Das neue Datenschutzrecht in der Apotheke

Juliane Franze, Berlin. Ab dem 25. Mai 2018 gilt die europäische Datenschutz-Grundverordnung (kurz DS-GVO) unmittelbar und ohne weitere Umsetzungsakte im gesamten EU-Raum. In Deutschland wird sie das bisherige nationale Datenschutzrecht weitestgehend ablösen. Aber auch der deutsche Gesetzgeber ist aktiv geworden und hat die Öffnungsklauseln in der DS-GVO genutzt, die es den Mitgliedstaaten erlauben, konkretere Regelungen in bestimmten Bereichen des Datenschutzes zu erlassen. Dazu hat er ein neues Bundesdatenschutzgesetz (kurz BDSG-neu) erlassen, welches ebenfalls ab dem 25. Mai gelten wird. Die umfangreichen Neuregelungen sollten kein Anlass zur Panik sein, sondern vielmehr zum Anlass genommen werden, sich erneut mit dem Thema Datenschutz im eigenen Betrieb auseinanderzusetzen, auch wenn unter den Datenschutzexperten in einigen Fragen bzgl. Interpretation und konkreter Umsetzung der Normen noch Uneinigkeit besteht. Dieser Artikel gibt zunächst eine Übersicht über die für Apotheken wichtigsten zehn Neuerungen. In nachfolgenden Ausgaben der PZ wird dann vertieft auf Einzelthemen eingegangen.

1. Datenschutzbeauftragter

Auch weiterhin müssen viele Apotheken einen Datenschutzbeauftragten benennen. Der deutsche Gesetzgeber hat in § 38 BDSG-neu die Regelung übernommen, dass ein Datenschutzbeauftragter zu benennen ist, soweit in der Regel mindestens 10 Personen ständig mit der automatischen Verarbeitung personenbezogener Daten beschäftigt sind. Zu den automatisierten Verarbeitungen in der Apotheke zählen z.B. Rezeptabrechnungen oder die Zahlungen mit EC- und Kreditkarte. Bei der Berechnung ist zu beachten, dass Teilzeitkräfte als eine Person gelten und auch Auszubildende, Praktikanten und freie Mitarbeiter erfasst werden müssen. Bei Apotheken mit mehreren Filialen gilt, dass deren Mitarbeiteranzahlen nicht getrennt zu betrachten sind, sondern als eine Einheit. Es sollte daher ein Datenschutzbeauftragter für Haupt- und Filialapotheken zusammen benannt werden.

Sollte ein Betrieb weniger als 10 ständig mit der automatischen Verarbeitung personenbezogener Daten Beschäftigte haben, muss ein Datenschutzbeauftragter gleichwohl unabhängig von der Mitarbeiteranzahl benannt werden, wenn eine Datenschutz-Folgenabschätzung im Betrieb durchzuführen ist. Eine Folgenabschätzung ist gemäß Art. 35 DS-GVO immer dann durchzuführen, wenn eine Verarbeitung voraussichtlich ein besonders hohes Risiko für die Rechte und Freiheiten natürlicher Personen (keine Unternehmen, sondern Privatpersonen) zur Folge haben kann. Hier bestehen noch erhebliche Rechtsunsicherheiten in der Interpretation dieser Norm, die sich voraussichtlich erst durch gerichtliche Entscheidungen in den kommenden Jahren klären werden und die Apotheken und andere Betriebe bis dahin im Ungewissen lassen. Bei der Einschätzung, ob ein solches Risiko vorliegt, handelt es sich um eine Einzelfallentscheidung. Die Artikel-29-Datenschutzgruppe, ein Beratungsgremium auf EU-Ebene, hat dazu eine Liste von Kriterien als Orientierung veröffentlicht. Zu den Kriterien zählen unter anderem die Verarbeitung besonderer Kategorien von Daten, Daten von Geschäftsunfähigen und beschränkt Geschäftsfähigen sowie Datentransfers ins EU-Ausland. Der Begriff der besonderen Kategorien von Daten erfasst insbesondere Gesundheitsdaten, genetische Daten und Daten zum Sexualleben. Wenn weniger als zwei der auf der Liste der Artikel-29-Datenschutzgruppe genannten Kriterien erfüllt sind, ist davon auszugehen, dass keine Datenschutz-Folgenabschätzung erfolgen muss. In der Regel erfüllt eine Apotheke mindestens zwei der Kriterien, indem sie täglich Gesundheitsdaten und Daten von Geschäftsunfähigen wie Kindern verarbeitet. Die Annahme eines hohen Risikos und dem Erfordernis einer Datenschutz-Folgenabschätzung sowie der damit einhergehenden Pflicht zur Benennung eines Datenschutzbeauftragten erscheint naheliegend. Jedoch wird die umfangreiche Verarbeitung

besonderer Kategorien von Daten als Regelbeispiel für eine Pflicht zur Datenschutzfolgenabschätzung in Artikel 35 DS-GVO genannt. Eine solche umfangreiche Verarbeitung muss gerade bei kleineren Apotheken ernsthaft bezweifelt werden. Die Auslegung des Begriffs der „umfangreiche Verarbeitung“ ist derzeit noch nicht abschließend geklärt und unter den Datenschutzexperten streitig. Als Orientierung dient Erwägungsgrund 91 zur DS-GVO, wonach die Verarbeitung von Patientendaten durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs, wie Apotheker, keine umfangreiche Verarbeitung darstellt. Bei Krankenhäusern hingegen ist sicherlich von einer umfangreichen Verarbeitung auszugehen. Wie eine deutsche Durchschnittsapotheke mit 150 Patienten pro Tag einzuordnen ist, bleibt bisher unbeantwortet. Durch den Verzicht des Gesetzgebers auf klare Schwellenwerte wird jedoch deutlich, dass ein Risiko auch bei kleinen Personengruppen hoch sein kann. Es bleibt daher eine Einzelfallentscheidung, bei der in Zweifelsfragen eine rechtliche Beratung empfehlenswert ist.

Ein Datenschutzbeauftragter ist darüber hinaus unter den Voraussetzungen des Art. 37 DS-GVO zu benennen. Es wird unter weitgefassten Voraussetzungen die Benennung eines Datenschutzbeauftragten verlangt, die teilweise noch streitig zwischen den Datenschutzexperten sind. So ist ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit des Verantwortlichen (Apothekeninhaber) in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht. Zum Begriff der umfangreichen Verarbeitung ergeben sich auch hier die gleichen Fragestellungen, wie oben bereits dargestellt. Eine Kerntätigkeit ist nach vorherrschender Auffassung in der Literatur gegeben, wenn der Hauptzweck des Unternehmens in der Durchführung von Verarbeitungsvorgängen liegt. Die Haupttätigkeit ist dabei als Unternehmensschwerpunkt bzw. Unternehmensausrichtung und primärer Geschäftszweck zu verstehen. Von dieser Vorschrift sind Apotheken daher nach Auffassung der Autorin grundsätzlich nicht erfasst, da sie ihren Schwerpunkt in der Abgabe und Beratung zu Arzneimitteln, Medizinprodukten und apothekenüblichen Waren und nicht in der Datenverarbeitung haben.

Neu ist auch, dass jede betroffene Apotheke ab dem 25. Mai 2018 ihren Datenschutzbeauftragten der zuständigen Aufsichtsbehörde bzw. ihrem jeweiligen Landesdatenschutzbeauftragten melden muss.

Mehr zu den Fragen, wer als Datenschutzbeauftragter benannt werden sollte und welche Qualifikation und Aufgaben dieser erfüllen muss, wird in einem gesonderten Artikel thematisiert.

2. Informationspflichten/Datenschutzerklärung

Bei jeder Erhebung und Verarbeitung personenbezogener Daten in der Apotheke muss dem Betroffenen eine Datenschutzerklärung gemäß Artikel 12 ff. DS-GVO zugänglich sein. Eine Datenschutzerklärung dient der Information des Betroffenen, damit dieser die Tragweite der Verarbeitung seiner personenbezogenen Daten versteht und abschätzen kann. Daher sollte der Betroffene zumindest über Folgendes informiert werden:

- über die Kategorien der Daten (Gesundheitsdaten, Daten, aus denen die ethnische Herkunft etc. hervorgeht),
- Namen und Kontaktdaten des Verantwortlichen (Apothekeninhaber) und des Datenschutzbeauftragten sofern vorhanden,
- Zweck der Verarbeitung
- und die Rechtsgrundlage (Einwilligung, Vertragsabwicklung, Rechtsnorm z.B. § 300 SGB V zur Abrechnung mit den Gesetzlichen Krankenkassen),
- Empfänger oder Kategorien von Empfängern, sofern Daten an Dritte übermittelt werden (Rechenzentrum, Behörden).

Soweit es für eine faire und transparente Datenverarbeitung nötig ist, sollen die Dauer der Speicherung oder sofern diese Angabe nicht möglich ist, eine Darlegung der Kriterien wie lange gespeichert wird sowie die vertragliche oder gesetzliche Pflicht des Betroffenen zur Bereitstellung der Daten und Folgen bei Nichtbereitstellung angegeben werden. Weiterhin sollte ein Hinweis auf die Betroffenenrechte erfolgen, wie auf das Widerrufsrecht des Betroffenen bei einer Einwilligung, das Recht auf Auskunft über seine personenbezogenen Daten, das Recht auf Berichtigung und Löschung, Recht auf Datenübertragbarkeit, Recht auf Widerspruch gegen die Verarbeitung, Recht auf Beschwerde bei einer Aufsichtsbehörde und wie der Betroffene diese Rechte ausübt. Da eine Abwägung, ob die genannten Informationen für eine faire und transparente Verarbeitung nötig sind, schwierig ist, bleibt zu empfehlen, die Informationen ebenfalls standardmäßig in die Datenschutzerklärung aufzunehmen.

Die Informationen müssen dem Betroffenen spätestens bei der Erhebung bereitgestellt werden sowie bei jeder Weiterverarbeitung seiner personenbezogenen Daten zu einem anderen, neuen Zweck, ohne dass es einer Aufforderung durch den Betroffenen oder einer Mitwirkung des Verantwortlichen, dem Apothekeninhaber, bedarf. Insbesondere muss die Datenschutzerklärung dem Betroffenen mit dem ihm zur Verfügung stehenden, technischen Mitteln zugänglich sein. So bietet es sich etwa beim Erstellen einer Kundenkarte an, dem vom Patienten auszufüllenden analogen oder digitalen Formular eine Datenschutzerklärung und Einwilligungserklärung beizufügen. Da man jedoch nicht jedem Patienten einen Zettel mit einer Datenschutzerklärung in die Hand drücken will, wenn dieser nur schnell ein GKV-Rezept in der Apotheke einlösen möchte, empfiehlt es sich, einen Aushang mit einer Datenschutzerklärung gut sichtbar im Verkaufsraum anzubringen, wie man es vielleicht aus anderen Geschäften mit Aushängen zu den Allgemeinen Geschäftsbedingungen kennt. So hat jeder Patient zum Zeitpunkt der Erhebung seiner Daten die Möglichkeit, die Datenschutzerklärung wahrzunehmen. Darüber hinaus ist es möglich, die Datenschutzerklärung zusätzlich als QR-Code oder auf der Website zur Verfügung zu stellen.

Optisch muss sich die Datenschutzerklärung von anderen Inhalten, z.B. vom Formular einer Kundenkarte, abheben, damit sie dem Betroffenen überhaupt auffällt. Die Datenschutzerklärung sollte in einer klaren und einfachen Sprache und somit leicht verständlich für den Durchschnittspatienten gefasst sein.

Ein Verstoß gegen die Informationspflichten nach Artikel 13 und 14 DS-GVO führt grundsätzlich nicht zu einer Unzulässigkeit der Verarbeitung, er kann jedoch von der Aufsichtsbehörde mit einem Bußgeld geahndet werden.

3. Einwilligungserklärung

Wenn beim Betroffenen personenbezogene Daten erhoben werden, sollte sich jeder Verantwortliche in seinem Betrieb vergewissern, auf welcher Grundlage die Erhebung erfolgt, denn auch weiterhin gilt der Grundsatz des Verbotes mit Erlaubnisvorbehalt im Datenschutz. Als Erlaubnis kommen neben Rechtsnormen und Vertragsabwicklung besonders die Einwilligung des Betroffenen gemäß Artikel 7 DS-GVO in Betracht.

Der Betroffene muss durch eine eindeutige, bestätigende Handlung freiwillig für einen konkreten Zweck seine Einwilligung geben. Eine Einwilligung kann zwar in mündlicher Form abgegeben werden, jedoch ist der Verantwortliche in der Nachweispflicht, dass er auf Grundlage einer Einwilligung die personenbezogenen Daten erhebt und verarbeitet. Es empfiehlt sich daher immer eine Einholung der Einwilligung in Schriftform, also durch handschriftliche Unterzeichnung oder zumindest in Textform, z.B. per E-Mail. Bei Einwilligungen in elektronischer Form ist dies z.B. durch Setzen eines Hakens möglich, der Verantwortliche muss jedoch auch nachweisen, dass tatsächlich der Betroffene den Haken gesetzt hat. Es muss folglich zuvor eine Identifikation, z.B. durch Angabe des Namens, erfolgen. Auch der Einwilligungszeitpunkt sollte bei digitalen Einwilligungen vor der Verarbeitung gespeichert

werden. Optisch sollte sich die Einwilligungserklärung wie die Datenschutzerklärung von den restlichen Inhalten, z.B. durch Farbe, Umrahmung, Fettdruck oder andere Schriftart und –größe, abheben und sie darf nicht durch ein zuvor durch den Verantwortlichen angekreuztes Kästchen vorausgewählt sein. Es muss sich gerade um eine eindeutige, bestätigende, freiwillige Handlung des Betroffenen handeln, indem der Einwilligende ein Kreuz setzt (Opt-in) oder unter der Einwilligungserklärung unterschreibt.

Inhaltlich muss ein Augenmerk auf die klare Beschreibung des konkreten Zwecks der Datenerhebung- und Verarbeitung gelegt werden. Später dürfen diese Daten nur zu dem zuvor benannten Zweck verarbeitet werden. Eine Zweckänderung bedarf einer neuen Einwilligung und nochmaliger Bereitstellung der Datenschutzerklärung. Der Betroffene muss zudem darüber informiert werden, wer bzw. ob Dritte Zugang zu den Daten haben werden. Soll die Kundenkarte des Patienten auf einem zentralen Server gespeichert werden, auf den mehrere Betriebsstätten Zugriff haben, so ist dies in der Einwilligungserklärung darzulegen. Nur so ist es für den Patienten, der als Außenstehender die Inhaberverhältnisse an einzelnen Betriebsstätten im Filialverbund nicht kennen kann, ersichtlich, wer auf seine Daten Zugriff hat.

Mit der DS-GVO wird auch ein schärferes Kopplungsverbot eingeführt. Der Abschluss eines Vertrages darf nicht von einer Einwilligung abhängig gemacht werden, wenn diese zur Durchführung des Vertrages nicht notwendig ist. Werden zum Beispiel Medikationsdaten für ein Medikationsmanagement erhoben, so darf die Durchführung des Medikationsmanagements nicht von einer Einwilligung zur Zusendung von Werbung oder Weihnachtskarten abhängig gemacht werden. Vielmehr sollte eine Einwilligung zur Zusendung von Grußkarten, Werbung oder Gutscheinen gesondert, zum Beispiel durch das Setzen eines weiteren Hakens durch den Betroffenen, eingeholt werden. Daher lässt sich einfacher formuliert sagen: Eine Einwilligung pro Zweck.

Am Ende einer jeden Einwilligungserklärung muss sich wie auch unter der bisherigen Rechtslage weiterhin ein Hinweis über das Widerrufsrecht des Betroffenen mit Wirkung für die Zukunft finden.

Für eine problemlose Umstellung auf das neue Datenschutzrecht im Mai sollten nicht nur die Datenschutzerklärung und Einwilligungserklärungen aktualisiert werden, sondern auch die bereits eingeholten Einwilligungen überprüft werden. Einwilligungen, die bis zum 25. Mai 2018 eingeholt wurden und nicht den Anforderungen der DS-GVO entsprechen, sind für die Verarbeitung nach dem 25. Mai unwirksam. Es müssen neue, aktualisierte Einwilligungen eingeholt werden, auch wenn dies im täglichen Apothekenbetrieb mühselig ist. Alle übrigen Einwilligungen, die vor dem 25. Mai eingeholt wurden und der DS-GVO sowie der Richtlinie 95/46/EG bzw. dem bisherigen deutschen Recht entsprechen, behalten ihre Wirksamkeit.

4. Recht auf Löschung

Mit der DS-GVO wird auch das Recht auf Löschung bzw. „Vergessenwerden“ gestärkt. Für den Alltag in der Apotheke bedeutet dies, dass auf Wunsch des Patienten jederzeit seine Kundendaten oder ähnliches gelöscht werden müssen. Sofern die zu löschenden Daten auf mehreren Datenträgern oder ebenfalls in weiteren Betriebsstätten gespeichert werden, muss eine umfassende Löschung gewährleistet werden, indem beispielsweise ein Verzeichnis erstellt wird, wo Daten überall gespeichert und weitergeleitet werden. Nicht vom Recht auf Löschung sind jedoch die Daten erfasst, deren Verarbeitung auf einer Rechtsnorm beruhen. So müssen personenbezogene Daten, die zur Abrechnung mit der GKV benötigt werden oder einer gesetzlichen Dokumentations- bzw. Aufbewahrungspflicht unterliegen, nicht gelöscht werden. Diese Daten dürfen dann nur begrenzt und zu diesen Zwecken verarbeitet werden und müssen erst mit Ende der Aufbewahrungsfristen gelöscht werden.

5. Sicherheitsmanagement

Auch Apotheken sollten weiterhin ihren Betrieb auf Datensicherheit überprüfen und besonders ihre sensiblen Patientendaten vor einem unbefugten Zugriff Dritter schützen. Schon vor der Geltung der DS-GVO mussten Apotheken eine Dokumentation über ihre technischen und organisatorischen Maßnahmen pflegen, in der die Zugangs-, Zugriffs und Weitergabekontrolle etc. dargestellt wurden. Nunmehr sollten Maßnahmen vor allem gemessen an den Risiken für die Rechte und Freiheiten der Betroffenen ausgewählt und ergriffen werden. Es sollte sichergestellt werden, dass Firewall und Virenscanner auf dem neusten Stand sind und alle Datenträger, wie z.B. externe Festplatten, zumindest passwortgeschützt bzw. verschlüsselt sind.

6. Meldefristen bei Datenlecks

Sollte es im Betrieb doch zu einem Datenleck z.B. durch den Verlust von Datenträgern oder Phishing-Attacken gekommen sein, so muss eine damit einhergehende Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden gemäß § 65 BDSG-neu dem oder der Bundesbeauftragten für Datenschutz gemeldet werden. 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 (z.B. Gesundheitsdaten) betroffen sind, beschränken muss.

7. Höhere Bußgelder

Ein weiterer Ansporn, sich mit dem neuen Datenschutzrecht auseinanderzusetzen und es zu beachten, sollten die starken Erhöhungen der Bußgelder bei datenschutzrechtlichen Verstößen sein. Bei kleineren Verstößen, z.B. bei fehlerhaftem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, können bis zu 10.000 € oder 2% des Jahresumsatzes als Bußgeld anfallen, je nachdem welcher Betrag höher ist. Bei größeren Verstößen wie beispielsweise im Rahmen der Verarbeitung ohne Einwilligung können sogar bis zu 20.000 € oder 4% des Jahresumsatzes erhoben werden.

8. Portabilität der Daten

Artikel 20 DS-GVO gibt dem Betroffenen das Recht, die ihn betreffenden personenbezogenen Daten, die er dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten (Recht auf Datenübertragbarkeit). Die Apotheke muss daher in der Lage sein, Patientendaten wie z.B. Medikationsplan oder Kundenkartendaten in einem gängigen Format zu übermitteln, sodass die Daten ohne größere Kompatibilitätsprobleme an den Patienten oder auf seinen Wunsch an Dritte weitergeleitet werden können. Dazu werden die Apothekensoftware-Anbieter ihren Beitrag leisten müssen. Auch die kommende Telematikinfrastruktur sowie die elektronische Gesundheitskarte mit dem Medikationsplan werden die Portabilität der Daten fördern.

9. Auftragsdatenverarbeitung

Als weiterer Merkposten auf jeder To-Do-Liste zur Umstellung auf die DS-GVO sollte sich die Überprüfung aller Verträge zur Auftragsdatenverarbeitung finden. Eine schriftliche Zusicherung, dass das Rechtzentrum oder der IT-Dienstleister den Anforderungen der DS-GVO sowie dem nationalen Recht genügt, sollte für jede Austragsdatenverarbeitung vorhanden sein, denn der Apothekeninhaber bleibt aus datenschutzrechtlicher Sicht trotz der Verarbeitung durch Dritte Verantwortlicher und hat Kontrollpflichten. Die Kontrollen müssen nun nicht mehr unbedingt vor Ort erfolgen, sondern können durch einfache Überprüfung von Zertifikaten und anderen Garantien des Auftragsdatenverarbeiters erfolgen. Zudem sollte der Vertrag eine Absprache enthalten, dass eine Beauftragung von Unterauftragsnehmern nur mit schriftlicher Genehmigung des Verantwortlichen erfolgen darf.

10. Verarbeitungsverzeichnis und Dokumentation

Jeder Verantwortliche im datenschutzrechtlichen Sinne muss auch weiterhin eine sorgsame Dokumentation bzgl. Datenschutz führen, auch vor dem Hintergrund, dass ihm die Nachweispflicht über die Einhaltung des Datenschutzrechts gegenüber Aufsichtsbehörden, Betroffenen und in juristischen Auseinandersetzungen obliegt. So hat jede Apotheke ein Verzeichnis der Verarbeitungstätigkeiten zu führen, welches der bisher zu führenden Verfahrensdokumentation in weiten Teilen ähnelt. Muster für Verarbeitungsverzeichnisse finden sich online bei den Landesdatenschutzbeauftragten oder Gesellschaften und Verbänden für Datenschutz. Daneben oder besser gleich im Verarbeitungsverzeichnis selbst, sollten die Rechtsgrundlagen für die Verarbeitungsprozesse in der Apotheke (Abrechnung mit der GKV, Vertrag, Einwilligung) notiert werden. Weiterhin empfiehlt sich dem Betrieb entsprechend eine Dokumentation über die Belehrung und Schulung von Beschäftigen zur Verschwiegenheit und zum Datenschutz, den Umgang mit Datenlecks, die ergriffenen Sicherheitsmaßnahmen im Betrieb, die Verträge über Auftragsdatenverarbeitung, die Einwilligungserklärungen und eventuelle Datenschutz-Folgenabschätzungen.