# 7. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO ist für jede Form der Datenverarbeitung durchzuführen, wenn z.B. aufgrund des Umfangs und des Zwecks der Datenverarbeitung ein hohes Datenschutzrisiko besteht oder eine systematische Videoüberwachung der Praxisräume vorgenommen wird.

Nach Art. 35 Abs. 7 DSGVO hat die DSFA mindestens folgende Punkte zu enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DSGVO und
- 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.

Sofern eine Datenschutz-Folgenabschätzung erforderlich ist, muss ein Datenschutzbeauftragter benannt werden, auch wenn in der Praxis weniger als zehn Mitarbeiter tätig sind.

Wird eine erforderliche Datenschutz-Folgenabschätzung nicht durchgeführt, kann dies eine Geldbuße von bis zu 10 Mio. € oder bis zu 2 % des weltweit erzielten Gesamtjahresumsatzes zur Folge haben. Wird eine Geldbuße erhoben, ist der höhere der beiden Bußbeträge anzusetzen.

Ein ausführliches Informationsblatt zur Datenschutz-Folgenabschätzung ist folgendem Link zu entnehmen:

https://www.aekno.de/downloads/aekno/Infoblatt-Datenschutzfolgeabschaetzung-Stand-15.05.18.pdf

# 8. Auftragsdatenverarbeitung

Geben Ärzte die Verwaltung Ihrer Daten an externe Dritten weiter, gelten für diese die Regeln der Datenschutzverordnung und des neuen BDSG (Art. 28 DSGVO). **Auftragsdatenverarbeitung** liegt vor, wenn sich der Verantwortliche in der Praxis zur Verarbeitung von Daten eines externen Dritten bedient und diesem Weisungen erteilt.

**Tipp!**

Der Auftragsbearbeiter und der Arzt sollten ein gemeinsames Sicherheitskonzept erarbeiten und einen schriftlichen Vertrag schließen.

**Beispiele:**

- Externe Abrechnungskraft, die in der Praxis die Abrechnung erstellt.
- Beauftragung eines externen Labors, bei der die Patientendaten an das Labor übermittelt werden.

Die **Mindestinhalte des zwischen dem Praxisinhaber und den Auftragsdatenverarbeitern abzuschließenden Vertrags** regelt Art. 28 Abs. 3 DSGVO. Der Vertrag sieht insbesondere vor, dass der Auftragsverarbeiter:

- die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen ergreift;
- die in Art. 28 Abs. 2 und 4 DSGVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
- angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen;

- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützt;
- nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Wegen einer Musters Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO s. Kap. 12.7.

# 9. IT-Sicherheitsmaßnahmen

## 9.1 Kennwörter

Die in der Praxis eingesetzten Programme sind durch Kennwörter zu schützen. Die Kennwörter sollten nicht kurz (8 oder mehr Zeichen) und nicht leicht zu erraten sein, also keine Namen oder Geburtsdaten enthalten. Außerdem ist ein Sonderzeichen z.B. #, + und ein Wechsel von Groß- und Kleinbuchstaben empfehlenswert. Kennwörter sind in kürzeren Abständen zu ändern. Für Mitarbeiter, die nicht mehr in der Praxis arbeiten, sind deren Kennwörter zu löschen bzw. zu ändern.

Wird mehrmals ein falsches Passwort eingegeben, dann sollte der Zugriff automatisch gesperrt werden.

Außerdem können Zugriffsrechte des Mitarbeiters auf die zu nutzenden Daten eingeschränkt werden.

Wird ein Praxisverwaltungssystem genutzt, ist sicherzustellen, dass dort keine versteckten Kennwörter zur Wartung enthalten sind.

## 9.2 Virenschutz-Software

Die Praxis hat dringend ein Virenschutzprogramm zu verwenden, das mittels automatischen Updates aktuell gehalten wird.

## 9.3 Öffnen von Dateianhängen

Per Mail übermittelte Text-, Bild- oder Datendateien dürfen nicht ohne vorherige Prüfung des Absenders und der Echtheit der Daten geöffnet werden, da durch Schadprogramme, die Schwachstellen von Anwendungsprogrammen oder des Betriebssystems ausnutzen, Viren oder Trojaner in die EDV gelangen können.

## 9.4 Datensicherung

Die Daten der Praxis sind regelmäßig zu sichern. Dabei sind die Aufbewahrungsfristen zu berücksichtigen und es sind Maßnahmen zu ergreifen, die einen Datenverlust unmöglich machen.

Auch Geschehnisse wie Einbruch bzw. Diebstahl der Praxis-EDV sowie andere Risiken wie Hochwasser oder ein Brand können zu Datenverlust führen.

Die Praxisdaten sind regelmäßig – idealerweise täglich – auf mindestens 2 verschiedenen transportablen oder externen Speichermedien (z.B. externe Festplatten, USB-Sticks, Online-Speicherung im Internet) in automatisierter Form zu sichern und an einem sicheren Ort aufzubewahren.

Für die Sicherung der Daten sollte eine konkrete Person und ein Vertreter zuständig sein.

## 9.5 Fernwartung

Wird das Praxisverwaltungssystem mittels Fernwartung gepflegt, sind folgende Punkte zu beachten:

- Die Fernwartung muss vom Praxisrechner aus gestartet werden.
- Der Rechner darf während der Dauer der Fernwartung, nicht ausschließlich allein demjenigen überlassen werden, der die Wartungsarbeiten durchführt.
- Ist die Fernwartung fertig, so muss die EDV vom Internet getrennt werden.
- Bei der Verwendung personenbezogener Daten, sind bei Auftragsvergabe an ein Unternehmen, das Fernwartung anbietet, die Voraussetzungen des Art. 9 Abs. 1 DSGVO i.V.m. § 22 Abs. 2 BDSG zu beachten und eine Verschwiegenheitserklärung einzuholen.
- Der Umfang und der Zeitpunkt der Wartung ist unter Angabe des Namens des Servicetechnikers zu dokumentieren.

## 9.6 Weitergabe von Datenträgern an fremde Dritte

Werden Datenträger an fremde Dritte weitergegeben, sind die Daten zu verschlüsseln. Der Datenempfänger erhält den verwendeten Schlüssel auf andere Weise mitgeteilt und hat sich schriftlich zur Geheimhaltung und Verschwiegenheit im Umgang mit den Daten zu verpflichten.

## 9.7 Unerwünschter Zugriff Dritter auf Daten der Praxis

EDV-Geräte wie Bildschirm, Tastatur, Maus, Kartenlesegerät, Drucker und Rechner sowie die Speichermedien sind so zu platzieren, dass ein unerwünschter Zugriff Dritter auf Daten der Praxis nicht möglich ist.

Verlassen Mitarbeiter Ihren Arbeitsplatz, ist der Computer automatisch per Kennwortschutz zu sperren.