Checkliste Datenschutz in der Praxis

Dies soll nur zur Orientierung und Hilfestellung dienen. Die Liste soll helfen die notwendigen Maßnahmen der DS-GVO zu ergreifen, aber mehr noch. Es soll das Bewusstsein für den Datenschutz geschärft werden. Eine Rechtsverbindlichkeit wird vom Autor ausdrücklich verweigert.

Die Maßnahmen sind entsprechend den Vorgaben der DS-GVO zu dokumentieren. Alle Verfahrensanweisungen / Arbeitsanweisungen / Formulare / Protokolle u.ä. sollen idealerweise im QM System hinterlegt und regelmäßig kontrolliert werden (z.B. Verfahrensanweisung Datensicherung, Unterweisungen Datenschutz usw.)

Zunächst erfolgt die Bewertung, ob ein Vorgang notwendig oder relevant ist. Danach erfolgt die Bearbeitung. Obligate Vorgänge sind bereits als notwendig markiert. Natürlich können noch mehr Vorgänge auftauchen, die hier noch nicht aufgelistet sind. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

	Notwendig	**Erfüllt**
Verzeichnis von Verarbeitungstätigkeiten **Siehe 1**	✓	O
Verzeichnis technischer und organisatorischer Maßnahmen zum Schutz von patientenbezogenen Daten **Siehe 2**	✓	O
Bereitstellung von Patienteninformation zum Datenschutz in der Praxis, zum Beispiel als Aushang, aber auch als Flyer zur Mitgabe. Bereitstellung auf der Homepage **Siehe 3**	✓	O
Auftragsdatenverarbeitung mit externen Anbietern **Siehe 4**	✓	O
Bestellung eines Datenschutzbeauftragten **Siehe 5**	O	O
Datenschutzfolgeabschätzung **Siehe 6**	O	O
	O	O
	O	O

1 Verarbeitungstätigkeiten	**Notwendig**	**Erfüllt**
Einsatz und Nutzen eines Praxisverwaltungssystems	✓	O
Führen von Personalakten. Lohnbuchhaltung	✓	O
	O	O

	O	O

Zur Dokumentation sind Vorlagen der KBV sinnvoll www.kbv.de/datenschutz

2 Technische und organisatorische Maßnahmen zum Schutz von patientenbezogenen Daten	**Notwendig**	**Erfüllt**
Empfang		
Gibt es eine Zutrittskontrolle?	O	O
Ist die ununterbrochene Besetzung des Empfangs während der Öffnungszeiten gewährleistet?	O	O
Kann kein Unbefugter auf PCs & Co. zugreifen?	O	O
Sind Bildschirme, Fax, Telefone & Co. vor dem Einblick Dritter geschützt?	O	O
Sind die Patientenakten vor unbefugtem Zugriff abgesichert? (abschließbare Schränke)	O	O
Werden die Schränke außerhalb der Öffnungszeiten abgeschlossen?	O	O
Ist ein Diskretionsbereich eingerichtet?	O	O
Haben die Patienten die Möglichkeit ein diskretes Gespräch mit den Angestellten zu führen? Werden sie darauf hingewiesen?	O	O
Werden die Anmelde- und Patientendaten des Betroffenen diskret erhoben?	O	O
Werden die Patienten auf die Freiwilligkeit des Ausfüllens eines Anamneseformulars hingewiesen?	O	O
Ist das Wartezimmer so abgetrennt, dass Dritte keine Gespräche am Empfang oder in den Behandlungsräumen mithören können?	O	O
Werden Telefonate so geführt, dass Dritte keine Information über die Person am anderen Ende der Leitung erlangt?	O	O
Werden die Fristen für die Aufbewahrung und Vernichtung von Gesundheitsdaten eingehalten?	O	O
Erfolgt die Aktenvernichtung DIN konform?	O	O
Ist die Arztpraxis gegen Diebstahl und Einbruch angemessen abgesichert?	O	O
	O	O
	O	O
	O	O

Behandlungsräume		
Sind Patienten niemals allein in einem Behandlungsraum?	O	O
Ist sichergestellt, dass unter Abwesenheit des Arztes / MFAs keine Fremdinformationen durch den Patienten eingesehen werden können?	O	O
Werden Patientenproben sofort beschriftet, damit eine Verwechslung nicht möglich ist?	O	O
	O	O
	O	O
Datensicherheit und -verwaltung		
Sind die Datenverarbeitungssysteme physisch geschützt? (z.B. Beschränkung des Zugangs zum Server)	O	O
Ist der Zugriff auf elektronische Arbeitsplätze durch ausreichend sichere Passwörter beschränkt?	O	O
Werden die Passwörter regelmäßig gewechselt?	O	O
Sind unbeaufsichtigte PCs stets gesperrt (inkl. Passwortschutz)?	O	O
Ist nur dem betreffenden Mitarbeiter das Passwort für den jeweiligen EDV – Arbeitsplatz bekannt?	O	O
Ist die Einsicht jedes einzelnen Mitarbeiters in die Daten an deren jeweilige Berechtigung zur Einsicht angepasst?	O	O
Kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden?	O	O
Gibt es eine ausreichend gesicherte Internetverbindung?	O	O
Gibt es Anweisungen zum Umgang mit E-Mails und Internetnutzung?	O	O
Werden die notwendigen Updates regelmäßig eingespielt? Wird der Vorgang dokumentiert?	O	O
Werden regelmäßig Sicherungen der Daten erstellt? (Backup) Ist der Vorgang dokumentiert?	O	O
Gibt es einen Plan zur Wiederherstellung der Arbeitsplätze bei Systemausfall? (Desaster Recovery) Ist der Vorgang dokumentiert?	O	O
Ist eine verschlüsselte und/oder sichere Übertragung von Daten (auch physischen) gewährleistet?	O	O
Sind Virenschutzprogramme und ggf. auch Firewalls installiert und auf dem aktuellsten Stand?	O	O

Werden nicht mehr benötigte Patientenakten, Informationen und Datenträger gemäß Datenschutzbestimmungen korrekt entsorgt?	O	O
Wird eine Online Terminvereinbarung genutzt? Wenn ja wer betreibt diese? Besteht bei externen Betreibern ein Vertrag zur Auftragsdatenverarbeitung?	O	O
Ist eine Homepage eingerichtet? Besteht eine Verschlüsselung? (HTTPS) Ist eine Datenschutzerklärung vorhanden?	O	O
Ist eine Facebook Fanpage eingerichtet? Ist eine Datenschutzerklärung vorhanden?	O	O
	O	O
	O	O
Mitarbeiter		
Sind alle Angestellten auf das Datengeheimnis verpflichtet worden?	O	O
Wurden Sie darüber hinaus auch auf die besondere Verschwiegenheitspflicht hingewiesen und entsprechend belehrt?	O	O
Werden externe Personen (Auditoren, Probearbeit vor Einstellung u.ä.) auf die Verschwiegenheitspflicht hingewiesen und bestätigen sie das schriftlich?	O	O
	O	O
	O	O
Rechte der Betroffenen		
Werden Patientendaten an den Hausarzt nur mit schriftlicher Einwilligung des Patienten übermittelt?	O	O
Werden Patientenauskünfte an Dritte zunächst an den Patienten weitergeleitet, bevor sie (nach Einwilligung des Patienten) von der Praxis herausgegeben werden?	O	O
Ist in der Praxis ein Ablauf definiert, wie mit datenschutzrechtlichen Anfragen von Betroffenen (Patienten) umgegangen wird?	O	O
Erfolgt eine Abrechnung über private Versicherungen oder privatärztliche Verrechnungsstellen ausschließlich nach ausdrücklicher Einwilligung des Patienten?	O	O
Werden die Ansprüche der Patienten aus dem Patientenrechtegesetz (Anspruch auf Kopie der Patientenakte, Zurverfügungstellung der im Rahmen der Patientenaufklärung oder -einwilligung unterzeichnete Unterlagen) umgesetzt?	O	O
Werden entsprechend dem Patientenrechtegesetz unterschriebene Aufklärungsbögen dem Patienten mitgegeben?	O	O

Sind bei Einwilligungserklärungen (z.B. PVS Abrechnungstelle) Hinweise auf die Möglichkeit des Widerrufes enthalten?	O	O
Wird bei Übersendung von Patientendaten per Fax oder Email sichergestellt, dass nur der Patient oder Berechtigte Empfänger der Daten sind?	O	O
Werden Nachrichten über Facebook versendet und empfangen? Werden die Patienten hingewiesen, dass es sich nicht um eine sichere Verbindung handelt?	O	O
Werden Nachrichten über Whats App versendet und empfangen? Werden die Patienten hingewiesen, dass es sich nicht um eine sichere Verbindung handelt?	O	O
Haben die Patienten die Möglichkeit verschlüsselte E-Mails zu senden? (z.B. PGP)	O	O
	O	O
	O	O

3 Patienteninformationen zum Datenschutz	**Notwendig**	**Erfüllt**
Existiert eine Patienteninformation zum Thema Datenschutz	✓	O
Ist diese Information als Aushang in der Praxis vorhanden?	O	O
Können Patienten diese Information auf Anfrage erhalten?	O	O
Sind die Homepage und ggf. Facebook Seite mit den entsprechenden Angaben versehen?	O	O
Ist die Information auch fremdsprachig vorhanden?	O	O
	O	O
	O	O

4 Auftragsdatenverarbeitung	**Notwendig**	**Erfüllt**
Werden Daten von Mitarbeitern extern bearbeitet?	O	O
Werden EDV Wartung mittels Fernwartung durchgeführt?	O	O
Muss ein Mitarbeiter die Fernwartung aktiv beginnen?	O	O
Ist während der Fernwartung ein Mitarbeiter am Monitor und kann ggf. eingreifen?	O	O

Wird der Vorgang protokolliert?	O	O
Existieren Verträge mit den Anbietern?	O	O
	O	O
	O	O

5 Datenschutzbeauftragter	**Notwendig**	**Erfüllt**
Sind mehr wie 10 Mitarbeiter regelmäßig mit der automatisierten Verarbeitung von Personendaten beschäftigt?	O	O
Besteht ein MVZ oder eine BAG?	O	O
Ist der Datenschutzbeauftragte der Aufsichtsbehörde namentlich gemeldet?	O	O
	O	O
	O	O

Stand 30.03.2018: Eine Einzelpraxis benötigt keinen Datenschutzbeauftragten.

6 Datenschutzfolgeabschätzung	**Notwendig**	**Erfüllt**
Werden überdurchschnittlich viele Personendaten verarbeitet?	O	O
Werden die Praxisräume systematisch videoüberwacht?	O	O
	O	O
	O	O

Stand 30.03.2018: Was eine überdurchschnittliche Verarbeitung von Personendaten ist, wurde bis dato nicht definiert.