EU-DATENSCHUTZ-GRUNDVERORDNUNG

FAKTENCHECK: DS-GVO

Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung (DS-GVO) in Kraft und überlagert das bisherige nationale Datenschutzrecht. Da Apotheken mit sensiblen Daten arbeiten und künftig empfindliche Strafen verhängt werden können, sollten sich Inhaber rechtzeitig auf die neuen Regeln einstellen. Was ändert sich für die Apotheken? Der Faktencheck!

Wer ist verantwortlich?

Die Verantwortung liegt immer beim Apothekenleiter. Ihm obliegt die Einhaltung des Datenschutzes und er muss bei Verstößen mit Sanktionen rechnen. Der Apothekenleiter muss den Datenschutzbeauftragten bestellen, er kann diese Aufgabe nicht selbst übernehmen, dennoch bleibt Datenschutz Chefsache.

Wer braucht einen Datenschutzbeauftragten?

In der Apotheke besteht per se eine Bestellpflicht für einen Datenschutzbeauftragten, da sensible und gesundheitsbezogene Daten erhoben, gespeichert, verarbeitet und vernichtet werden. Das Gesetz sieht schon heute einen Datenschutzbeauftragten ab zehn Personen vor. Dabei wird der Filialverbund als Ganzes betrachtet, so ist für alle Apotheken nur ein Verantwortlicher zu bestellen. Dieser muss bei der zuständigen Behörde gemeldet werden. Ob Apotheken mit weniger als zehn Mitarbeitern künftig auch einen Datenschutzbeauftragten benötigen, wird je nach Bundesland unterschiedlich bewertet. Am besten fragen Apothekenleiter bei ihrer zuständigen Landesdatenschutzbehörde nach. Wer keinen Datenschutzbeauftragten bestellen will, sollte sich dazu eine schriftliche Genehmigung einholen.

Wer darf Datenschutzbeauftragter sein?

Der Inhaber kann nicht selbst Datenschutzbeauftragter sein, auch Hilfspersonal scheidet für diese Funktion aus. Hintergrund ist eine mögliche Interessenkollision. Der Datenschutzbeauftragte darf sowohl intern als auch extern bestellt werden, wobei besonders preiswerte Pauschalangebote kritisch hinterfragt werden sollte. Angestellte des Betriebs haben den Vorteil, vor Ort zu sein und sich mit den Vorgängen in der Apotheke auszukennen. Denn Datenschutz ist eine kontinuierliche Aufgabe. Der Mitarbeiter hat einen persönlichen Vorteil: Er genießt als Person mit vollstem Vertrauen einen Kündigungsschutz von einem Jahr. Gleichzeitig ist es für den Inhaber sinnvoll, für Kontinuität zu sorgen, um nicht immer wieder einen Mitarbeiter entsprechend schulen zu müssen. Viele Apotheker wählen aus diesem Grund Vertraute wie Familienangehörige oder Lebens- und Ehepartner als Datenschutzbeauftragten.

EU-DATENSCHUTZ-GRUNDVERORDNUNG

Datenschutzbeauftragter darf werden, wer über das notwendige Fachwissen auf dem Gebiet des Datenschutzrechts verfügt. Genaue gesetzliche Vorgaben zur Aneignung des Fachwissens gibt es jedoch nicht.

Welche Aufgaben hat der Datenschutzbeauftragte?

Der Datenschutzbeauftragte ist intern wie extern Anlaufstelle für alle Fragen rund um den Datenschutz. Er muss mit den Aufsichtsbehörden kooperieren und die Einhaltung der Vorgaben überwachen. Er muss ein Verfahrensverzeichnis – einen Überblick über alle Datenverarbeitungsprozesse in der Apotheke – führen. Verfahrensverzeichnisse dienen der Einhaltung der DS-GVO und sollen detaillierte Angaben zu den einzelnen Datenverarbeitungsvorgängen wie Zweck, Betroffener, Empfänger, Sicherheitsvorkehrungen und Speicherfristen enthalten. Auch die Überwachung der Einhaltung des Datenschutzkonzeptes gehört zu seinen Aufgaben.

Was ist ein Datenschutzkonzept?

Der Datenschutzbeauftragte muss für die Apotheke ein Datenschutzkonzept erarbeiten. Mitarbeiter sollen so über die eigenen Standards informiert werden. Zudem gilt das Konzept als Rechtfertigung gegenüber den Aufsichtsbehörden. Zum Inhalt zählt auch der Umgang mit Datenpannen, denn diese müssen innerhalb von 72 Stunden angezeigt werden. Außerdem soll das dauerhafte Training der Mitarbeiter dokumentiert werden, denn dies soll nachweisbar und regelmäßig stattfinden.

Was ist mit alten Kundenkarten?

Alte Kundenkarten haben grundsätzlich Bestandsschutz, aber nur, wenn sie schon bisher den Bedingungen der DS-GVO genügen. Also in den Bereichen, für die die Kunden ihre Einwilligung per Unterschrift bestätigt haben. Jedoch dürfen ab dem 25. Mai die Daten für eine Verarbeitung darüber hinaus nicht verwendet werden. Apotheker müssen also prüfen, ob alle relevanten Vorgänge mit den alten Einwilligungserklärungen abgedeckt werden. Wenn nicht, müssen diese angepasst werden und der Kunde aktiv – per Unterschrift – seine ausdrückliche Einwilligung bestätigen. Kunden müssen wissen, welche Daten verarbeitet werden und wohin diese weitergeleitet werden. Kundenkarten, die seit 1,5 Jahren ungenutzt sind, sollen gelöscht werden. Für „temporäre Kunden“, die lediglich ein Arzneimittel erwerben, ist zu diesem Zweck keine Einwilligungserklärung erforderlich.

Wie lange dürfen Daten gespeichert/aufbewahrt werden?

Der Zeitraum der Speicherung muss dem Erhebungszweck entsprechen. So sind Daten zu Betäubungsmitteln drei Jahre, im Rahmen des Transfusionsgesetzes 30 Jahre und Rechnungen zehn Jahre aufzubewahren. Kundendaten zum Ausdruck einer Übersicht für das Finanzamt oder die Krankenkasse oder der Medikationsplan sind mit dem Wissen des Ablebens sofort zu löschen.

EU-DATENSCHUTZ-GRUNDVERORDNUNG

Besteht eine Informationspflicht und wie komme ich ihr nach?

Apotheken unterliegen bei Datenerhebung Informationspflichten. Dazu zählen unter anderem die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, der Zweck und die Rechtsgrundlage der Verarbeitung, Empfänger und Speicherdauer sowie Widerrufsrecht und Beschwerderecht. Apotheken können der Informationspflicht sowohl online – auf der eigenen Website –, als auch offline – durch einen Aushang in der Apotheke – nachgekommen. Realitätsfern scheint jedoch ein Hinweis bei einem Telefonat. Jedoch kann im Nachhinein ein Hinweis beim Besuch in der Apotheke oder auf dem Kassenbon erfolgen. Auch ist es möglich, im Gespräch auf die Grundsätze der Datenverarbeitung auf der Website hinzuweisen.

Welche Maßnahmen gehören zum Offline-Datenschutz?

Datenschutz beginnt offline – auch hier sollte mit Arbeitsanweisungen gearbeitet werden. Diese sollten unter anderem den Diskretionsabstand, den Umgang mit nicht mitgenommenen Kassenbons, den Sichtfeldern der Bildschirme und den Botendienst betreffen.

Was muss in der Zusammenarbeit mit externen Dienstleistern beachtet werden?

Die Weitergabe von Daten an den Steuerberater bedarf keiner vertraglichen Regelung, da dieser zu den Berufsgeheimnisträgern zählt. Mit allen anderen externen Dienstleistern wie Rechen- und Blisterzentren sowie Herstellerbetrieben müssen Auftragsdatenverarbeitungsverträge geschlossen und der Vertragspartner zur Vertraulichkeit verpflichtet werden. Dies gilt auch für Softwarehäuser, wenn diese sich per Fernwartung in die Apothekensoftware einloggen können. Wer keine Verschwiegenheitserklärung (Kettenverpflichtung) mit den Externen abschließt, muss mit Sanktionen rechnen.

Wer kontrolliert die Umsetzung?

Zuständig sind die Datenschutzbehörden der Länder. Apotheken müssen den Mitarbeitern der Behörde auf Anweisung alle erforderlichen Informationen bereitstellen und den Zugang zu den Geschäftsräumen und den datenverarbeitenden Geräten gewähren.

Welche Strafen sind möglich?

Es können je nach Verstoß Bußgelder von bis zu 2 Prozent des Jahresumsatzes, 10 Millionen Euro oder bei schweren Verstößen bis zu 4 Prozent des Jahresumsatzes oder bis zu 20 Millionen Euro verhängt werden. In die Verantwortung wird immer der Apothekenleiter gezogen nicht der Datenschutzbeauftragte.

Darf ich noch WhatsApp für Kundenbestellungen nutzen?

Von einer Bestellung per WhatsApp ist abzuraten. Das Problem: Der Sitz der WhatsApp Inc. befindet sich in einem unsicheren Drittland – außerhalb der EU – und trotz

EU-DATENSCHUTZ-GRUNDVERORDNUNG

Ende-zu-Ende-Verschlüsselung findet ein Datentransfer in die USA statt. So wird beispielsweise das Rezeptfoto übermittelt. Wer jetzt denkt, der Kunde sei in der Haftung, liegt falsch. Auch wenn der Patient den Kontakt zur Apotheke aufnimmt, hat der Apothekeninhaber die volle Verantwortung, sofern er den Service selbst anbietet.

Darf ich ein gefälschtes Rezept der Polizei vorlegen?

Die Antwortet lautet Ja, denn hier geht es um die Aufklärung eines strafrechtlichen Tatbestandes. Somit ist eine Freigabe der mutmaßlichen Fälschung erlaubt.

Was muss ich noch beachten?

Wer Leasingverträge für Geräte mit einer Schnittstelle hat, sollte klären, was mit den gespeicherten sensiblen Daten geschieht. So sollte geklärt werden, wann die Daten von den integrierten Speichern gelöscht werden und was damit nach Ablauf der Leasingverträge geschieht.