Datenschutz in der Apotheke

Seit 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) sowie das Datenschutz-Anpassungs- und -umsetzungsgesetz EU.

Hier helfen wir Ihnen, die wichtigsten Fragen zum Datenschutz in Ihrer Apotheke zu klären. Außerdem finden Sie Links zu hilfreichen weiterführenden Informationsquellen und Verweise auf geeignete Muster (bspw. für Ihre Datenschutzerklärung für die Homepage und Ihre Offizin). Die Muster sollen eine erste Orientierung geben und werden, auch mit Anregungen aus der Kollegenschaft, stetig aktualisiert und durch Ihre Anfragen und Hinweise ergänzt und vervollständigt.

Kontaktdaten der zuständigen Aufsichtsbehörde für Datenschutz:

Sächsische Datenschutz- und Transparenzbeauftragte
Postfach 11 01 32
01330 Dresden
Telefon: 0351/85471-101
Fax: 0351/85471-109
E-Mail: post@stdb.sachsen.de
Internet: www.datenschutz.sachsen.de

Literatur und Info-Material

Patricia Kühnel, Apotheke und Datenschutz, 3. Auflage, Stand: 2018
Andreas Schaupp, Datenschutz, Arbeitshilfe für die Apotheke, 2018
Thomas Kieser, Svenja Buckstegge, Pflichtenschulung Datenschutz, 3. Auflage, 2021

Die Sächsische Datenschutz- und Transparenzbeauftragte veröffentlicht jährlich einen Tätigkeitsbericht zum Datenschutz. Darin fasst sie die Arbeit des zurückliegenden Jahres zusammen, insbesondere: Schwerpunkte der Aufsichtstätigkeit, Statistiken, Hinweise zur Auslegung der DSGVO, zur Sanktionspraxis und zur Rechtsprechung im Datenschutz (https://www.datenschutz.sachsen.de/taetigkeitsberichte.html)

Juliane Franze, *Das neue Datenschutzrecht in der Apotheke*, PZ Nr. 3 vom 18. Januar 2018, S. 46 ff.
Juliane Franze, *Der Datenschutzbeauftragte in der Apotheke*, PZ Nr. 7 vom 15. Februar 2018, S. 52 ff.

Artikelreihe „DSGV in der Apotheke“ in der Apothekerzeitung (Montagsausgabe der DAZ)
Teil 1: *Die Grundsätze der Datenverarbeitung* (AZ Nr. 10 vom 5. März 2018, S. 6-7)
Teil 2: *Die neuen Dokumentations- und Rechenschaftspflichten* (AZ Nr. 11 vom 12. März 2018, S. 6-7)
Teil 3: *Wächter über den Datenschutz: Der Datenschutzbeauftragte* (AZ Nr. 12 vom 19. März 2018, S. 6)
Teil 4: *Neue Risikobewertung – die Datenschutzfolgeabschätzung* (AZ Nr. 13/14 vom 26. März 2018, S. 6)
Teil 5: *Informationspflichten und Kundenrechte* (AZ Nr. 15 vom 9. April 2018, S. 6–7)
Teil 6: *Auftragsverarbeitung bei Rezeptabrechnung, Apps, Fernwartung* (AZ Nr. 16 vom 16. April 2018, S. 5)
Teil 7: *Verstöße gegen das Datenschutzrecht – Meldepflichten und Sanktionen* (AZ 2018, Nr. 17 vom 23. April 2018, S. 5)

Ausführliche Praxishilfen, Leitfäden, Muster und To-Do-Listen finden unter
https://www.gdd.de/service/publikationen-und-aktionen/

Die wichtigsten Fragen zum Thema "Datenschutz in der Apotheke" im Überblick:
1) Ist für meine Apotheke ein Datenschutzbeauftragter notwendig?
2) Prüfung des Internetauftritts; Datenschutzerklärung
3) Prüfung von Einwilligungserklärungen
4) Belehrung von Mitarbeitern
5) Prüfung von Verträgen mit Drittanbietern in Bezug auf Auftrags(daten)verarbeitung
6) Erstellung eines Verarbeitungsverzeichnisses
7) Erarbeitung einer Datenschutzfolgeabschätzung
8) Sind Leitbild und Prozessbeschreibung des QMS angepasst?

1) Ist für meine Apotheke ein Datenschutzbeauftragter notwendig?

Ob eine Apotheke einen Datenschutzbeauftragten bestellen muss, hängt von mehreren Faktoren ab.

Anhaltspunkte geben hier aber die folgenden Kriterien, nach denen Sie einen Datenschutzbeauftragten benennen müssen, sofern auch nur **einer (!)** der folgenden Punkte auf Ihre Apotheke zutrifft:

1. **Kerntätigkeit der Apotheke:** Wenn die Apotheke als Kerntätigkeit regelmäßig und systematisch umfangreiche Überwachung von betroffenen Personen durchführt oder besondere Kategorien personenbezogener Daten (wie Gesundheitsdaten) in großem Umfang verarbeitet, ist ein Datenschutzbeauftragter erforderlich.

   Die DSGVO und das BDSG bieten keine explizite Definition, ab wann eine Verarbeitung von Gesundheitsdaten "im großen Umfang" vorliegt. Allerdings haben Aufsichtsbehörden und Datenschutzexperten einige Kriterien entwickelt, die bei der Bewertung helfen können. Folgende Faktoren sollten berücksichtigt werden:

   - **Anzahl der betroffenen Personen**: Die Anzahl der Personen, deren Daten verarbeitet werden, ist ein wesentlicher Faktor.
   - **Datenvolumen und -vielfalt**: Die Menge und Vielfalt der verarbeiteten Gesundheitsdaten spielen eine Rolle (z. B. Führung detaillierter Patientenakten und Verarbeitung einer Vielzahl unterschiedlicher Gesundheitsdaten)
   - **Geografischer Umfang**: Die geografische Reichweite der Datenverarbeitung kann ebenfalls ein Indikator sein (z. B. eine Apotheke, die Daten von Patienten aus einer größeren Region oder mehreren Standorten sammelt)

   Eine kleine Apotheke in einer ländlichen Gegend, die Daten von einigen Patienten verarbeitet, würde wahrscheinlich nicht als "im großen Umfang" betrachtet werden. Ein Filialverbund, der zentrale Datenbanken verwendet und Daten von Patienten aus mehreren Filialen verarbeitet, könnte als "im großen Umfang" betrachtet werden. Es gibt keine feste Schwelle, ab der eine Verarbeitung von Gesundheitsdaten als "im großen Umfang" betrachtet wird. Es ist eine Einzelfallbewertung erforderlich, bei der die genannten Faktoren berücksichtigt werden. Im Zweifel kann es sinnvoll sein, Rücksprache mit der zuständigen Datenschutzbehörde zu halten oder einen Datenschutzexperten zu konsultieren, um die genaue Situation zu bewerten.

2. **Anzahl der Mitarbeiter**: Gemäß § 38 BDSG ist ein Datenschutzbeauftragter notwendig, wenn in der Apotheke in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

3. **Verarbeitung mit hohem Risiko**: Wenn die Apotheke besonders sensiblie Daten verarbeitet, die einer Datenschutz-Folgenabschätzung (DSFA) unterliegen (z. B. die Erhebung von biometrischen Daten der Mitarbeiter durch sog. Fingerprint-Systeme).

Die Antwort des Sächsischen Datenschutzbeauftragten vom 7. Mai 2018 zu unserer Anfrage "Bestellung eines Datenschutzbeauftragten in der Apotheke" finden Sie auf unserer SLAK-Homepage (damals lag die Grenze der Mitarbeiter noch bei 10 statt 20). Eine generelle Bestell**pflicht** bei Apotheken allein aufgrund der Verarbeitung von Gesundheitsdaten wurde hierbei verneint. Maßgeblich sind die oben genannten Kriterien. Nach aktuellen Erkenntnissen muss wegen einer Videoüberwachung noch kein Datenschutzbeauftragter benannt werden. Falls Sie unsicher sind, grundsätzlich aber gegen die Benennung eines internen Datenschutzbeauftragen nichts spricht, wäre es in diesem Fall nicht schädlich, einen solchen zu benennen und bei der Aufsichtsbehörde anzuzeigen.

Die DSGVO liefert diesbezüglich einen Anreiz für freiwillige Bestellungen: Der/Die Datenschutzbeauftragte/r hat, anders als der/die für die Verarbeitung Verantwortliche, einen Anspruch auf unentgeltliche Beratung durch die Aufsichtsbehörde (Art. 57 Abs. 3 DSGVO). Ein weiteres Argument für die freiwillige Bestellung eines Datenschutzbeauftragen könnte sein, dass die Bestellung eines solchen als zentraler Beitrag zur Gewährleistung von Datenschutzkonformität und als Vermeidung von Unternehmensrisiken gilt.

Anforderungen an den zu bestellenden Datenschutzbeauftragten:

- Der zu benennende (interne) Datenschutzbeauftragte muss für diese Aufgabe die nötige Qualifikation und das hierfür notwendige Fachwissen besitzen oder sich aneignen.
- Die zu benennende Person darf aufgrund der Tätigkeit als Datenschutzbeauftragte nicht in Interessenskonflikte geraten, d. h. der Apothekeninhaber selbst kann kein Datenschutzbeauftragter werden, da dies zur Folge hätte, dass er sich als zugleich Verantwortlicher selbst überprüfen müsste.

Die Bestellung des Datenschutzbeauftragten sollte, auch wenn diese grundsätzlich formfrei ist, zumindest in Textform erfolgen. Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht werden (z. B. in Ihren Datenschutzerklärungen auf der Homepage und in der Offizin) und der Aufsichtsbehörde (Sächsische Datenschutz- und Transparenzbeauftragte) mitgeteilt werden (Art. 37 Abs. 7 DSGVO).

Unter https://www.datenschutz.sachsen.de/datenschutzbeauftragten-melden.html finden Sie das Onlineformular zur Mitteilung über die Bestellung eines Datenschutzbeauftragten.

Datenschutzbeauftragter	
Intern	Extern
Vorteil • Kennt sich mit den Gegebenheiten in der Apotheke aus • Ist vor Ort • Beratung und Entscheidungen sind individueller • Keine zusätzlichen Kosten **Nachteil** • Fachwissen und Kompetenz hängt von den eingeräumten Fortbildungsmöglichkeiten des Arbeitgebers ab • Arbeitskapazitäten des betreffenden Personals werden eingeschränkt **Achtung!** • Sonderkündigungsschutz des Datenschutzbeauftragten beachten	**Vorteil** • Qualifizierte und fachlich kompetente Beratung ist zu erwarten • Apotheke kann von Expertise einer Vielzahl von Fällen und betreuten Unternehmen profitieren **Nachteil** • Kennt sich mit den Gegebenheiten vor Ort nur beschränkt aus; vor allem durch viele Sondervorschriften im Bereich der Heilberufe (Stichwort Gesundheitsdaten, Schweigepflicht nach § 203 StGB) ist im Zweifel nicht jeder externe Datenschutzbeauftragte gleich gut geeignet • Apotheke muss Dritten detaillierte Einblicke in Firmeninterna gewähren • Kosten

2) Prüfung des Internetauftritts; Datenschutzerklärung

Ein Muster zur Orientierung für die Erarbeitung einer **Datenschutzerklärung für Ihren Internetauftritt** finden Sie auf unserer SLAK-Homepage.

Ein etwas umfangreiches Muster von Professor Dr. Thomas Hoeren, das zusammen mit Mitarbeitern der Forschungsstelle Recht des DFN Vereins entwickelt wurde, finden Sie auf unserer SLAK-Homepage.

Bitte beachten Sie hinsichtlich Ihres Internetauftritts auch unsere Hinweise und Vorbehalte zu Kommunikationswegen, wie beispielsweise WhatsApp (Informationsblatt SLAK V/2017, S. 11).

Ebenso wichtig ist die Information Ihrer Patienten in Form einer **Datenschutzerklärung in Ihrer Offizin.** Das von der ABDA erstellte Muster finden Sie auf unserer SLAK-Homepage.

Ein Informationsblatt/Aushang zur Videoüberwachung der Landesbeauftragten für den Datenschutz Niedersachsen finden Sie auf unserer SLAK-Homepage.

Nähere Ausführungen zu den Betroffenenrechten, auf die Sie jeweils in Ihren Datenschutzerklärungen hinweisen müssen, finden Sie in AZ Nr. 15 vom 9. April 2018, S. 6 – 7, Teil 5: *Informationspflichten und Kundenrechte* erläutert.

3) Prüfung von Einwilligungserklärungen

Im Datenschutzrecht gilt der Grundsatz des „Verbots mit Erlaubnisvorbehalt“. Dies bedeutet, dass jedwede Datenerhebung und Verarbeitung grundsätzlich verboten ist, es sei denn, diese wird durch Rechtsvorschriften oder Einwilligung des Betroffenen legitimiert.

Sollten Sie in Ihrer Apotheke Kundenkarten nutzen, achten Sie darauf, dass Ihre hierfür eingeholten Einwilligungserklärungen noch den Maßgaben der DSGVO entsprechen. Sie müssen vor allem folgende Punkte enthalten:

- Die Einwilligungserklärung muss den konkreten Zweck der Datenerhebung und -verarbeitung beschreiben.

- Informationen, wer bzw. ob Dritte Zugang zu den Daten haben werden (Soll Kundenkarte im Filialverbund nutzbar sein, muss Patient darüber unterrichtet werden, dass seine Daten auf einem Server gespeichert werden, auf den auch andere Filialapotheken Zugriff haben).

- Hinweis auf die Betroffenenrechte (siehe Pkt. 2); Wichtig sind in diesem Zusammenhang vor allem die Beschreibungen zum Löschen der Daten. Unproblematisch ist die personenbezogene Speicherung der abgegebenen Arzneimittel für ca. zwei Jahre. Über diesen Zeitraum hinaus lässt sich u. a. der Zweck der Speicherung von Medikationsübersichten für die Krankenkasse und das Finanzamt des Patienten kaum rechtfertigen. Sollte eine längerfristige Speicherung der Daten für das Medikationsmanagement des Patienten erforderlich sein, muss dies in der Zweckbestimmung der Datenerhebung ausdrücklich benannt und erläutert werden.

- Außerdem ist der Patient über sein Widerrufsrecht zu belehren.

Einwilligungen, die bis zum 25. Mai 2018 eingeholt wurden und nicht den Anforderungen der DSGVO entsprechen, sind für die Verarbeitung nach dem 25. Mai unwirksam. Es müssen neue, aktualisierte Einwilligungen eingeholt werden. Alle übrigen Einwilligungen, die vor dem 25. Mai eingeholt wurden und bereits diesen Maßgaben entsprechen, behalten ihre Wirksamkeit.

Nähere Ausführungen zum Thema Einwilligungserklärungen und Kundenkarten finden Sie in:

Juliane Franze, Das neue Datenschutzrecht in der Apotheke, PZ Nr. 3 vom 18. Januar 2018, S. 46 ff., abrufbar unter https://www.pharmazeutische-zeitung.de/index.php?id=73729

Ein ABDA-Muster für eine Einwilligungserklärung bzgl. Kundenkarten finden Sie auf unserer SLAK-Homepage.

4) Belehrung von Mitarbeitern

Ihren Mitarbeitern sollten die Neuerungen im Datenschutzrecht bekannt sein. Zu Beweis- und Dokumentationszwecken ist es sinnvoll, Unterweisungen durchzuführen und die Belehrung durch Ihre Mitarbeiter mit Datum und Unterschrift bestätigen zu lassen.

Die Meldung von Datenpannen muss innerhalb von 72 Stunden gegenüber der Aufsichtsbehörde erfolgen (in Ihrem Fall der Sächsischen Datenschutz- und Transparenzbeauftragten unter https://www.datenschutz.sachsen.de/meldung-eines-datenschutzverstosses.html).

Bei der Meldung ist zu beachten, dass der Apotheker zugleich dem Berufsgeheimnis unterliegt und somit nicht die konkreten personenbezogenen Daten der Patienten melden darf, sondern, soweit möglich, sich auf die ungefähre Anzahl der betroffenen Personen und welche Kategorien von Daten (zum Beispiel Gesundheitsdaten) betroffen sind, beschränken muss.

Gemäß § 53 BDSG dürfen mit der Datenverarbeitung befasste Personen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Danach ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch

nach der Beendigung der Tätigkeit fort. Im Bereich des Apothekerberufs ist außerdem die Verschwiegenheitsverpflichtung nach § 203 Strafgesetzbuch (StGB) zu beachten.

Zu Beweis- und Dokumentationszwecken sollte der Apothekeninhaber sowohl das eigene Personal als auch etwaige externe Dritte mittels schriftlicher Verpflichtungserklärung zur Verschwiegenheit unter Hinweis auf die strafrechtlichen Folgen einer Pflichtverletzung unterweisen und sich diese gegenzeichnen lassen.

5) Prüfung von Verträgen mit Drittanbietern in Bezug auf Auftrags(daten)verarbeitung

Eine Auftragsdatenverarbeitung liegt immer dann vor, wenn Datenverarbeitungsprozesse auf einen oder mehrere externe Dienstleister ausgelagert werden. Im Rahmen solcher Auftragsverhältnisse bedarf es einer schriftlichen Zusicherung, dass das Rechenzentrum oder der IT-Dienstleister den Anforderungen der DSGVO sowie dem nationalen Recht genügt. Der Grund für eine solche Zusicherung liegt darin, dass der Apothekeninhaber aus datenschutzrechtlicher Sicht trotz der Verarbeitung durch Dritte Verantwortlicher bleibt und damit seinen Kontrollpflichten nachkommen muss. Diese Kontrollen müssen hierbei nicht zwingend vor Ort erfolgen, es genügt dem Überprüfungserfordernis, wenn sich der Apothekeninhaber die Einhaltung der datenschutzrechtlichen Vorschriften durch Zertifikate und anderen Garantien des Auftragsdatenverarbeiters zusichern lässt.

Eine solche Zusicherung des Auftragsdatenverarbeiters sollte folgende Punkte enthalten:

- Benennung der Beteiligten,
- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung der Daten,
- Art der zu verarbeitenden Daten,
- Benennung der Kategorien der betroffenen Personen (Personenkreise),
- Beschreibung der technisch-organisatorischen Maßnahmen,
- Rechte und Pflichten des Auftragnehmers,
- Rechte und Pflichten des Auftraggebers,
- Unterauftragsverhältnisse,
- Regelung zur Löschung und Rückgabe von personenbezogenen Daten bei Beendigung des Auftragsverhältnisses.

In der Regel wird sich eine Apotheke ausschließlich in der Rolle des Auftraggebers befinden. Zumeist ist es auch üblich, dass eine solche Zusicherung durch den Auftragnehmer erstellt wird, da nur dieser die Möglichkeit hat, seine Datenverarbeitungsprozesse darzustellen und die hierfür notwendigen Sicherungsmaßnahmen vorzuweisen. Prüfen Sie in diesem Zusammenhang die Unterlagen Ihrer Drittanbieter und fordern Sie eine solche Zusicherung von diesen ab, sofern diese noch nicht vorliegt.

Drittanbieter sind beispielsweise:

- IT-Dienstleister,
- Rechenzentren,
- Anbieter von datenspeichernder Hardware (z. B. geleaste Drucker und Kopierer).

6) Erstellung eines Verarbeitungsverzeichnisses

Den Inhalt des Verarbeitungsverzeichnisses regelt Art. 30 DSGVO. Danach müssen folgende Angaben gemacht werden:

- Name und Kontaktdaten des Verantwortlichen, seines Vertreters und des Datenschutzbeauftragten
- Kategorien der betroffenen Personen (z. B. Patientendaten)
- Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt werden (z. B. Mitarbeiter in Filialapotheken, Rechenzentren, Steuerberater)
- Wurden personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt?
- Auflistung automatisierter und teilweise automatisierter Verarbeitungen in Dateisystemen (z. B. auch Karteikartensysteme und Papieraktenablage)
- Welche personenbezogenen Daten werden verarbeitet?

- Zu welchem Zweck werden diese personenbezogenen Daten verarbeitet?
- Sinnvoll ist es, Rechtsgrundlagen für die aufgelisteten Verarbeitungsprozesse direkt im Verarbeitungsprozess anzugeben (z. B. Abrechnung mit der GKV, Vertrag, Einwilligung)

Dem Verantwortlichen nutzt die sorgsame Dokumentation zum Datenschutz vor allem auch vor dem Hintergrund, dass ihm die Nachweispflicht über die Einhaltung des Datenschutzrechts gegenüber Aufsichtsbehörden, Betroffenen und in juristischen Auseinandersetzungen obliegt.
Ein ABDA-Muster zur Orientierung finden Sie auf unserer SLAK-Homepage.

Einen Leitfaden mit Muster eines Verarbeitungsverzeichnisses finden Sie außerdem unter https://www.gdd.de/service/publikationen-und-aktionen/

7) Erarbeitung einer Datenschutzfolgeabschätzung

Die Durchführung einer Folgeabschätzung wird dann notwendig, wenn in Ihrer Apotheke Verarbeitungsprozesse mit hohem Risiko für Rechte und Freiheiten natürlicher Personen vorliegen (Artikel 35 DSGVO).

Eine Datenschutzfolgeabschätzung ist danach u. a. in folgenden Fällen erforderlich:

1. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen oder
2. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder
3. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Unter Punkt 2 fallen u. a. auch die Erhebung und Verarbeitung von biometrischen Daten, wie z. B. der Einsatz von Fingerprint-Scannern.

Die Datenschutzbeauftragten der Länder und des Bundes haben ihre ersten Positivlisten für die Datenschutzfolgenabschätzung veröffentlicht. Es werden Verarbeitungsprozesse mit konkreten Beispielen aufgelistet, für die eine Folgenabschätzung gemäß Artikel 35 DSGVO durchzuführen ist und die in der Konsequenz eine Pflicht zur Benennung eines Datenschutzbeauftragen im Unternehmen nach sich ziehen.

Die Listen sind nicht abschließend und können jederzeit noch ergänzt oder inhaltlich abgeändert werden. Immerhin geben sie den Verantwortlichen schon einmal ein Gefühl dafür, welche Verarbeitungsprozesse einer Folgenabschätzung zu unterziehen sein könnten. Für die Apotheken lässt sich nach erster Durchsicht zunächst sagen, dass weder eine Videoüberwachung des Verkaufsraums noch der Einsatz von Rezeptscannern einer Folgenabschätzung bedarf.

Alle bislang verfügbaren Listen finden Sie verlinkt unter: https://www.datenschutzbeauftragter-info.de/erste-deutsche-positivlisten-fuer-die-datenschutz-folgenabschaetzung/

Wenn Sie eine Folgeabschätzung durchzuführen haben, unterliegen Sie gemäß § 38 Absatz 1 BDSG auch automatisch der Pflicht zur Bestellung eines Datenschutzbeauftragten (siehe Punkt 1).

Nach Artikel 35 Abs. 7 DSGVO enthält die Folgeabschätzung zumindest Folgendes:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Ein ABDA-Muster zur Folgeabschätzung finden Sie auf unserer SLAK-Homepage.

8) Sind Leitbild und Prozessbeschreibung des QMS angepasst?

Die vorgenommenen Änderungen sollen sich abschließend auch im Qualitätsmanagement Ihrer Apotheke widerspiegeln. Hierfür kann an den betroffenen Stellen in den Arbeitsabläufen auf die entsprechenden Dokumente verwiesen werden. Es empfiehlt sich, bspw. die notwendigen Belehrungen und Unterweisungen von Beschäftigen zur Verschwiegenheit, zum Datenschutz und dem Umgang mit Datenlecks zu dokumentieren und die hieraus abzuleitenden Vorgehensweisen in die Prozessbeschreibungen zu integrieren.