Great Oak
Datenschutz
GmbH & Co. KG

Sehr geehrte Damen und Herren,

mit diesem Fragebogen und der anschließenden Auswertung durch uns haben Sie die Möglichkeit, den Ist-Zustand des Datenschutzes in Ihrer Praxis mit dem gesetzlich geforderten Soll-Zustand abzugleichen und so eine Entscheidungsgrundlage für zukünftige Investitionen in den Schutz personenbezogener Daten zu bekommen. Die Kosten für die Auswertung betragen pauschal 50 Euro netto pro Fragebogen. Es geht hierbei nicht um das maximal Mögliche an Datenschutz, sondern lediglich um die Erfüllung des gesetzlich Notwendigen. Hierbei nehmen wir hauptsächlich Bezug auf das aktuelle Bundesdatenschutzgesetz und die EU-Datenschutzgrundverordnung.

Bitte füllen Sie das Dokument so vollständig wie möglich aus und schicken es uns per Fax an 02985 99 99 693 oder per E-Mail an info@great-oak.de. Der verschlüsselte Versand per PGP ist mit dem Key, den Sie auf great-oak-datenschutz.de im Impressum finden, möglich.

1. Grundlegendes

Bitte geben Sie Ihre vollständigen Praxisnamen, Praxisadresse sowie einen Ansprechpartner und dessen Kontaktdaten an.

Wie viele Mitarbeiter sind in Ihrer Praxis tätig?
Hierzu zählen auch Partner, Aushilfen, Hausmeister, Reinigungspersonal etc.

Haben alle Mitarbeiter eine Verpflichtung auf das Datengeheimnis nach §5 BDSG unterschrieben?
Auf den Paragraphen und dessen Inhalt muss in der Verpflichtung explizit hingewiesen werden.

Haben Sie für Ihre Praxissoftware eine Vorabkontrolle durch einen Datenschutzbeauftragten durchführen lassen?
Eine Vorabkontrolle ist eine schriftliche Bewertung der Risiken für die Rechte der Betroffenen der Datenverarbeitung.

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

Haben Sie Folgeabschätzungen für Datenverarbeitungen mit Patientendaten durchgeführt?
Eine Folgeabschätzung ist eine schriftliche Bewertung der Risiken für die Rechte der Betroffenen der Datenverarbeitung und eine Darlegung, wie diese Risiken minimiert werden.

Haben Sie für jede Datenerhebung bei Patienten, die auf freiwilligen Angaben beruht, eine schriftliche Einwilligung vorliegen?
Z.B. für E-Mail-Adressen, Telefon- und Handynummern, Angehörigenkontakte, Vorgeschichte, Anamnesebögen usw.

Haben Sie die Einwilligungstexte innerhalb des letzten Jahres an die EU-Datenschutzgrundverordnung angepasst?

2. Organisatorisches

Führen Sie ein vollständiges und aktuelles Verfahrensverzeichnis aller dauerhaften Datenverarbeitungen?
Verfahren sind z.B. Bewerbungen, Lohnabrechnung, Med. Dokumentation, Abrechnung GOÄ usw.

Gibt es eine Datenschutzrichtlinie?
In einer Datenschutzrichtlinie werden Handlungsweisungen und Ge- und Verbote rund um das Thema Datenschutz festgelegt.

Wie oft wird die Datenschutzrichtlinie aktualisiert?

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

Wie wird der Nachweis der Einhaltung der Datenschutzrichtlinie geführt?

Auf welche Weise klären Sie die Patienten und Mitarbeiter über die Verarbeitung Ihrer Daten auf?
Bitte eine kurze Beschreibung des Umfangs und der Art und Weise

Wie lautet die Adresse Ihrer Datenschutzerklärung auf Ihrer Webseite?

Hat jeder Mitarbeiter einen eigenen Anmeldenamen und ein nur ihm persönlich bekanntes Passwort in der Praxissoftware?

Sind die Benutzerrechte in der Praxissoftware so gestaltet, dass jeder nur das absolut notwendige sieht oder kann jeder Mitarbeiter die vollständige Patientenakte sehen?

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

Haben Sie Auftragsdatenverarbeitungsverträge mit Ihren Dienstleistern abgeschlossen?

Diese Verträge sind speziell als solche nach §11 BDSG gekennzeichnet und sollten mit allen IT-Dienstleistern und allen Dienstleistern, die Patientendaten von Ihnen bekommen, abgeschlossen worden sein.

Wie oft führen Sie Überprüfungen Ihrer Datenverarbeitungen hinsichtlich des Datenschutzes durch?

Hierbei ist sowohl die Überprüfung der rechtlichen Zulässigkeit als auch die Überprüfung des angemessenen Schutzes gemeint.

Gibt es einen Reaktionsplan für Datenschutzverletzungen? Wenn ja, in welchem Umfang?

Wie werden die Betroffenenrechte sichergestellt?

Jeder von einer Datenverarbeitung Betroffene hat datenschutzrechtliche Grundrechte, deren Sicherstellung schriftlich nachgewiesen werden muss.

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

3. Technisches

Gibt es eine IT-Sicherheitsrichtlinie?

In einer IT-Sicherheitsrichtlinie werden die technischen Schutzmaßnahmen festgelegt. Beispielsweise welche Hard- und Software zum Einsatz kommen darf, wie ein WLAN aufgebaut sein muss, aber auch Zugriffsrechte auf DV-Systeme.

Wie oft wird die IT-Sicherheitsrichtlinie aktualisiert?

Wie wird der Nachweis der Einhaltung der IT-Sicherheitsrichtlinie geführt?

Sind die Festplatten Ihrer Server und PCs verschlüsselt? Wenn ja, mit welchem Standard?

Haben Sie ein IT-Sicherheitsmanagementsystem (ISMS) im Einsatz?

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

Falls Sie kein IT-Sicherheitsmanagementsystem im Einsatz haben, wie dokumentieren Sie Ihre IT-Infrastruktur und Änderungen an derselben?

Falls Sie kein IT-Sicherheitsmanagementsystem im Einsatz haben, wie bewerten Sie die Wirksamkeit Ihrer Schutzmaßnahmen?

Führen Sie einmal jährlich oder öfter eine Überprüfung Ihrer IT-Infrastruktur hinsichtlich der Wirksamkeit Ihrer Datensicherheitsmaßnahmen durch?

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

In welcher Weise werten Sie die Ergebnisse der Überprüfung Ihrer IT-Infrastruktur aus?

Wie oft führen Sie ein Backup Ihrer Datenbestände durch und wo werden diese gelagert?
Bitte zur Lagerung nur Angaben wie „im Safe“ oder „im Schrank im Büro“ angeben.

Wie entsorgen Sie Ihren Papiermüll?
Bitte mit Angabe der Entsorgungsstufe nach DIN 33699 (Steht meist auf dem Entsorgungszertifikat oder hinten auf dem Schredder)

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de

4. Aus- und Fortbildung

Haben Ihre Mitarbeiter eine Grundlagenschulung im Umgang mit personenbezogenen Daten und die für sie geltenden gesetzlichen Pflichten erhalten?

Wie oft werden findet eine Auffrischungsschulung über das Thema Datenschutz statt?

Wie führen Sie neben den Schulungen gezielte Sensibilisierungsmaßnahmen zu einzelnen Datenschutzthemen durch?
Beispiele hierfür sind Gespräche, Rollenspiele, Informationstexte usw.

Wie oft nimmt im Durchschnitt jeder Mitarbeiter an einer solchen Sensibilisierungsmaßnahme teil?

Vielen Dank für Ihre Teilnahme.

Great Oak Datenschutz GmbH & Co. KG. – Ruhrstraße 18 – 59955 Winterberg
Tel. 02985 / 99 99 69 0 – Fax 02985 / 99 99 69 3 – E-Mail info@great-oak.de