voraus. Viele Regelungen der DSGVO sind für Sie als Apothekeninhaber(in)[1] auch in der Vergangenheit schon verpflichtend gewesen. Wer diesen Verpflichtungen daher nachgekommen ist und entsprechendes Knowhow besitzt, für den wird die Umsetzung der DSGVO mit überschaubarem Aufwand zu meistern sein.

Der Fokus der Neuerungen durch die DSGVO liegt auf der Rechenschaftspflicht des für die Verarbeitung Verantwortlichen und dem hierdurch erforderlichen Datenschutz-Management-System (DSMS), das die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen darstellt, mit denen der datenschutzkonforme Umgang mit personenbezogenen Daten im Unternehmen systematisch gesteuert und kontrolliert wird.

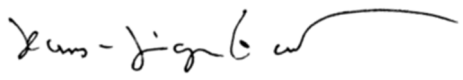
Datenschutz wird nicht statisch verstanden, sondern ist ein lebendiger, dynamischer und mitunter täglicher Prozess, der immer wieder neue Prüfungen, Anpassungen und Dokumentationen erfordert. Eine persönliche Auseinandersetzung mit den maßgeblichen Regelungen und Anforderungen ist unumgänglich. **Datenschutz ist Chefsache!** Die Einführung regelmäßiger Prozesse und Routinen wie Mitarbeiterbesprechungen, Prozessanalysen, Überprüfungen, Checklisten etc. helfen dabei nicht nur den Überblick zu behalten, sondern auch das gesamte DSMS effizient auszugestalten. Der zu betreibende Aufwand lässt sich so auf das nötige (aber auch zu leistende) Maß reduzieren.

[1] Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beiderlei Geschlecht.

Die nachfolgenden Ausführungen sollen Ihnen als Apothekeninhaber und damit Verantwortlichem im Sinne der DSGVO/des BDSG-neu eine Hilfe zur Selbsthilfe bieten. Sie enthalten das aus unserer Sicht Wichtigste, beabsichtigen zugleich aber nicht die allumfassende Behandlung aller denkbaren Themen und Probleme. Die Unterschiedlichkeit der Erscheinungsformen von Apotheken sowie die Vielschichtigkeit der Tätigkeit in Apotheken bedingen zudem je nach Fall eine intensivere Auseinandersetzung mit einzelnen Punkten. Erschwerend kommt hinzu, dass es zu vielen mit der DSGVO verbundenen Fragestellungen bislang nicht nur kein gefestigtes Meinungsbild gibt, sondern es existieren vor allen Dingen kaum Auslegungs- und Umsetzungsempfehlungen für Apotheken durch die Datenschutzbehörden. Zumindest kurz angemerkt sei in diesem Zusammenhang, dass mittels der DSGVO erstmals per EU-Verordnung der Versuch einer Vereinheitlichung des Datenschutzes unternommen wird. Die Einführung der DSGVO hat nicht nur zu neuen Begrifflichkeiten, sondern auch teilweise zu neuen Rechtspflichten geführt. Ferner weist sie eine Vielzahl unbestimmter Rechtsbegriffe auf. Zwangsläufig verbunden sind damit Auslegungs- und Anwendungsschwierigkeiten. Viele der den Apothekenalltag betreffenden, noch offenen Fragestellungen werden sich daher erst in den kommenden Wochen und Monaten eingrenzen und (hoffentlich) klären lassen. Bis zu den ersten – letztlich maßgeblichen – gerichtlichen Entscheidungen wird weitere Zeit ins Land gehen.

Wir werden diese Entwicklungen aufmerksam für Sie begleiten und Sie regelmäßig über Neuerungen informieren. Dazu gehört auch, dass wir diesen Leitfaden anlassbezogen überarbeiten werden, was Sie an der Angabe zur Version auf dem Deckblatt und in den Kopfzeilen ersehen können. Dies gilt auch für die übrigen Handreichungen wie die auf der Internetseite eingestellten Merkblätter und Formulare. Bitte kontrollieren Sie auch diese regelmäßig auf den aktuellen Stand.

Schließlich ist mit Blick auf das vorstehend Gesagte zwangsläufig verbunden, dass wir – trotz sorgfältigster Recherche und Aufbereitung der Themen – **keinerlei Haftung** für die Inhalte des Leitfadens, der weiteren Handreichung und sonstigen, auf der Internetseite eingestellten Informationen übernehmen können. In Zweifelsfragen sollten Sie sich daher z.B. an einen auf das Datenschutzrecht spezialisierten Anwalt wenden. Wir bitten insoweit um Verständnis.



Hans-Jürgen Simacher
AVWL-Geschäftsführer

Inhaltsverzeichnis:

Abkürzungen:

BDSG – Bundesdatenschutzgesetz
DSB – Datenschutzbeauftragter
DSFA – Datenschutzfolgeabschätzung
DSGVO – Datenschutzgrundverordnung
DSMS – Datenschutz-Management-System
LDA Bayern – Bayerisches Landesamt für Datenschutzaufsicht
LDI NRW – Landesbeauftragte für Datenschutz und Informationsfreiheit NRW
TOM – technisch-organisatorische Maßnahmen

1. Warum Datenschutz?

In der DSGVO geht es um den Schutz personenbezogener Daten. Hierunter fallen alle Angaben, die sich einem bestimmten Menschen zuordnen lassen und diesen dadurch identifizieren oder identifizierbar machen kann (Art. 4 Abs. 1 DSGVO). Beispiele für personenbezogene Daten sind: Name, Geburtsdatum, Kontaktdaten wie Adressen und Telefonnummer, Kontodaten, Krankenversicherungsnummern etc.

Besondere Arten personenbezogener Daten, die in höherem Maße sensibel sind, unterliegen sogar einem verschärften Schutz. In diese Kategorie fallen unter anderem auch Angaben zur Gesundheit (Gesundheitsdaten).

Warum müssen sich gerade Apotheker an den Datenschutz halten?
Datenschutz betrifft nahezu alle Branchen und Institutionen. Insbesondere gilt er aber im Gesundheitsbereich, also bspw. für Ärzte, Zahnärzte, aber auch Krankenkassen. Strengen Pflichten unterliegt daher auch der Apotheker bei der Verarbeitung sensibler Gesundheitsdaten, die er zudem teilweise an Dritte (z.B. das Rechenzentrum oder den Verband) übermittelt.

Datenschutz umfasst auch den „Offline"-Datenschutz, also z.B. die Einhaltung von Diskretionsabstand, Umgang mit Fax-Sendeberichten oder nicht mitgenommenen Kassenzetteln, Sichtfelder auf PC-Bildschirmen, Reichweite von Mithörgelegenheit bei Telefonaten in normaler Lautstärke, Botendienst, handschriftliches Notieren von Arzneimittelvorbestellungen etc.

2. Die wichtigsten Neuerungen

- Empfindliche Sanktionen: Bußgelder je nach Verstoß bis zu 2% des Jahresumsatzes bzw. 10 Mio. EUR oder 4% des Jahresumsatzes bzw. 20 Mio. EUR
- Wettbewerbsrecht: Im Sinne eines Mitbewerberschutzes eröffnet die DSGVO neue Möglichkeiten für Abmahnungen, zivilgerichtliche Verfügungs- und Hauptsacheverfahren, Auskunftsansprüche etc.
- Behörden-Befugnisse: Aufforderung zur Bereitstellung der erforderlichen Informationen und Zugang hierzu, Datenschutzprüfungen etc.
- Erweiterung der Pflicht, einen Datenschutzbeauftragten zu benennen
- Geänderte Rahmenbedingungen des Verarbeitungsverzeichnisses
- Durchführung von Datenschutzfolgeabschätzungen
- Erweiterung der Rechte der Betroffenen
- Ausweitung der Transparenzpflichten
- Erstellen eines Löschkonzeptes
- Erstellen und Ausführen eines DSMS
- Meldung von Datenschutzverstößen binnen 72 Stunden

ACHTUNG: Erhöhte Gefahr für Abmahnungen etc. durch u.a. Mitbewerber!

3. Was unterscheidet den Datenschutz von der Schweigepflicht des Apothekers?

Der Datenschutz hat den Zweck, das Recht jedes einzelnen Menschen zu gewährleisten, selbst über seine Daten zu bestimmen. Datenmissbrauch soll verhindert und die Privatsphäre des Einzelnen geschützt werden. Daten sollen u.a. vor dem unberechtigten Zugriff Dritter geschützt werden. Sie dürfen ferner nur in dem für den Zweck der Speicherung erforderlichen Umfang und für die erforderliche Zeit „festgehalten" und nur für

diese Zwecke genutzt werden. Beispielsweise berechtigt Sie ein Ihnen durch Vorlage einer Verordnung bekannt gewordenes Geburtsdatum nicht zum Versenden von Glückwünschen an den Kunden. Dieser Verstoß gegen das Datenschutzgesetz stellt jedoch keine Verletzung Ihrer Schweigepflicht dar. Die Schweigepflicht betrifft das unbefugte Offenbaren von fremden Geheimnissen, die Ihnen im Rahmen Ihrer Berufsausübung bekannt geworden sind. Gratulieren Sie Ihrem Kunden aufgrund der Ihnen vorgelegten Verordnung zum Geburtstag, verletzen Sie also nicht Ihre Schweigepflicht, denn Ihr Kunde ist kein Dritter, dem Sie etwas ihm Unbekanntes offenbaren.

In manchen Fällen kann jedoch sowohl ein Verstoß gegen das Datenschutzgesetz als auch gegen die Schweigepflicht vorliegen. Dies ist z.B. der Fall, wenn Sie an einen Hersteller von Inkontinenzprodukten die Adresse und das Geburtsdatum Ihrer Inkontinenzkunden weitergeben.

4. Glossar: Wichtige Begriffe der Datenschutzgrundverordnung (DSGVO)

Allg. Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO):

Rechtmäßigkeit der Datenverarbeitung:
Bei der Datenverarbeitung gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt, d.h. die Verarbeitung personenbezogener Daten ist grundsätzlich verboten – außer es liegt eine ausdrückliche Erlaubnis vor. Die Erlaubnis zur Datenverarbeitung ist zum Beispiel im Fall einer gesetzlichen Regelung oder einer individuellen Einwilligung des Betroffenen gegeben. Ferner dann, wenn die Verarbeitung zur Erfüllung eines Vertrages erforderlich ist. Handelt es sich bei den personenbezogenen Daten um Gesundheitsdaten, dann sind die Anforderungen an die Rechtmäßigkeit noch strenger, d.h. es kommen nur noch bestimmte, ausgewählte Rechtsgrundlagen als Erlaubnis in Betracht, die von den allgemeinen, oben genannten, abweichen. Bspw. reicht es für die Rechtmäßigkeit einer Verarbeitung von Gesundheitsdaten grundsätzlich nicht aus, dass diese zum Zwecke der Erfüllung eines Vertrages erfolgt.

Keine Datenverarbeitung ohne Rechtsgrundlage!

Zweckbindung:
Die Datenverarbeitung ist nur zu einem bestimmten Zweck erlaubt. Dieser Zweck muss vorab festgelegt sein und dem Betroffenen bekannt gemacht werden. Erheben Sie also z.B. Daten eines Kunden, um für diesen ein Bonuskonto zu führen oder ihm eine steuerliche Bescheinigung über seine Medikamentenkäufe zukommen zu lassen, dann dürfen Sie ihn deswegen nicht zugleich auch anschreiben, um ihm zum Geburtstag zu gratulieren, es sei denn, auch dieser Zweck ist vorab festgelegt worden und die Verarbeitung erfolgt auf Basis einer Rechtsgrundlage, hier einer Einwilligung des Kunden.

Legen Sie vorab die Zwecke fest, für die Sie personenbezogene Daten verarbeiten wollen.

Datenminimierung:
Es dürfen nur die Daten erhoben werden, die zur Zweckerreichung notwendig sind. Im Beispielsfall der Führung eines Bonuskontos und/oder der Übermittlung von Steuerbescheinigungen wäre es also nicht notwendig, auch die Konfession des Kunden abzufragen, denn diese spielt für die Zweckerreichung keine Rolle.

Datenrichtigkeit:
Die über die betroffene Person gespeicherten Daten müssen mit der Realität übereinstimmen, ggf. sind sie zu korrigieren. Führen Sie also eine Kundendatei, dann müssen Sie regelmäßig nachfragen, ob die erhobenen Daten nach wie vor zutreffen.

Personenbezogene Daten (z.B. Kundenkartei) müssen regelmäßig auf ihre Richtigkeit überprüft werden.

Speicherbegrenzung:
Ist der angestrebte Zweck erreicht, dann sind die Daten zu löschen. Möchte Ihr Kunde also nicht mehr am Bonusprogramm teilhaben und/oder keine Steuerbescheinigungen mehr erhalten, dann sind seine Angaben, die zu diesem Zweck gespeichert wurden, zu löschen. Um dies zu gewährleisten, ist eine getrennte Speicherung der Daten nach Zweck der Verarbeitung möglicherweise erforderlich.

Integrität/Vertraulichkeit:
Personenbezogene Daten dürfen nur in einer Art und Weise verarbeitet werden, die eine angemessene Daten-Sicherheit gewährleistet. Zur Risikoprävention sind daher u.a. geeignete technische und organisatorische Maßnahmen zu ergreifen.

Personenbezogene Daten:
Der Apothekeninhaber hat täglich vielfältige Kontakte mit anderen Personen. So etwa zu seinen Mitarbeitern, seinen Kunden und Patienten. Darüber hinaus hat er Beziehungen zu Dienstleistern wie seinem Rechenzentrum, seinem Großhändler oder seinem Verband. Ferner hält er z.B. Rücksprache mit Ärzten, Krankenhäusern, Pflegeheimen etc. Alle aus diesen Kontakten resultierenden unmittelbaren oder mittelbaren Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, sind personenbezogene Daten im Sinne der DSGVO. Selbstverständlich fallen hierunter Name, Anschrift und Geburtsdatum einer Person. Ebenso erfasst sind aber z.B. auch IP-Adressen.
Der Anwendungsbereich der DSGVO wird auch nicht etwa dadurch ausgeschlossen, dass eine Verarbeitung dazu führt, dass die Daten ohne Verknüpfung mit weiteren Informationen (sog. Pseudonymisierung) keinen Rückschluss mehr auf eine bestimmte Person zulassen. Lediglich die vollständige anonymisierte Information fällt nicht unter die DSGVO.

Die Pseudonymisierung von personenbezogenen Daten schließt den Anwendungsbereich der DSGVO nicht aus.

Besondere Kategorien personenbezogener Daten:
An die Verarbeitung besonderer Kategorien personenbezogener Daten stellt die DSGVO besonders strenge Anforderungen. Darunter fallen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen,

religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Ferner genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung all dieser Daten setzt das Vorliegen bestimmter Rechtsgrundlagen voraus.

Gesundheitsdaten:
Dabei handelt es sich um personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleitungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Beispiele: Angaben über den Medikamentenkonsum, Erwerb verschreibungspflichtiger und nichtverschreibungspflichtiger Medikamente (vorausgesetzt, sie werden für den Eigenbedarf erworben).

Verarbeitung:
Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Beispiele: Erhebung, Speicherung, Anpassung, Veränderung, Verwendung, Übermittlung oder auch Löschung von Daten.

Online wie Offline! Hierzu zählt auch die handschriftliche Notiz.

Verantwortlicher:
Verantwortlich für den Datenschutz ist die Stelle, die allein oder gemeinsam mit anderen (z.B. weiterer Gesellschafter im Rahmen einer in der Rechtsform einer OHG geführten Apotheke) über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche ist und bleibt Verantwortlicher auch dann, wenn er einen (internen oder externen) Datenschutzbeauftragten benannt hat. Für Verstöße gegen die DSGVO haftet er im Außenverhältnis in jedem Fall.

Datenschutz ist Chefsache! Die Einhaltung des Datenschutzes obliegt dem Unternehmensinhaber – daran ändert sich auch durch die Einstellung eines Datenschutzbeauftragten nichts.

Verarbeitungsverzeichnis:
Der Zweck des Verarbeitungsverzeichnisses ist der Nachweis der Einhaltung der DSGVO. Zum Inhalt hat es detaillierte Angaben zu einzelnen Datenverarbeitungsvorgängen (z.B. Angaben zum Verantwortlichen, Zweck, Kategorie der betroffenen Daten, Betroffene, Empfänger etc.). Es besteht eine Vorlagepflicht des Verzeichnisses gegenüber den Behörden auf Anfrage. Die Nichtführung eines Verarbeitungsverzeichnisses wird behördlich sanktioniert.

Datenschutzbeauftragter:
Der Datenschutzbeauftragte wird vom Verantwortlichen (Apothekeninhaber) benannt. Er muss über Wissen auf dem Gebiet des Datenschutzrechtes verfügen. Die Funktion des Datenschutzbeauftragten kann nicht vom Inhaber wahrgenommen werden. Er muss im Verhältnis zum Apothekenleiter unabhängig von dessen fachlichen Weisungen im Bereich des Datenschutzes sein. Die Aufgaben des Datenschutzbeauftragten bestehen in der Einhaltung und Überwachung der Datenschutzvorschriften in der Apotheke. Er ist interne wie externe Anlaufstelle und kooperiert mit den Behörden. Bei Nichtbestellung trotz Erforderlichkeit droht ein Bußgeld.

Datenschutzfolgeabschätzung:
Die Datenschutzfolgeabschätzung (DSFA) ist ein Instrument zur Identifizierung riskanter Verarbeitungsvorgänge und der internen Bewertung des Risikos, um die Folgen einer geplanten Verarbeitung für den Schutz der Daten Betroffener abzuschätzen.

Einwilligungserklärung:
Eine Einwilligung ist jede freiwillige, für einen bestimmten Fall/Zweck, in informierter Weise und unmissverständlich abgegebene Willenserklärung oder eine sonstige eindeutige bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung bestimmter personenbezogener Daten einverstanden ist.

Zusammenarbeit mit externen Dienstleistern
Hierunter ist die Zusammenarbeit z.B. mit Rechenzentren, Blisterzentren, Herstellerbetrieben aber auch dem Apothekerverband zu verstehen. Im Grundsatz ist zu beachten, dass die Apotheke stets verantwortlich bleibt. Die unzureichende Auswahl und Kontrolle des Dienstleisters fällt auf den Apothekeninhaber zurück.

5. Was bedeutet Rechenschaftspflicht?

Eine der wichtigsten Neuerungen ist die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) des für die Verarbeitung Verantwortlichen (d.h. des Apothekeninhabers). Nicht die Aufsichtsbehörde muss – wie bisher – einen Verstoß gegen datenschutzrechtliche Bestimmungen belegen, sondern der Verantwortliche hat die Einhaltung sämtlicher datenschutzrechtlicher Vorschriften nachzuweisen. Es findet also eine Beweislastumkehr statt. Daraus folgt, dass die Apotheke das erforderliche Maß an organisatorischen Vorkehrungen und entsprechender Dokumentation durchführen muss, um sich nötigenfalls „frei beweisen“ zu können.

Die Beweislast liegt bei Ihnen!

6. Was ist ein Datenschutzmanagementsystem (DSMS)?

Zentraler Baustein der bereits erwähnten organisatorischen Vorkehrungen und Dokumentation ist das Datenschutz-Management-System (DSMS). Es bezeichnet die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen, mit denen der datenschutzkonforme Umgang mit personenbezogenen Daten im Unternehmen systematisch gesteuert und kontrolliert wird.

Wir empfehlen Ihnen, die Unterstützung Ihres Systemadministrators einzuholen und diesen bei der Erstellung des DSMS mit einzubeziehen.

Diese Dokumente sollten in jedem Fall Bestandteil eines DSMS sein:

- ✓ Dokumentationen zum Datenschutzbeauftragten (Erforderlichkeit, Bestellung, Meldung, Erreichbarkeit)
- ✓ Rechtmäßigkeit der Datenverarbeitung
- ✓ Datenschutzkonforme Auftragsverarbeitungen (Verträge)
- ✓ Vollständiges Verzeichnis der Verarbeitungstätigkeiten
- ✓ Technische und organisatorische Maßnahmen
- ✓ Risikoadäquate Datensicherheit gemäß dem Stand der Technik
- ✓ Ggf. Durchführung von Datenschutzfolgeabschätzungen
- ✓ Löschkonzept
- ✓ Rechte der Betroffenen
- ✓ Meldung von relevanten Datenschutzvorfällen binnen 72 Stunden
- ✓ Schulung von Mitarbeitern

7. Der Datenschutzbeauftragte

7.1 Ist jede Apotheke verpflichtet, einen Datenschutzbeauftragten zu benennen?

Unter welchen Voraussetzungen eine Pflicht zur Benennung (früher: Bestellung) eines Datenschutzbeauftragten besteht, wird in Art. 37 Abs. 1 DSGVO und in § 38 Abs. 1 BDSG-neu geregelt.

Es gibt verschiedene Tatbestände, die jeder für sich die Benennung eines Datenschutzbeauftragten nach sich ziehen. Im Folgenden stellen wir Ihnen daher die aus unserer Sicht für die Apotheke relevantesten Vorschriften vor.

- Sie benötigen einen Datenschutzbeauftragten, wenn Sie in der Regel **mindestens 10 Personen ständig** mit der automatischen Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 S. 1 BDSG-neu). Das entspricht der bisherigen Regelung nach dem BDSG-alt.
- Sollten Sie die 10-Personen-Grenze nicht erreichen, benötigen Sie dennoch einen Datenschutzbeauftragten, wenn die Kerntätigkeit der Apotheke in einer umfangreichen **Verarbeitung besonderer Kategorien von Daten** besteht (Art. 37 Abs. 1 Buchst. c DSGVO).
  Besondere Kategorien von Daten werden in der Apotheke in Form von Gesundheitsdaten verarbeitet. Ungeklärt ist derzeit, ob die Verarbeitung dieser Daten als **Kerntätigkeit** der Apotheke anzusehen ist. Unter „Kerntätigkeit" soll jede Tätigkeit zu fassen sein, die essentiell für die Erreichung der Ziele des Verantwortlichen ist. Die Verarbeitung von Gesundheitsdaten könnte eine Kerntätigkeit der Apotheke neben ihrer Haupttätigkeit sein, der Sicherstellung der Arzneimittelversorgung der Bevölkerung nach § 1 ApoG.

10-Personen-Grenze: Es zählen Köpfe, unabhängig davon, ob es sich um Teilzeit- oder Vollzeitmitarbeiter, Azubis, Praktikanten oder freie Mitarbeiter handelt. Urlaubsaushilfen z.B. sind nicht „ständig" beschäftigt und zählen daher nicht mit. Hauptapotheke und Filialen zählen als ein Unternehmen, d.h. die Kopfzahl wird zusammengezählt.

Die sog. Artikel-29-Datenschutzgruppe sieht beispielsweise die Verarbeitung von Gesundheitsdaten als Kerntätigkeit eines jeden Krankenhauses an. Das legt nahe, auch für die Apotheke von einer entsprechenden „Kerntätigkeit" auszugehen. Auch die Thüringer Landesdatenschutzbehörde hat sich jüngst in diese Richtung geäußert.

Um zur Benennung eines Datenschutzbeauftragten verpflichtet zu sein, muss schließlich von einer **„umfangreichen Verarbeitung"** auszugehen sein. Laut den Erwägungsgründen zur DSGVO soll die Verarbeitung von Patientendaten durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs keine umfangreiche Verarbeitung darstellen. Dies hat jüngst am 26.04.2018 die Konferenz der Datenschutzbehörden des Bundes und der Länder dahingehend bestätigt, dass „in der Regel" nicht von einer umfangreichen Verarbeitung auszugehen sei – dies selbst dann nicht, wenn eine Arztpraxis bzw. eine Apotheke zu mehreren betrieben würde (z.B. in der Rechtsform einer OHG) oder aber mehrere Apotheker in einer Apotheke beschäftigt seien.

Leider sieht der entsprechend Konferenzbeschluss auch umgehend wieder eine Einschränkung vor: Von einer Regelhaftigkeit im dargelegten Sinne könne nicht ausgegangen werden, wenn es sich um eine umfangreiche Verarbeitung in z.B. „großen Praxisgemeinschaften" handele. Damit scheint das Problem der Bestimmung einer „umfangreichen Verarbeitung" lediglich verlagert auf die nicht minder schwierige Festlegung, wann eine „große Praxisgemeinschaft" bzw. Apotheke vorliegt. Was ist z.B. mit Apotheken, die ein oder mehrere Altersheime und/oder Krankenhäuser beliefern? Was mit sehr „großen" Apotheken wie der 24/7-Apotheke im Berliner Hauptbahnhof oder Apotheken, die z.B. eine bundesweite Diabetikerversorgung o.Ä. betreiben. Wichtige Abgrenzungsfragen sind damit nach wie vor ungeklärt. Beispielhaft zeigen sich hier die mit der praktischen Umsetzung der DSGVO verbundenen gravierenden (Auslegungs-)Schwierigkeiten.

Bei der sogenannten Artikel-29-Datenschutzgruppe handelt es sich um ein unabhängiges Beratungsgremium auf EU-Ebene.

Erwägungsgründe werden einem Rechtsakt wie der DSGVO vorangestellt. Sie dienen der Erläuterung der maßgeblichen Überlegungen, die zu dessen Erlass geführt haben. Sie haben keine unmittelbare rechtliche Wirkung, werden jedoch für die Auslegung des Rechtsaktes herangezogen und sind insoweit relevant.

Den Beschluss der Konferenz der Datenschutzbehörden des Bundes und der Länder vom 26.04.2018 finden Sie auf der Internetseite im Mitgliederbereich unter *Recht > Datenschutz*.

- Unabhängig von der Frage der Kerntätigkeit müssen Sie einen Datenschutzbeauftragten benennen, wenn eine **Datenschutzfolgeabschätzung** (DSFA) in Ihrem Betrieb durchzuführen ist (§ 38 Abs. 1 Satz 2 BDSG-neu). Das ist dann der Fall, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen (d.h. Privatpersonen, keine Unternehmen) zur Folge hat. Bei der Einschätzung, ob ein solches Risiko vorliegt, handelt es sich um eine Einzelfallentscheidung:

  Die Artikel-29-Datenschutzgruppe hat mit dem Ziel der Schaffung einheitlicher Bewertungskriterien und daraus folgend der Möglichkeit zur rechtssicheren Beurteilung durch den für den Datenverarbeitungsvorgang Verantwortlichen Leitlinien entwickelt. Demnach soll eine DSFA immer dann vonnöten sein, wenn eine Verarbeitung ein ähnlich hohes Risiko birgt, wie die in der DSGVO ausdrücklich genannten, risikobehafteten Verarbeitungsvorgänge.

Nach Art. 35 DSGVO kann sich ein (voraussichtlich) hohes Risiko zunächst ganz generell aus der Art, dem Umfang, den Umständen und dem Zweck einer Verarbeitung, insbesondere bei Verwendung neuer Technologien, ergeben. Mit neuen Technologien wird ein hohes Risiko verbunden, wenn sie umfangreiche Verarbeitungsvorgänge ermöglichen, die dazu dienen, große Mengen personenbezogener Daten zu verarbeiten, eine große Zahl von Personen betreffen können und beispielsweise eine besondere Sensibilität aufweisen, so etwa im Fall neuer Sicherheits- und Überwachungstechnik.

Ausdrücklich genannt werden in Art. 35 Abs. 3 DSGVO u.a. die folgenden Fälle:

- **Umfangreiche Verarbeitung besonderer Kategorien von Daten**: Hier ist in erster Linie an die tägliche Verarbeitung von Gesundheitsdaten in der Apotheke zu denken. Als besondere Daten-Kategorie gelten nach Art. 9 DSGVO aber auch biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person. Nutzen Sie etwa Fingerprints zur Freischaltung des PC oder bestimmter Software so kann dies, erst recht in Kombination mit weiteren Technologien wie z.B. einer Gesichts- oder Iris-Erkennung, eine DSFA erfordern.

  Im Übrigen gelten die obigen Ausführungen zur schwierigen Konkretisierung des Merkmals „umfangreiche Verarbeitung“ im Rahmen des § 37 Abs. 1 Buchst. c DSGVO entsprechend.

- **Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**: Gemeint ist hier insbesondere der Einsatz optoelektronischer Überwachungstechnik. Tatbestandlich erfasst wird dabei nicht nur der öffentliche Raum, sondern auch das Privatgelände, soweit es der Öffentlichkeit zugänglich gemacht wird. Betreiben Sie also eine Videoüberwachung, dann ist nach der DSGVO hiermit ein hohes Risiko verbunden, sodass der Verarbeitungsvorgang die Durchführung einer DSFA erforderlich macht.

Der Einsatz einer Videoüberwachung macht die Durchführung einer DSFA erforderlich.

Auf dem Regelungsinhalt von Art. 35 DSGVO basierend, sehen die Leitlinien der Artikel-29-Datenschutzgruppe neun Kriterien vor, die bei der Beurteilung der Risikogeneigtheit eines Verarbeitungsvorganges grundsätzlich heranzuziehen sind. Sind zwei Kriterien erfüllt, soll der für die Datenverarbeitung Verantwortliche in der Regel eine DSFA durchführen. Zu den Kriterien zählen u.a. die Verarbeitung besonderer Kategorien von Daten wie z.B. Gesundheitsdaten oder biometrische Daten (s.o.) und die Verarbeitung von Daten zu schutzbedürftigen Betroffenen (z.B. Geschäftsunfähige und beschränkt Geschäftsfähige, Arbeitnehmer, Senioren). Eine Apotheke erfüllt diese zwei Kriterien regelmäßig. Es müsste daher von einem (voraussichtlich) hohen Risiko des Verarbeitungsvorganges und damit einhergehend von dem Erfordernis einer DSFA auszugehen sein. Andererseits – und auch hieran zeigen sich erneut die Schwierigkeiten bei der praktischen Auslegung und Anwendung der DSGVO – führt die Artikel-29-Datenschutzgruppe verschiedene Einzelfallbeispiele an. Danach soll die Verarbeitung personenbezogener Daten von Patienten durch ei-

nen Arzt oder einen sonstigen Angehörigen eines Gesundheitsberufs nicht per se zur Notwendigkeit einer DSFA führen. Dies mag vor dem Hintergrund zu verstehen sein, dass die Erwägungsgründe zur DSGVO die Durchführung einer DSFA für Heilberufler nur dann zu verlangen scheint, wenn diese personenbezogene Daten „umfangreich" im Sinne von Art. 37 Abs. 1 Buchst. C DSGVO verarbeiten.

ACHTUNG: Die DSGVO sieht zudem eine Ermächtigung zugunsten der Datenschutzbehörden vor, durch Negativ- und Positivlisten klarzustellen, welche konkreten Verarbeitungsvorgänge keine bzw. eine DSFA erforderlich machen. Solche Listen sind von der LDI NRW für den 25.05.2018 angekündigt. Wir werden die Veröffentlichungen dieser Listen für Sie im Blick behalten und Sie bei relevanten Präzisierungen und/oder Änderungen entsprechend informieren.

Die Datenschutzbehörde kann über Positiv- und Negativlisten die näheren Voraussetzungen für die Pflicht zur Durchführung einer DSFA klarstellen.

Zusammenfassend ist festzustellen, dass Sie in jedem Fall bei Überschreitung der 10-Personen-Grenze einen DSB benennen müssen. Unter dieser Grenze spricht u.E. einiges dafür, dass nicht selten von einer Benennungs-Pflicht auszugehen sein dürfte. Jedoch ist eine abschließende Beurteilung, wann eine „umfangreichen Verarbeitung" und/oder aber ein „voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen" tatbestandlich vorliegt bzw. ausgeschlossen werden kann, derzeit noch nicht möglich. Die weitere Entwicklung bleibt also zunächst abzuwarten.

EMPFEHLUNG:

Angesichts der bestehenden Unsicherheiten kann derzeit nur empfohlen werden, unabhängig von der Mitarbeiterzahl einen Datenschutzbeauftragten für die Apotheke zu benennen. Nur auf diese Weise sind Sie „auf der sicheren Seite" (Vorsichtigkeitsprinzip). Letztlich kennen Sie als Inhaber die Situation in Ihrer Apotheke am besten und müssen als Verantwortlicher unter Abwägung aller Umstände – hierzu haben wir versucht, Ihnen die wesentlichen rechtlichen Gesichtspunkte aufzuzeigen – die Entscheidung treffen.

7.2 Ernennung, Funktionen und Pflichten des Datenschutzbeauftragten

- Der Datenschutzbeauftragte (DSB) muss über **Fachwissen** auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie über Kenntnisse im IT-Bereich verfügen (z.B. durch Schulungen, Seminare, Weiterbildungen).
- Er übernimmt die **Unterrichtung und Beratung** des Verantwortlichen und der Beschäftigten zu ihren datenschutzrechtlichen Pflichten, überwacht die Einhaltung des Datenschutzrechts und ist Ansprechpartner für die Beschäftigten. Er kontrolliert und berät zum Thema Mitarbeiterschulung (verantwortlich für die Durchführung bleibt aber der Apothekeninhaber); obwohl nicht gesetzlich dazu verpflichtet, kann auch der DSB die Mitarbeiterschulungen selber durchführen.
- Er wirkt bei der **Datenschutzfolgeabschätzung** vor risikoreichen

Datenverarbeitungen mit (Art. 35 Abs. 2 DSGVO).

- Er ist berechtigt, gegebenenfalls von sich aus die **Aufsichtsbehörde** zu konsultieren.
- Er ist **Anlaufstelle** für die betroffenen Personen, die sich in allen Fragen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte an ihn wenden können. Dies gilt auch für die übrigen Mitarbeiter in der Apotheke.
- Er nimmt seine Funktionen und Pflichten für **sämtliche Apotheken** eines Filialverbundes wahr.
- Art. 38 Abs. 3 Satz 1 DSGVO regelt die **Weisungsfreiheit** des betrieblichen Datenschutzbeauftragten bezogen auf den Bereich der Wahrnehmung seiner datenschutzrechtlichen Aufgaben. Insoweit tritt auch die nach § 7 ApoG geforderte eigenverantwortliche Leitungsfunktion des Apothekeninhabers zurück.
- Es besteht ferner ein ausdrückliches **Benachteiligungsverbot** gem. Art. 38 Abs. 3 Satz 2 DSGVO. Nach § 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG-neu genießt der interne Datenschutzbeauftragte wie nach dem BDSG-alt Kündigungsschutz. Rechtmäßigkeit und Reichweite dieser Regelung werden jedoch teilweise in Frage gestellt.
- Die **Kontaktdaten** des DSB sind nunmehr auf der Internetseite an leicht auffindbarer Stelle (z.B. Impressum) auszuweisen. Es empfiehlt sich die Einrichtung einer Funktions-E-Mail-Adresse (z.B. datenschutzbeauftragter@musterapotheke.de). Auf jeden Fall muss sichergestellt werden, dass diese E-Mails nur vom DSB oder seinem Vertreter gelesen werden können.
- **Die Kontaktdaten sind der Landesdatenschutzbeauftragten mittels eines Online-Formulars auf der Internetseite des LDI NRW zu melden.** Derzeit ist das entsprechende Tool noch nicht fertiggestellt. Bitte kontrollieren Sie daher regelmäßig die Internetseite des LDI NRW. Sobald das Tool funktioniert, sollten Sie Ihren DSB unverzüglich benennen.
- Die **persönliche Haftung** des Datenschutzbeauftragten für Nichtbeachtung der oder Verstöße gegen die DSGVO ist strittig.
- Es kann ein **interner oder ein externer** Datenschutzbeauftragter (Näheres dazu s. unsere Empfehlung) benannt werden, Art. 37 Abs. 6 DSGVO.

Es ist nur ein Datenschutzbeauftragter im gesamten Filialverbund erforderlich.

Die Ausweisung der Kontaktdaten des DSB umfasst nicht zwingend auch dessen Namen.

Die Haftung des verantwortlichen Inhabers hingegen ist stets gegeben.

ACHTUNG: Die fehlende, nicht rechtzeitige oder in vorgeschriebener Weise vorgenommene Benennung eines Datenschutzbeauftragten ist – wie bisher – bußgeldbewehrt; unter der DSGVO kann hierfür jetzt ein Bußgeld von bis zu 10 Mio. € oder 2% des weltweiten Jahresumsatzes verhängt werden, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 4 Buchst. a DSGVO). Allerdings wendet sich der Bußgeldrahmen in seiner Spitze an große Unternehmen. Zudem hängt die im Einzelfall zu verhängende Geldbuße von den konkreten Umständen eines Verstoßes ab. So finden u.a. Art, Schwere und Dauer eines Verstoßes bei der Bemessung des Bußgeldes ebenso Berücksichtigung wie die Verschuldensform (Vorsatz, Fahrlässigkeit). Zu den Einzelheiten vgl. Art. 83 Abs. 2 DSGV.

EMPFEHLUNG:

Wichtig ist, dass Sie sich rechtzeitig darüber Gedanken machen, wer als Datenschutzbeauftragter für Sie in Frage kommt. Sie können weder sich selbst noch einen Filialleiter zum DSB bestellen, da dann Interessenkonflikte bestünden. Die Benennung eines Mitarbeiters ist hingegen möglich. Im Fall Ihres Ehepartners ist wiederum zu befürchten, dass dieser nicht die erforderliche Unabhängigkeit besitzt, sprich ein Interessenkonflikt unterstellt werden könnte. Die Benennung eines anderen Apothekeninhabers – ggf. sogar auf Gegenseitigkeit – dürfte zwar grundsätzlich möglich sein, aber bitte bedenken Sie, dass diesem dann auch Einblick in nahezu alle Betriebsabläufe zu gewähren ist.

Der Zeitaufwand ist nicht unerheblich. Ein Mitarbeiter braucht ein angemessenes Zeitkontingent und Sie müssen sich überlegen, wie Sie ihn schulen wollen. Soll die Aufgabe ein externer DSB übernehmen, so muss dieser zunächst einmal die Abläufe, insbesondere die einzelnen Datenverarbeitungsvorgänge, in Ihrem Betrieb kennenlernen. Diese hat er dann regelmäßig zu überprüfen, wofür er einen Ansprechpartner in der Apotheke benötigt. Ferner hat er in angemessenem Umfang erreichbar zu sein. In keinem Fall reicht es, „irgendjemanden“ zu benennen. Vielmehr schulden Sie als Verantwortlicher auch eine ordnungsgemäße Auswahl. Der externe DSB muss seine Aufgaben wahrnehmen, was von Ihnen zu kontrollieren ist. Vor unseriösen und allzu „günstigen“ Anbietern kann nur gewarnt werden.
Bestellen Sie einen Ihrer Mitarbeiter, dann wissen Sie in aller Regel, wen Sie bekommen und wie dessen Arbeitshaltung ist. Zudem kennt er den Betrieb, die Kollegen, die Arbeitsabläufe und auch seine Erreichbarkeit ist gewährleistet. In kritischen Fällen mag zudem eine Abstimmung mit einem internen DSB leichter fallen als mit einem externen.

Ganz gleich, wen Sie benennen und wie viel dieser ggf. auch kostet, Verantwortlicher für alle Verstöße gegen die DSGVO bleiben Sie auch nach der Benennung des DSB: Datenschutz ist und bleibt Chefsache! Eine andere Frage ist, ob Sie den DSB wegen eines Ihre Haftung begründenden Verstoßes in Regress nehmen können. Im Fall eines externen DSB ist dies denkbar, denn er haftet Ihnen auf dem seiner Bestellung zugrundeliegenden Vertrag auf Schadensersatz. Bei einem internen DSB kann allenfalls nach den Grundsätzen der Arbeitnehmerhaftung und insoweit abhängig vom Verschuldensgrad und in der Höhe begrenzt regressiert werden.

Haben Sie sich entschieden, so sollten Sie die Kontaktdaten auf der Internetseite Ihrer Apotheke angeben und die Meldung an die Aufsichtsbehörde vorrangig erledigen. Das Gesetz schreibt in diesem Fall keine namentliche Benennung vor. Dennoch empfiehlt es sich, als vertrauensbildende Maßnahme auch den Namen des DSB (soweit dieser einverstanden ist) anzugeben. Jeder erkennt so, dass sich nicht der Apothekeninhaber selbst zum DSB ernannt hat, sondern dass ein Ansprechpartner existiert, an den man sich wenden kann, ohne gleich die Aufsichtsbehörde einzuschalten.

Musterschreiben für die Benennung eines internen Datenschutzbeauftragten und die Verpflichtung der Mitarbeiter auf den Datenschutz finden Sie im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz.*
Außerdem haben wir Ihnen eine Liste von externen Datenschützern erstellt, die Sie ebenfalls im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz* finden. Dabei haben wir versucht, Ihnen möglichst flächendeckend Anbieter zu nennen. Für weitere Informationen sehen Sie bitte die Liste nebst Einleitung ein.

Datenschutz ist und bleibt immer Chefsache!

8. Wann ist eine Datenverarbeitung zulässig?

8.1 „Verbot mit Erlaubnisvorbehalt“

8.1.1 Verarbeitung personenbezogener Daten (Art. 6 DSGVO)

Wie bisher gilt das sogenannte **„Verbot mit Erlaubnisvorbehalt“.** D.h. eine Verarbeitung personenbezogener Daten (z.B. Name, Anschrift, Geburtsdatum) ist nur dann zulässig, wenn mindestens eine der in Art. 6 DSGVO genannten Voraussetzungen erfüllt ist:

Alles, was nicht erlaubt ist, ist verboten. Die erste Frage, die man sich somit stellt: Ist die Datenverarbeitung erlaubt?

- **Einwilligung** der betroffenen Person zur Datenverarbeitung
- **Vertrag oder vorvertragliche Maßnahme**
  Die Verarbeitung ist rechtmäßig, wenn sie zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist (z.B. Datenerhebung bei EC-Cash) oder zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der Person (z.B. Vorbestellung von Medikamenten, Beratung zur notwendigen Inkontinenzversorgung) erforderlich ist.
- **Rechtliche Verpflichtung**
  Die Verarbeitung ist rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt
- **Schutz lebenswichtiger Interessen**
  Diese Rechtsgrundlage dürfte für Sie im Apothekenalltag kaum Relevanz haben. Beispiele für diesen Anwendungsfall sind Epidemien und Naturkatastrophen.
- **Öffentliches Interesse oder hoheitliche Gewalt**
- **Wahrung berechtigter Interessen**
  Die Verarbeitung ist rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Rechte und Interessen der betroffenen Person nicht überwiegen (z.B. Videoüberwachung in der Apotheke, soweit die Rechte und Interessen der betroffenen Personen nicht überwiegen – bitte prüfen Sie dies im Einzelfall!).

8.1.2 Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)

Betrifft die Verarbeitung sogar eine besondere Kategorie personenbezogener Daten wie z.B. Gesundheitsdaten, dann sind die Voraussetzungen für eine rechtmäßige Verarbeitung nochmal strenger. Ähnlich der bisherigen Regelung im BDSG sieht Art. 9 DSGVO besondere Daten-Kategorien vor, die grundsätzlich nicht verarbeitet werden dürfen. Neben den Gesundheitsdaten gehören dazu Daten zur religiösen und weltanschaulichen Überzeugung, Daten zum Sexualleben, der sexuellen Orientierung und biometrische Daten (z.B. Fingerprint, Gesichtserkennung, Stimmerkennung).

ACHTUNG: Die Einwilligung durch schlüssiges Handeln ist bei der Einwilligung in die Verarbeitung besonderer Kategorien von Daten grundsätzlich nicht möglich. Erforderlich ist eine ausdrückliche, aktive Zustimmung.

Die Verarbeitung ist nur unter folgenden Voraussetzungen erlaubt:

- **ausdrückliche Einwilligung** der betroffenen Person zur Verarbeitung von Daten besonderer Kategorien

- **Arbeitsrecht, soziale Sicherheit und Sozialschutz**
  Die Verarbeitung ist im Arbeitsrecht und aus Gründen der sozialen Sicherheit und dem Sozialschutz unter den in Art. 9 Abs. 2 Buchst. b DSGVO genannten Voraussetzungen – insbesondere der Erforderlichkeit der Verarbeitung – zulässig (z.B. Verarbeitung von Angaben zur Religionszugehörigkeit zwecks Abführung von Kirchensteuer; Verarbeitung von Gesundheitsdaten, soweit dies zur Erbringung von Sozialleistungen erforderlich ist).
- **Geltendmachung und Abwehr von Rechten oder Ansprüchen**, soweit die Verarbeitung hierfür erforderlich ist
- **Versorgung im Gesundheitsbereich**
  Dieser Erlaubnisgrund erfasst die Verarbeitung von u.a. Gesundheitsdaten im Bereich der medizinischen Versorgung. Erlaubt ist die Verarbeitung in der Apotheke. Sie muss sich auf die Versorgung mit Medikamenten und medizinischen Hilfsmitteln beziehen. Umfasst ist davon auch die Verarbeitung von Daten, die Apotheken gem. §§ 294 ff SGB V den Krankenkassen mitteilen (Abrechnung). Ebenfalls umfasst sein dürften die vertraglich mit den Krankenkassen vereinbarten Verfahren zur Kostenübernahme (Kostenvoranschlag, Genehmigung). Neben den datenschutzrechtlichen Bestimmungen ist das Berufsgeheimnis zu wahren. Wäre etwa eine Datenübermittlung oder -nutzung datenschutzrechtlich zulässig, verstieße aber gegen ein Berufsgeheimnis, so wäre sie insgesamt unzulässig. Neben der Regelung in Art. 9 DSGVO ist es dem nationalen Gesetzgeber erlaubt, im Bereich der Gesundheitsversorgung zusätzliche Verarbeitungsvoraussetzungen zu schaffen. Solche sind beispielsweise für die Abrechnung mit den Krankenkassen in den §§ 300 und 302 SGB V geregelt.
  Die Verarbeitung ist auch durch Fachpersonal zulässig, soweit dieses ebenso dem Berufsgeheimnis unterliegt. Zudem ist eine Verarbeitung durch „eine andere Person“ zulässig, wenn diese ebenfalls einer Geheimhaltungspflicht unterliegt. Einer Geheimhaltung nach § 203 StGB unterliegen beispielsweise berufsmäßig tätige Gehilfen (z.B. die PTA), ein (externer) Datenschutzbeauftragter oder an der Berufsausübung mitwirkende Personen. Der AVWL wird u.E. im Bereich der Clearing- und Retaxstelle aufgrund der Auftragsverarbeitung (s. dazu Punkt 8.3) zu einer solchen, an der Berufsausübung mitwirkenden Person. Zur Bestätigung dieser Auffassung haben wir eine Anfrage an den LDI NRW gestellt; die Antwort steht noch aus.

8.2 Voraussetzungen der Einwilligung

Die Einwilligung ist Ausdruck des Rechts auf informationelle Selbstbestimmung. Jede Person soll grundsätzlich selbst über das „Ob“ und „Wie“ der Verarbeitung ihrer Daten entscheiden.

Unter Einwilligung versteht man jede

- freiwillige,
- für einen bestimmten Fall (Zweckbindung),
- in informierter Weise und
- unmissverständlich

abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der personenbezogenen Daten einverstanden ist (Art. 4 Nr. 11 DSGVO). Die Einwilligung kann vom Betroffenen grundsätzlich widerrufen werden.

ACHTUNG: Sie müssen die Einwilligung stets nachweisen können (Rechenschaftspflicht)! Eine mündliche Einwilligung ist schwer bis gar nicht nachweisbar! Wir empfehlen daher, immer eine schriftliche oder anders nachweisbare Einwilligung einzuholen.

Folgende Punkte sind bei der Einholung einer Einwilligung zu beachten:

- Eine Einwilligung ist künftig statt in schriftlicher auch in elektronischer oder mündlicher Form zulässig.
- Erforderlich ist eine eindeutige bestätigende Handlung. Bloße Untätigkeit, z.B. ein bereits durch die Apotheke angekreuztes Kästchen (Opt-out-Lösungen), reicht nicht aus. **ACHTUNG**: Bei Gesundheitsdaten ist eine aktive, ausdrückliche Einwilligung erforderlich. Schlüssiges Verhalten genügt nicht.
- Die Einwilligung muss in leicht zugänglicher Form und in einfacher und klarer Sprache verfasst sein.
- Sie darf grundsätzlich nicht mit sachfremden Erwägungen gekoppelt werden, so z.B. bei Einkaufsvorteilen oder reduzierten Seminargebühren, die nur im Fall der Einwilligung gewährt werden. Maßgeblich für die Zulässigkeit einer solchen Kopplung ist die Bewertung der konkreten Umstände des Einzelfalls. Die Einwilligung muss für jeden Verarbeitungsvorgang/Zweck erteilt werden (z.B. die Datennutzung zwecks Versendung von Glückwunsch- oder Weihnachtskarten, die Datenweitergabe an Filialapotheken im Rahmen von Bonusprogrammen)
- Alte Einwilligungen behalten nur dann ihre Gültigkeit, wenn sie den neuen Anforderungen entsprechen. Die bisher von uns zur Verfügung gestellten Muster entsprechen lediglich dem alten Recht.

Überprüfen Sie Ihr bisheriges Einwilligungsmuster am Maßstab der DSGVO.

Die Einwilligung ist nicht nur für die Verarbeitung von Kundendaten erforderlich. Sie benötigen auch eine Einwilligung Ihrer Mitarbeiter, wenn Sie z.B. deren biometrische Daten verarbeiten, also beispielsweise ein Fingerprint-System einsetzen oder aber deren Fotos oder Teamfotos auf der Internetseite der Apotheke veröffentlichen wollen.

Muster für eine Einwilligung in die Datenspeicherung (Kundenkarte) sowie eine Formulierungshilfe für einen Vertrag über die Auftragsverarbeitung finden Sie im Mitgliederbereich unserer Internetseite unter *Recht* > *Datenschutz*. Ein Muster für den Sonderfall „Einwilligung - Heimbewohner“ ist in Vorbereitung.

ACHTUNG beim Apothekenverkauf: Der Kundenstamm ist ein für den Wert einer Apotheke wesentlicher Faktor. Auch wenn dies für den Nachfolger von besonderem Interesse ist: Beachten Sie, dass Sie beim Verkauf auf keinen Fall die Kundendatei ohne die ausdrückliche Einwilligung der Kunden übertragen dürfen. Wenn die Ihnen vorliegenden Einwilligungserklärungen den Fall einer Veräußerung nicht umfassen, müssen Sie die Kunden vor der Apothekenübergabe anschreiben oder bei deren Besuch ansprechen und die Einwilligungserklärung nachholen. Ohne diese Einwilligung dürfen Sie die Daten nicht an den Nachfolger übergeben.

Zu den spezifischen datenschutzrechtlichen Voraussetzungen bezogen auf Ihre Mitarbeiter haben wir Ihnen am Ende dieser Abhandlung verschiedene Fachartikel aufgelistet (s. Punkt 15).

8.3 Auftragsverarbeitung

Die Auftragsverarbeitung (früher: Auftragsdatenverarbeitung) betrifft die Fälle, in denen an einen Auftragnehmer (Auftragsverarbeiter) Daten übermittelt werden, der dann im Pflichtenkreis und auf Weisung des Auftraggebers tätig wird. Beispiele: Rechenzentren, AVWL im Rahmen der Tätigkeit der Clearing- und Retaxstelle, Zusammenarbeit mit Blisterzentren oder anderen Lohnherstellern etwa im onkologischen Bereich. Über die Auftragsverarbeitung hinaus bedarf es wohl keiner weiteren, die Übermittlung rechtfertigenden Rechtsgrundlage, insbesondere keiner (zusätzlichen) Einwilligung. Dies gilt selbst dann, wenn es sich um Gesundheitsdaten handelt.

ACHTUNG: Nicht jede Verarbeitung von personenbezogenen Daten durch einen Dienstleister im Interesse des Apothekers führt zu einer Auftragsverarbeitung. Trägt der Dienstleister tatsächlich selbst die Verantwortung für die Datenverarbeitung, liegt keine Auftragsverarbeitung vor. Für die Übermittlung der Daten an den Dienstleister bedarf es dann einer Rechtsgrundlage (s. Punkt 8.1). Denn die – vermeintliche – Auftragsverarbeitung deckt diese Verarbeitung ja gerade nicht.

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt gemäß Art. 28 Abs. 3 DSGVO in der Regel auf der Grundlage eines Vertrags, in dem unter anderem festzulegen sind:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- die Art der personenbezogenen Daten
- die Kategorien betroffener Personen
- die Pflichten und Rechte des Verantwortlichen.

Muster für einen Vertrag über die Auftragsverarbeitung finden Sie im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz.*

Beachten Sie bitte, dass Sie die Muster stets an die individuellen Gegebenheiten Ihrer Apotheke anpassen müssen.

Der Vertrag muss ferner vorsehen, dass der Auftragsverarbeiter

- gewährleistet, dass sich die zur Datenverarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen (Art. 28 Abs. 3 Buchst. b),
- alle gemäß Art. 32 DSGVO erforderlichen Sicherheits-Maßnahmen ergreift (Art. 28 Abs. 3 Buchst. c) und
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellt; ferner Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht oder dazu beiträgt (Art. 28 Abs. 3 Buchst. h).

Aktualisieren Sie bestehende Verträge zur Auftragsverarbeitung!

Durch die DSGVO neu hinzugekommen sind folgende Aspekte:

- Verstößt der Auftragsverarbeiter gegen Pflichten, so ist er selbst neben dem Auftraggeber Verantwortlicher
- Spezielle Haftungsregelungen

- Der Auftragsverarbeiter hat zusätzlich zum Verantwortlichen ein eigenes Verzeichnis der Verarbeitungstätigkeiten zu führen
- Der Vertrag über die Auftragsverarbeitung kann nun auch in elektronischer Form geschlossen werden

In eigener Sache: Bislang ist der AVWL im Rahmen eines Auftragsdatenverarbeitungsverhältnisses als „verlängerter Arm" der Apotheke tätig. Eine Einwilligung der Apothekenkunden in die Datenweitergabe war nicht erforderlich, denn aufgrund des Auftragsdatenverarbeitungsverhältnisses werden die Daten nicht an einen „Dritten" im Rechtssinne weitergegeben.
Sollte stattdessen unter Geltung der DSGVO künftig stets eine Einwilligung einzuholen sein, dann lässt sich dies weder praktisch noch rechtssicher umsetzen. Eine Apotheke wird ihren Kunden einen solchen Vorgang im Rahmen einer Rezepteinreichung kaum vermitteln können. Eine alternative (oder gar kumulative) Schwärzung des Rezeptes ist indes ebenfalls problematisch, denn die Krankenkasse benötigt eine Verordnung, die sie ihrem Versicherten zuordnen kann. Das ginge zwar über die Versichertennummer, diese ist aber möglicherweise personenbezogen bzw. nicht ausreichend anonymisiert.
Wir gehen auch weiterhin davon aus, dass die durch die Apotheke auf der Grundlage einer Auftragsverarbeitung in Anspruch genommene Clearing- und Retax-Dienstleistung nach Art. 9 Abs. 2 Buchst. h DSGVO zulässig ist. Demnach ist die „Verarbeitung für Zwecke der Gesundheitsvorsorge" erlaubt (s.o.). Zu diesem zentralen Problem haben wir eine Anfrage an die Landesdatenschutzbeauftragte gestellt. Wir werden Sie über das Ergebnis unverzüglich informieren.

9. Die Verarbeitungstätigkeiten

9.1 Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten für die Apotheke

Art. 30 DSGVO fordert, dass der Verantwortliche ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen hat, die in seinem Unternehmen stattfinden. Nach dem Wortlaut der Vorschrift sind Unternehmen mit weniger als 250 Mitarbeitern von dieser Pflicht freigestellt, wenn die Datenverarbeitung „nur gelegentlich" erfolgt und kein Risiko für das Freiheits- und Betroffenenrecht besteht bzw. keine besonderen Datenkategorien wie z. B. Gesundheitsdaten verarbeitet werden. Für die Apotheken gilt die Ausnahme folglich nicht, sodass die Erstellung eines Verzeichnisses verpflichtend ist.
Das Verzeichnis soll jedem verantwortlichen Apothekeninhaber einen Überblick geben, was im eigenen Unternehmen geschieht, ob es so geschehen darf und welche Sicherungsmaßnahmen zum Schutz personenbezogener Daten bestehen. Insoweit ist das Verzeichnis der Verarbeitungstätigkeiten als Einstieg in die Materie des Datenschutzes sehr wichtig. Das Verzeichnis ist schriftlich zu führen, es kann allerdings auch ein elektronisches Format benutzt werden. Die Erstellung des Verzeichnisses ist grundsätzlich Aufgabe des Apothekeninhabers. Er kann dies allerdings

Das Verzeichnis von Verarbeitungstätigkeiten nach der DSGVO entspricht inhaltlich weitestgehend dem „alten" Verfahrensverzeichnis auf Grundlage des bisherigen Rechts. Insoweit dürfte der Umstellungsaufwand für Sie in diesem Fall gering sein. Als QMS-zertifizierte Apotheke können Sie gegebenenfalls auf bereits bestehende Verfahrensdokumentationen zurückgreifen und diese anpassen.

an Mitarbeiter delegieren und sich der Hilfe des Datenschutzbeauftragten bedienen. Das Verfahrensverzeichnis ist immer aktuell zu halten. Eine neue Software oder ein neuer Verarbeitungsvorgang muss in das Verfahrensverzeichnis aufgenommen werden.

ACHTUNG: Das Verfahrensverzeichnis war schon bislang in jeder Apotheke zu führen, unabhängig davon, ob ein DSB zu bestellen war oder nicht (sog. „Jedermann-Verzeichnis", weil es von „jedermann" eingesehen werden konnte). Die DSGVO enthält – insoweit vereinfachend gegenüber der bisherigen Rechtslage – weder die Möglichkeit zur Einsichtnahme für jedermann noch eine Meldepflicht der Verfahren gegenüber der Datenschutzbehörde. Das Verzeichnis kann allerdings durch die zuständige datenschutzrechtliche Aufsichtsbehörde jederzeit angefordert werden und es drohen Bußgelder, falls das Verzeichnis von Verarbeitungstätigkeiten nicht oder nur unvollständig vorliegt. Auch der Amtsapotheker mag sich im Rahmen z.B. einer Revision für das Verzeichnis interessieren. Insgesamt steht es im primären Interesse der Behörden und sollte daher stets aktuell und vollständig sein.

Das Verzeichnis aller Verarbeitungstätigkeiten muss folgende Angaben enthalten:

- ✓ Name und Kontaktdaten des Verantwortlichen
- ✓ Name und Kontaktdaten des DSB (soweit ein solcher benannt ist)
- ✓ Zwecke der Verarbeitung (z.B. Rezeptabrechnung, Kundendatei, Bonussystem, Geburtstagsglückwünsche)
- ✓ Beschreibung der Kategorien betroffener Personen (z.B. Kunden, Mitarbeiter, Ärzte)
- ✓ Beschreibung der Kategorien personenbezogener Daten (z.B. Kontaktdaten, Gesundheitsdaten)
- ✓ Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt worden sind oder noch offengelegt werden (z.B. Rechenzentren, Verbände, Krankenkassen)
- ✓ ggf. Übermittlungen von personenbezogenen Daten an ein Drittland mit zusätzlichen Angaben zur Datenübermittlung
- ✓ vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Beachtung von Fristen z.B. nach Arzneimittelgesetz, ApBetrO, nach Handels- und/oder Steuerrecht)
- ✓ eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (s. Punkt 9.2)

Muster für ein Verarbeitungsverzeichnis finden Sie im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz*. Das Verarbeitungsverzeichnis ist für jeden Verarbeitungsvorgang in der Apotheke getrennt auszufüllen. Die typischen Verarbeitungsvorgänge haben wir beispielhaft für Sie abgebildet. Sie müssen diese ggf. ergänzen.

9.2 Welche technisch-organisatorischen Maßnahmen (TOM) sind erforderlich?

Verantwortliche und Auftragsverarbeiter haben nach Art. 32 DSGVO unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der be-

troffenen Personen die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Besondere Schutzwürdigkeit kommt dabei wieder den Gesundheitsdaten zu.

Bitte bedenken Sie, dass es auch hier nicht etwa nur um digitale Verarbeitungsprozesse geht, sondern ebenso der räumlich-organisatorische Bereich Ihrer Apotheke betroffen ist. So muss z.B. das Beratungsgespräch unter Wahrung der Vertraulichkeit möglich sein, d.h. es sind Diskretionsabstände einzurichten, Schall- und Blickschutzmaßnahmen zu ergreifen. Ebenso wenig darf die telefonische Klärung zu einem Rezept in Hörweite zu anderen Patienten geführt werden. Passanten darf kein Blick durch die Schaufensterscheibe auf einen HV-Tisch möglich sein. Und auch dem liefernden Großhändler darf ein solcher nicht gewährt werden. Ziel technisch-organisatorischer Maßnahmen ist die Risikovermeidung. Eine Maßnahme ist dann geeignet, wenn sie das Ziel der Risikovermeidung zumindest fördert.

Von Ihnen wird erwartet, dass Sie sämtliche Verarbeitungsprozesse in Ihrer Apotheke durch die „Datenschutz-Brille“ analysieren und hinsichtlich des jeweiligen Risikos bewerten.

Bei der Bestimmung geeigneter TOMs zu berücksichtigen sind die im Gesetzeswortlaut genannten Kriterien:

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zweck der Datenverarbeitung
- Eintrittswahrscheinlichkeit und Schwere des Risikos

Ferner hat eine Risikobewertung zu erfolgen. Die DSGVO sieht sodann folgende mögliche Maßnahmen zur Risikominimierung vor:

Pseudonymisierung und Verschlüsselung

- Bei der **Pseudonymisierung** werden Daten in einer Weise verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Sie dient der **Datenminimierung**.
- Eine **Verschlüsselung** ist ein Vorgang, bei dem klar lesbare Informationen mit Hilfe eines Verschlüsselungsverfahrens in eine nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt werden. Sie dient der Zweckbindung, der Vertraulichkeit und der Integrität der Daten.

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

- Die **Vertraulichkeit** der Systeme und Dienste kann z.B. durch Zutritts- und Zugangskontrollen gewährleistet werden. Wenn auf die Systeme und Dienste bereits keine unberechtigten Personen zugreifen können, verringert sich natürlich das Risiko, dass in diesem System gespeicherte Daten von einem Nichtberechtigten zur Kenntnis genommen werden.

- Die **Integrität** der Systeme und Dienste ist gewährleistet, wenn sie gegen (unerkannte) Manipulationen geschützt sind (z.B. durch Firewalls, Antivirensoftware, Software-Updates, E-Mail-Filter etc.).
- Die **Verfügbarkeit** ist gewährleistet, wenn die Daten über das System/den Dienst jederzeit genutzt/abgerufen werden können (z.B. durch einen Funktionstest, Notstromversorgung und Backup-Systeme).
- Systeme und Dienste sind **belastbar**, wenn sie die Fähigkeit besitzen, mit Veränderungen umzugehen. Das System/der Dienst ist dann in der Lage, Störungen auszugleichen.

Verfügbarkeit der und Zugang zu den Daten
Durch diese Maßnahme sollen die Verfügbarkeit und der Zugang zu den Daten bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen sein. Dies betrifft weniger die alltäglichen Sicherheitsrisiken und Nutzungsbeeinträchtigungen als Sondersituationen wie einen gezielten Angriff auf das System oder einen Brand.

Kontrollverfahren
Mit dem Kontrollverfahren wird die Datensicherheit mittelbar hergestellt, die unmittelbar wirkenden Maßnahmen werden einer regelmäßigen internen Kontrolle unterzogen. Die Kontrolle kann durch Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen erfolgen.

Anweisung durch den Verantwortlichen
Hierbei handelt es sich nicht um eine technische, sondern um eine personelle Maßnahme. Datenverarbeitung darf nur auf Anweisung des Verantwortlichen ausgeführt werden, es sei denn, die Person ist zur Datenverarbeitung rechtlich verpflichtet.

Dieser Maßnahmenkatalog ist weder abschließend, noch müssen immer alle der genannten Maßnahmen ergriffen werden.

Der technische Schutz der von Ihnen verarbeiteten personenbezogenen Daten bedarf eines Sicherheitskonzeptes, das Sie mit ihrem Systemadministrator als Fachmann besprechen und von ihm erarbeiten lassen sollten. Dieses fängt an mit den Schlüsseln für die Apotheke, dem Abschließen der Apotheke am Abend, dem verschlusssicheren Serverraum und betrifft auch konkrete Handlungsanweisungen gegenüber den Mitarbeitern im Hinblick auf die E-Mail- und Internetnutzung.
Zum Nachweis der Gewährleistung eines angemessenen Schutzniveaus durch TOMs können genehmigte Verhaltensregeln (Art. 40 DSGVO) oder zertifizierte Verfahren (Art. 42 DSGVO) herangezogen werden. Die genehmigten Verhaltensregeln und Zertifizierungsverfahren sollen insbesondere kleineren und mittleren Unternehmen die Auswahlentscheidung der Maßnahmen erleichtern.

Muster für die technisch-organisatorischen Maßnahmen (TOM) finden Sie im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz.*

Ziehen Sie für die Erstellung der TOMs Ihren Systemadministrator zu Hilfe.

10. Wie wird eine Datenschutzfolgeabschätzung (DSFA) durchgeführt?

Auf die Datenschutzfolgeabschätzung (DSFA) ist bereits im Rahmen der Ausführungen zum Datenschutzbeauftragten eingegangen worden (s. Punkt 7.1).

Die Folgeabschätzung erfolgt in **drei Stufen**:

- Auf der **ersten Stufe** ist zu prüfen, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Das ist regelmäßig der Fall, da Apotheken täglich Gesundheitsdaten und Daten von Geschäftsunfähigen wie Kindern verarbeiten, darüber hinaus aber auch dann zu vermuten, wenn neue Technologien verwendet werden oder Sie eine Videoüberwachung installiert haben.
- Wenn ein solches Risiko besteht, ist auf einer **zweiten Stufe** eine Bewertung dahingehend vorzunehmen, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichen, um den Schutz der Daten zu gewährleisten. Außerdem muss der Nachweis erbracht werden, dass die DSGVO eingehalten und den Interessen der Betroffenen Rechnung getragen wird. Bei den Abhilfemaßnahmen und Sicherheitsvorkehrungen handelt es sich um die TOMs (s. Punkt 9.2). Die Dokumentation dieser Maßnahmen dient als Nachweis für die Einhaltung der Betroffenenrechte und -interessen.
- Kommt die Bewertung zu dem Ergebnis, dass trotz möglicher Maßnahmen ein hohes Risiko besteht, muss auf einer **dritten Stufe** die Aufsichtsbehörde konsultiert werden (Art. 36 DSGVO). Diese kann innerhalb von acht Wochen Empfehlungen aussprechen. In der Apotheke wird dieses kaum vorkommen, da es in der Regel keine Verarbeitungstätigkeiten geben wird, bei denen nicht die schon getroffenen oder verstärkten Maßnahmen den Schutz der Daten gewährleisten.

Ist in dem Unternehmen ein DSB bestellt, muss er in die DSFA eingebunden werden. Die DSFA ist schriftlich zu dokumentieren. Es kann u.U. zweckmäßig sein, dies mit dem Verzeichnis der Verarbeitungstätigkeiten (s. Punkt 9.1) zu verknüpfen. Sie ist regelmäßig zu überprüfen. Wenn z.B. neue Technologien eingesetzt werden, ist auch eine neue Risikobewertung erforderlich.

Nähere Erläuterungen zu Inhalten und Ablauf einer Folgeabschätzung sowie ein Beispiel einer Folgeabschätzung für die Videoüberwachung im öffentlich zugänglichen Bereich der Apotheke finden Sie im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz.*

Auch wenn die Erforderlichkeit einer DSFA und die daraus folgende Pflicht zur Benennung eines Datenschutzbeauftragten in einigen Fällen noch strittig sind, so resultiert daraus gleichzeitig aber auch die Möglichkeit, sowohl Ihrem Kunden als auch der Aufsichtsbehörde deutlich zu vermitteln: Sie nehmen den Datenschutz ernst und die sensiblen Kundendaten sind bei Ihnen in guten Händen.

11. Wie sind die Betroffenen über die Verarbeitung ihrer Daten zu informieren?

Betroffene sind über die Verarbeitung ihrer personenbezogenen Daten zu informieren (sog. Transparenzpflichten). Die Inhalte sind in Artt. 13, 14 DSGVO geregelt. Informationspflichten beziehen sich u.a. auf:

- **Adresse des Datenverarbeiters**: Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten
- **Verarbeitungsrahmen**: Datenkategorien, Quelle der Daten, Spei-

Die allgemeine Information über die Verarbeitung der Daten ist nicht zu verwechseln mit der Einwilligung in einen Datenverarbeitungsvorgang.
Bei Letzterer ist eine aktive Einwilligung erforderlich (s. Punkte 8.1 u. 8.2).

cherdauer, Verarbeitungszweck, Rechtsgrundlage

- **Weitergabe der Daten**: Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- **Betroffenenrechte**: Auskunft, Berichtigung, Löschung, Beschwerderecht bei der Aufsichtsbehörde

Die Information muss zum Zeitpunkt der Erhebung erfolgen (nicht zwingend „vor" der Erhebung). Beim Erstellen einer Kundenkarte bietet sich an, diese Informationen im Zuge der Einwilligung des Kunden mittels eines gesonderten Info-Blattes zu erteilen. Da man aber natürlich nicht jedem Kunden, der ein Rezept einlösen will, einen Zettel in die Hand drücken kann, können die relevanten Informationen auch in einem Aushang in der Apotheke oder am HV-Tisch erfolgen. Wer einen Onlineshop betreibt, kann die nötigen Informationen in die Datenschutzerklärung auf der Webseite integrieren, auf die wiederum zu verlinken ist. Eine solche Information in der Datenschutzerklärung ist aber auch schon dann erforderlich, wenn personenbezogene Daten auf der Internetseite eingegeben werden, also z.B. bei der Bestellung eines Newsletters, einer Broschüren-Bestellung oder einer Anmeldung zu Informationsveranstaltungen. Vor dem „Absenden" muss der Kunde – egal, ob er etwas kauft oder nur z.B. einen Newsletter bestellt – durch eine aktive Handlung (z.B. das Setzen eines Hakens) bestätigen, dass er die entsprechende Datenschutzerklärung gelesen hat. Sprechen Sie Ihren Softwareanbieter darauf an.

Ein Muster für die erforderlichen Informationen per Aushang in der Apotheke finden Sie im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz*. Diese Information ist noch auf die Gegebenheiten in Ihrer Apotheke anzupassen.

Sie finden dort auch ein Beispiel für ein Informationsblatt, falls Sie eine Videoüberwachung durchführen.

Für die Erstellung der erforderlichen Informationen auf Ihrer Internetseite empfehlen wir Ihnen das individuell anzupassende Muster von Prof. Dr. Hoeren (Universität Münster), das Sie ebenfalls im Mitgliederbereich unserer Internetseite unter *Recht > Datenschutz* einsehen können.

EMPFEHLUNG:

Die Umsetzung der aufgezeigten Informationspflicht sollten Sie zum Anlass nehmen, Ihre Internetseite und insbesondere die Datenschutzerklärung generell darauf zu prüfen, ob diese den gesetzlichen Anforderungen entspricht. Die Internetseite ist Ihre digitale Visitenkarte. Das bedeutet zugleich auch, dass sie durch jeden eingesehen werden kann. Sowohl die Aufsichtsbehörde, insbesondere aber lästige Abmahnanwälte können sich so – quasi vom Schreibtisch aus – einen Eindruck darüber verschaffen, wie gut Ihre Apotheke datenschutzrechtlich aufgestellt ist.

Checken Sie Ihre Internetseite je nach Einsatzzweck!

12. Rechte der Betroffenen

12.1 Recht auf Auskunft:

Betroffene haben nach Art. 15 DSGVO ein Recht zu erfahren, ob ein für die Verarbeitung Verantwortlicher personenbezogene Daten, die sie betreffen, verarbeitet. Soweit dies der Fall ist, hat die betroffene Person weiter ein Recht auf Auskunft über die Umstände der Datenverarbeitung. Das schon früher bestehende Auskunftsrecht ist in einigen Punkten erweitert worden.

Auskunftsrechte muss der Verantwortliche grundsätzlich innerhalb eines Monats kostenlos beantworten.

Die Auskunft muss mindestens folgendem vorgeschriebenem Inhalt entsprechen:

- Zwecke der Verarbeitung
- Kategorien der personenbezogenen Daten, die verarbeitet werden
- Empfänger der verarbeiteten personenbezogenen Daten
- Dauer der Speicherung oder die Kriterien der für die Speicherung maßgeblichen Dauer
- Hinweis auf das Recht zur Berichtigung oder Löschung
- Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
- Informationen über die Herkunft der Daten, soweit diese nicht vom Betroffenen erhoben wurden

Die Auskunft ist umfassend zu erteilen. Es reicht nicht aus, diese auf die erhobenen Datenkategorien zu beschränken, sie muss vielmehr inhaltlich vollumfänglich mit konkreten Daten erfolgen. Nur so kann der Betroffene prüfen, ob die Daten richtig sind und die Auskunft vollständig. Dies umfasst ggf. die Vorlage der gesamten gespeicherten Korrespondenz.

Wird der Auskunftsanspruch elektronisch gestellt, so sind die Informationen grundsätzlich in einem gängigen elektronischen Format zu Verfügung zu stellen.

12.2 Recht auf Löschung („Recht auf Vergessenwerden“)

Das „Recht auf Vergessenwerden" ist als ein wesentlicher Grundsatz in Art. 17 DSGVO geregelt.

Nach Artikel 17 Abs. 1 DSGVO sind personenbezogene Daten künftig unverzüglich zu löschen, wenn:

- die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,
- die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt,
- die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen,
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden,
- die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist oder
- die personenbezogenen Daten eines Kindes in Bezug auf angebotene Dienste der Informationsgesellschaft, d.h. Internetangebote wie Medien, Webshops oder Online-Spiele, erhoben wurden.

Wurde bei der Einwilligung nicht darauf hingewiesen, dass die konkrete Verarbeitung auch aufgrund einer gesetzlichen Grundlage möglich ist, kann die Verarbeitung nach Widerruf der Einwilligung nicht mehr auf diese gesetzliche Grundlage gestützt werden.

Von der Löschungspflicht gibt es allerdings auch Ausnahmen. Sie besteht nicht, soweit die Verarbeitung in folgenden Fällen erforderlich ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information,

- zur Erfüllung einer Rechtspflicht oder öffentlichen Aufgabe,
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder
- für im öffentlichen Interesse liegende Archivzwecke, Forschungszwecke und statistische Zwecke.

Die Apotheke muss daher ein Konzept erstellen, in dem die Dateiarten bestimmt, Löschfristen nach den einzelnen Kategorien definiert und Regeln für die Löschung erstellt werden. Zudem ist festzuhalten, wie die Regeln zur Löschung umzusetzen sind.

Erstellen Sie ein Löschkonzept!

EMPFEHLUNG:

Die Löschfristen für die einzelnen Daten sind bereits Bestandteil des Verarbeitungsverzeichnisses, so dass Sie dieses heranziehen können. So können Sie z.B. eine Tabelle erstellen, in die Sie die Verarbeitungsvorgänge aus dem Verarbeitungsverzeichnis übernehmen, die Grundlagen der Speicherung (z.B. Nennung der gesetzliche Regelung, erteilte Einwilligung) auflisten, die Fristen nennen und die Termine für Kontrollen bzw. Löschung festlegen. Bei einer Einwilligung beachten Sie bitte, dass die Löschung nach Widerruf der Einwilligung sofort zu erfolgen hat und zu dokumentieren ist.

12.3 Recht auf Datenübertragbarkeit („Datenportabilität“):

Neu ist das Recht auf Datenübertragbarkeit. Betroffene haben damit das Recht, sämtliche Daten, die sie dem Verantwortlichen bereitgestellt haben, in einem gängigen und maschinenlesbaren Format zurückzuerhalten und diese einem anderen Verantwortlichen zu übermitteln bzw. direkt an den neuen Verantwortlichen übermitteln zu lassen. So kann z.B. ein Kunde vom Apothekeninhaber eine Kopie der im Rahmen der Kundenkarte und mit der Einwilligung erhobenen Medikationsdaten und geleisteten Zuzahlungen verlangen, um die Daten einer anderen Apotheke seiner Wahl zur Verfügung stellen zu können.

Es empfiehlt sich, zum Umgang mit Betroffenenrechten **organisatorisch Vorsorge** zu treffen, wie im Fall der Fälle mit Auskunftsansprüchen umgegangen wird, d.h. wer intern die Daten zusammenstellt, den Datenschutzbeauftragten einbezieht und in welchem Format die Daten zusammenzustellen sind. Fragen Sie auch Ihr Softwarehaus, ob es Ihnen eine solche Funktion zur Verfügung stellen kann. Dieses organisatorische Vorgehen sollte dokumentiert werden und ist Teil des DSMS.

13. Datenschutzverstoß – was gilt es jetzt zu tun?

Datenschutzverstöße sind nach Artt. 33 und 34 DSGVO innerhalb von 72 Stunden nach Bekanntwerden **der zuständigen Aufsichtsbehörde zu melden**, es sei denn, der Verstoß führt „voraussichtlich nicht zu einem Risiko für den Betroffenen".

Aufsichtsbehörde ist:

Landesbeauftragte für Datenschutz und Informationsfreiheit NRW
Helga Block
Kavalleriestraße 2-4
40213 Düsseldorf

Telefon: 02 11/384 24-0
Telefax: 02 11/384 24-10
E-Mail: poststelle@ldi.nrw.de
Homepage: http://www.ldi.nrw.de

Die Meldung muss folgende Informationen enthalten:

- ✓ eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- ✓ den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- ✓ eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- ✓ eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die Regelungen in Art. 33 DSGVO und § 65 BDSG-neu sind abstrakt gehalten. Sie konkretisieren meldepflichtige Sachverhalte nicht näher und enthalten keine Bagatellregelungen, so dass grundsätzlich jeder Sachverhalt, der eine Verletzung der Datenschutzbestimmungen zur Folge hat und bei dem nicht von vorneherein ein Risiko für die Betroffenen ausgeschlossen werden kann (und das ist die Regel), der Aufsichtsbehörde anzuzeigen ist.

Im Grundsatz ist jeder risikobehaftete Datenverstoß zu melden.

Beispiel: Verlust eines Apothekenlaptops oder eines Speichermediums, auf dem personenbezogene Daten von Kunden gespeichert sind (z.B. E-Mail-Korrespondenz). Um die entsprechenden Feststellungen für die Meldung treffen zu können, muss im Fall der Fälle klar sein, welche personenbezogenen Daten sich auf dem Datenträger befinden. Dies erfordert

sowohl eine gründliche Dokumentation als auch eine kontinuierliche, akribische Datensicherung.

Der Verantwortliche hat jede Verletzung des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

Frist: Unverzüglich, d.h. ohne schuldhaftes Verzögern seitens des Verantwortlichen.

ACHTUNG: Eine zusätzliche Meldung an den Betroffenen ist dann erforderlich, wenn ein „hohes Risiko" für dessen Rechte und Freiheiten besteht.

Die **Benachrichtigungspflicht entfällt** aber, wenn:

- der Verantwortliche Vorkehrungen getroffen hat, die Daten Unbefugten unzugänglich zu machen, etwa durch Verschlüsselung
- der Verantwortliche nachträglich Maßnahmen ergriffen hat, durch die das hohe Risiko für die Rechte und Freiheiten der Betroffenen aller Wahrscheinlichkeit nach nicht mehr bestehen
- sie einen unverhältnismäßig hohen Aufwand erfordern würde – dann muss allerdings eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen.

14. WhatsApp, Amazon & Co.

Schließlich soll noch kurz auf einige Sonderfälle eingegangen werden:

Die Apotheke bedient sich verschiedener Dienstleister und übermittelt diesen hierzu personenbezogene Daten. Regelhaft geschieht dies auf Grundlage einer Auftragsverarbeitung (s. Punkt 8.3). Dies jedenfalls dann, wenn der Dienstleister nur auf Weisung und im Pflichtenkreis des Apothekeninhabers tätig wird. Anderenfalls hat der Betroffene einzuwilligen (s. Punkt 8.2).

Insoweit ließe sich jetzt mit Blick auf WhatsApp und andere Messenger-Dienste argumentieren, dass der jeweilige Bestellvorgang durch den Kunden initiiert würde, sich deshalb also nicht die Apotheke, sondern der Kunde des Dienstes bedient und er dadurch (konkludent) in die (Weiter-)Verarbeitung seiner Daten einwilligt. Abgesehen davon, dass eine konkludente Einwilligung in die Verarbeitung von Gesundheitsdaten nicht möglich ist, geht es letztlich auch um einen anderen Aspekt: **Der Apotheker entscheidet über das „Ob" der Nutzung und stellt den Nutzern über WhatsApp einen Bestellweg zur Verfügung. Damit übernimmt er auch die volle Verantwortung für die betroffenen Daten.**

Insbesondere muss er die technischen und organisatorischen Vorkehrungen treffen, um den Anforderungen der DSGVO gerecht zu werden. Bei WhatsApp stößt er jedoch zwangsläufig an seine Grenzen, denn es werden von den Nutzern nicht nur die für die Bestellung erforderlichen Daten verarbeitet. Der Dienst greift z.B. auch auf das vollständige Adressbuch

eines Nutzers zu. Wozu und wo diese Daten genutzt und gespeichert werden, kann der Apotheker nicht kontrollieren, geschweige denn ist die Verarbeitung durch einen vorher mitgeteilten Zweck „gedeckt".

Noch schwerer wiegt allerdings der Umstand, dass WhatsApp die Daten in die USA auf dort stehende Server transferiert. Eine Speicherung in sog. Drittländern außerhalb der EU ist jedoch untersagt, sofern das dortige Schutzniveau nicht ausreicht. Bzgl. der USA genügt das Schutzniveau nicht, sodass bereits dieser Umstand die Verwendung von WhatsApp unzulässig macht. **Der Einsatz von WhatsApp ist somit rechtwidrig und wird ggf. mit einem Bußgeld geahndet.**

Soweit Medikamente über Amazon vertrieben werden, hat jüngst das Landgericht Dessau eine viel beachtete Entscheidung gefällt: Es hat entschieden (Urteil vom 28.03.2018, Az. 3 O 29/17), dass der Vertrieb von Medikamenten über Amazon unzulässig ist, solange bei dem Anmelde- bzw. Kaufprozess nicht sichergestellt sei, dass der Kunde vorab seine Einwilligung mit der Verarbeitung seiner Gesundheitsdaten erteilt habe. Die Einwilligung müsse sich explizit auf die Gesundheitsdaten beziehen. Ferner müsse ihr zu entnehmen sein, welche Daten in welchem Kontext unter welchen Bedingungen und für welche Zwecke verarbeitet werden. Auch sah das Gericht darin einen durch einen Mitbewerber abmahn- und beklagbaren Wettbewerbsverstoß, denn die Kundendaten, die von Amazon im Rahmen des Kaufs verarbeitet würden, würden zu kommerziellen Zwecken verarbeitet. Das Wettbewerbsrecht sei deshalb anwendbar, sodass der Mitbewerber u.a. zur Abmahnung befugt sei.

Eröffnen Sie also Ihren Patienten und Kunden digitale Möglichkeiten zur Bestellung, Korrespondenz etc., dann vergewissern Sie sich stets anhand der skizzierten Grundsätze, ob Sie das Medium vollständig kontrollieren, also insbesondere die Hoheit über die Daten besitzen sowie deren Vertraulichkeit gewährleisten können. Ferner denken Sie stets daran: **Keine Verarbeitung ohne Rechtsgrundlage und nur zu vorab bestimmten Zwecken!** Denken Sie schlussendlich an die Informations- und Transparenzpflichten zum Zeitpunkt der Datenerhebung.

15. Wo können Sie sich weiter informieren?

Douglas/Kalkbrenner, Arzneimittel & Recht (A&R)
„Die datenschutzrechtliche Bewertung der Einbindung von WhatsApp in die Arzneimittelvorbestellung“ – A&R, 2018, S. 3 ff.

Franze, Pharmazeutische Zeitung (PZ)
beginnend mit PZ Nr. 03/2018, S. 46ff und 07/2018, S. 52 ff (wird fortgesetzt)

Herz, Aktueller Wirtschaftsdienst für Apotheker (AWA)
„Umsetzung der neuen EU-Datenschutz-Grundverordnung: Rückhalt durch das Warenwirtschaftssystem“ - Ausgabe 06/2018, S. 7

Hossenfelder, Betriebs-Berater (BB)
„Die DSGVO kommt bald: TOP 5 Handlungsempfehlungen zur Umsetzung des neuen Datenschutzrechts.“ – Ausgabe 18/2018, S. 963

Kieser/Buckstegge, Apotheker Zeitung (AZ)
„Neue Datenschutzregeln ante portas“, wöchentlich, 7-teilige Serie beginnend in Nr. 10, S.6 ff.

Mecking, Apotheke heute (AH)
„Neue Anforderungen im Apothekenalltag durch die Datenschutz-Grundverordnung der EU (DSGVO)“ - Ausgabe 02/2018, S. 8 ff.
„Das neue Bundesdatenschutzgesetz: Machen Sie Ihre Apotheke fit für den Datenschutz“ - Ausgabe 04/2018; S. 8 ff.
„Das neue Datenschutzrecht: Last-minute-Tipps“ - Ausgabe 05/2018; S. 9 ff.

Mecking, AWA
„Der Countdown läuft: EU-Datenschutz-Grundverordnung ante portas“ - Ausgabe 03/2018, S. 14 f.
„Neue Datenschutz-Vorschriften: Tipps für das Verzeichnis von Verarbeitungstätigkeiten in der Apotheke“ - Ausgabe 05/2018, S. 14 f.
„Besonders heikel im neuen Datenschutzrecht: Der richtige Umgang mit Gesundheitsdaten“ - Ausgabe 07/2018, S. 14 f.
„Datenschutzbeauftragter und Datenschutz-Folgenabschätzung: Was Apothekenleiter wissen müssen.“ – Ausgabe 09/2018, S. 14f.

Pomana/Schneider, BB
„Wettbewerbsrecht und Datenschutz: Facebook im Visier des Bundeskartellamts.“ – Ausgabe 18/2018, S. 965f.

Theuringer, AWA
„Ein weiterer Aspekt der Datenschutz-Grundverordnung – Was gilt beim Arbeitnehmer-Datenschutz?“ - Ausgabe 08 / 2018, S. 14

Wybitul, BB
„Die DSGVO tritt in Kraft – wie geht es weiter?“ – Ausgabe 18/2018, S. 1

Verschiedene **Rechenzentren und Softwarehäuser** haben ihrerseits die sie betreffenden Unterlagen überarbeitet und teilweise schon versandt. Zudem bieten einige von ihnen Seminare etc. an.

AVWL-Seminare zum Thema „EU-Datenschutzgrundverordnung – was gilt es zu beachten?“ Referentin: Rechtsanwältin Patricia Kühnel. Die aktuellen Termine sind ausgebucht. Im Herbst sind weitere Termine geplant. Daneben gibt es aber derzeit eine ganze Reihe von Seminarangeboten durch Fremdanbieter.

Zu guter Letzt

Es besteht kein Anlass zu übereilten Aktionen und unüberlegtem Tätigwerden!

Die wichtigsten Schritte sind zunächst die Auswahl und Benennung eines Datenschutzbeauftragten, die Angabe der erforderlichen Kontaktdaten auf der Internetseite und anschließend die Meldung bei der Aufsichtsbehörde (sobald technisch möglich). Überprüfen Sie bei der Gelegenheit unbedingt auch die Datenschutzerklärung auf Ihrer Internetseite.

Auch wenn Sie nicht alle Dokumentationen sofort erstellen können, so ist es wichtig, technisch-organisatorisch sicherzustellen, dass niemand unbefugt auf die Daten Zugriff nehmen kann. Bewahren Sie bereits vorliegende Dokumente wie Verfahrensverzeichnisse und Einwilligungen auf, auch wenn Sie diese jetzt erneuern. Denn es kommt auch auf die historische Nachvollziehbarkeit an. Schließlich gilt es, die Mitarbeiter rechtzeitig zu informieren, zu integrieren und zu sensibilisieren.

Wir hoffen, wir konnten Ihnen mit diesem Leitfaden die beabsichtigte Hilfe zur Selbsthilfe ermöglichen. Für Anregungen, Ergänzungen, selbstverständlich aber auch für inhaltliche Kritik sind wir Ihnen dankbar und nehmen diese gerne entgegen.