Auftragsverarbeitung: Zusammenarbeit mit Dienstleistern (Stand 05.04.2018)

Die Praxissoftware wird gewartet, Akten- und Datenträger müssen nach Ablauf der Aufbewahrungsfrist vernichtet werden. Immer dann, wenn ein externer Dienstleister auf Patienten- oder Mitarbeiterdaten zugreifen kann, ist der Abschluss eines Vertrages zur Auftragsverarbeitung (als Anlage zum Hauptvertrag) erforderlich.
Die Auftraggeber müssen sich ferner davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Die Firmen sollen dem Auftragsnehmer dazu ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen.

Auftragsverarbeitung: ja oder nein?

Eine Auftragsverarbeitung liegt nicht nur bei der Wartung der Praxis-EDV oder der Akten- und Datenträgervernichtung vor. Weitere Beispiele sind die Nutzung von Cloud-Systemen und die Terminvergabe durch Externe (die Terminservicestellen der KVen fallen nicht darunter).
Dagegen ist eine rein technische Wartung der IT-Infrastruktur durch einen Externen, zum Beispiel Arbeiten an der Stromzufuhr, Kühlung oder Heizung, keine Auftragsverarbeitung.
Dies gilt ebenso bei der Beauftragung von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und Angehörigen anderer Berufe, die als „Geheimnisträger“ gelten. Auch hier liegt in der Regel keine Auftragsverarbeitung vor.

Das ist zu tun

Schritt 1: Schauen Sie zunächst, ob Sie für Ihre Dienstleistungsverträge (z.B. zur Wartung der Praxis-EDV) jeweils einen Vertrag zur Auftragsverarbeitung haben, und passen Sie diesen in Abstimmung mit dem Auftragnehmer gegebenenfalls an.

Schritt 2: Ist das nicht der Fall, sprechen Sie Ihren Dienstleister an. Er benötigt einen Vertrag zur Auftragsverarbeitung und wird Ihnen in der Regel einen Entwurf zusenden.

Folgende Inhalte sollte der Vertrag enthalten:

- Gegenstand und Dauer der Verarbeitung (um welche Leistung handelt es sich, wie lange wird diese beauftragt)
- Art und Zweck der Verarbeitung (wozu dient sie, welches Ziel soll erreicht werden)
- Art der personenbezogenen Daten und Kategorien betroffener Personen (z.B. Zugriff auf Gesundheitsdaten)
- Rechte und Pflichten des Auftraggebers sowie dessen Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung berechtigten Personen zur Vertraulichkeit
- Benennung der technischen und organisatorischen Maßnahmen, die das Unternehmen zum Schutz personenbezogener Daten durchführt (z.B. Einhaltung von Vorgaben der ISO/IEC 27001)
- Verpflichtung des Auftragnehmers zur Unterstützung des Auftraggebers bei:
- Anfragen und Ansprüchen Betroffener im Zusammenhang mit der Auftragsverarbeitung
- der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung
- Verpflichtung des Auftragnehmers, dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Pflichten bereitzustellen. Möglich ist auch eine Überprüfung oder Inspektion durch einen vereinbarten Prüfer.

Schritt 3: Lassen Sie sich vom Dienstleister ein geeignetes Zertifikat, zum Beispiel ISO/IEC 27001, vorlegen. Das Zertifikat dient dem Nachweis der eingesetzten technischen und organisatorischen Maßnahmen zum Schutz der Daten beim Auftragnehmer. Eine weitergehende Pflicht zur Kontrolle durch Sie besteht nicht.

-Information der KBV vom 5. April 2018-