info@ehealth-zentrum.de
www.ehealth-zentrum.de

Checkliste: Wie passe ich die Prozesse in meiner Arztpraxis an die Anforderungen der EU-DSGVO an?

Die Gültigkeit der EU-DSGVO ab Mai 2018 wirft eigene Fragen bei Praxisinhabern auf. Die neuen Anforderungen müssen von allen EU-Mitgliedsstaaten eingehalten werden. Dabei nehmen die Gesundheitsdaten einen wichtigen Stellenwert ein, da sie zu personenbezogenen Daten zugeordnet werden, die sowohl nach dem BDSG als auch der EU-DSGVO einen hohen Schutzbedarf haben. Aufgrund der undurchsichtigen Formalitäten in Bezug auf die umfangreiche DSGVO, fehlen vielen Ärzten die ersten Schritte, die sie für die Konformität umzusetzen haben. Die nachstehende Checkliste stellt einen Überblick über die zu erforderlichen Prozessschritte der DSGVO in einer Arztpraxis dar.

Hinweis: Die Checkliste dient lediglich der Unterstützung der Umsetzung der Anforderungen der DSGVO. Für die Umsetzung dieser Anforderungen empfehlen wir ein entsprechend geschultes Personal oder die Anspruchnahme eines externen Beratungsdienstleiters wahrzunehmen. Das Kompetenzzentrum für Telemedizin und E-Health Hessen bietet eine unentgeltliche Beratung vor Ort an, sofern die Praxis sich im Bundesland Hessen befindet. Kontaktieren Sie uns diesbezüglich unter info@ehealth-zentrum.de.

6 Schritte zur Umsetzung der EU-DSGVO in Ihrer Praxis

JA	NEIN	Schritt 1: Vorbereitung
○	○	Haben Sie die Verantwortlichkeiten (Art. 4 Nr. 7 DSGVO) geregelt?
○	○	Ist das Bewusstsein über Datenschutzrisiken in Ihrer Praxis vorhanden?
○	○	Haben Sie bereits einen (internen/ externen) Datenschutzbeauftragten bestimmt? Dieser ist auf jeden Fall in folgenden Situationen nach Art. 37 Abs. 1 DSGVO/ dem BDSG-neu zu benennen: • Der Verantwortlicher (= Ihre Praxis) ist Teil einer Behörde oder öffentlichen Stelle • Die Kerntätigkeit Ihrer Praxis besteht in der Durchführung von Datenverarbeitungsvorgängen, welche aufgrund ihrer Art,

		ihres Umfangs und/ oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von Patienten erforderlich macht • Die Kerntätigkeit Ihrer Praxis besteht in der umfangreichen Verarbeitung von besonderen Kategorien von Daten gemäß Art. 9 DSGVO, worunter u.a. die Gesundheitsdaten fallen • In Ihrer Praxis sind mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt
○	○	Haben Sie Ihren Datenschutzbeauftragten gemäß Art. 30 DSGVO bei der zuständigen Aufsichtsbehörde gemeldet?
○	○	Verfügen Sie über eine interne Datenschutzrichtlinie zur Definition von klaren Verhaltensregeln im Umgang mit Patientendaten und zur Stärkung des Bewusstseins für den Datenschutz?
		Schritt 2: Übersicht von Verarbeitungstätigkeiten
○	○	Ist ein Verzeichnis mit den Verarbeitungstätigkeiten gemäß Art. 30 DSGVO angelegt worden?
○	○	Existiert eine Dokumentation des Verzeichnisses?
		Schritt 3: Regelungen des Patientenverhältnisses
○	○	Sind Ihre Texte zur Information über die Erhebung personenbezogenen Daten und Auskunftsrechte der betroffenen Personen bereits nach Art. 13 und Art. 14 DSGVO angepasst worden? • Name und Kontaktdaten des Verantwortlichen der Praxis sowie ggf. dessen Vertreter • Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten • Rechtsgrundlage, auf der die Verarbeitung personenbezogener Daten erfolgt • Das berechtigte Interesse, sofern die Datenerhebung mit Ihren berechtigten Interessen oder die eines Dritten beruht • Geplante Dauer der Speicherung. Sofern dies nicht möglich sein sollte, die Kriterien für die Festlegung dieser Speicherdauer • Hinweis auf das Wahrnehmen der Betroffenenrechte auf

		o Auskunft über die betreffenden personenbezogenen Daten (Art. 15) o Berichtigung/ Löschung/ Einschränkung der Verarbeitung (Art. 16/ 17) o Widerspruch gegen die Datenverarbeitung aufgrund besonderer Situation des Patienten (Art. 21) o Datenübertragbarkeit (Art. 20) o Beschwerde bei der Aufsichtsbehörde (Art. 77) • Recht zum jederzeitigen Widerruf einer Einwilligung, ohne dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Wiederruf erfolgten Verarbeitung berührt wird • Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist • Sofern die Datenverarbeitung eine automatische Entscheidungsfindung (einschließlich Profiling) beinhaltet: Aussagekräftige Informationen über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für den betroffenen Patienten • Sofern die Praxis vorhat, die personenbezogenen Daten in Drittländer oder internationale Organisation zu übermitteln: o Die Absicht der Praxis o Die Rechtsgrundlage, welche die Übermittlung legitimiert o Die vom Verantwortlichen zum Einsatz gebrachten geeigneten Garantien zum Schutz dieser Daten • Sofern die Daten nicht beim betroffenen Patienten erhoben worden sind (Dritterhebung): o Die Datenquelle o Ob sie aus öffentlich zugänglichen Quellen stammen o Eine allgemeine Information muss dennoch angegeben werden, auch wenn es sich um mehrere Datenquellen handelt und die Herkunft nicht mehr eindeutig zugeordnet werden kann

○	○	Geeignete Verfahren einrichten, um Auskunftsrecht-Anträge von betroffenen Patienten nach Art. 15 DSGVO zu erfüllen. Gemäß Art. 12 Abs. 1 DSGVO sind die bereitgestellten Informationen in einer präzisen, transparenten, verständlichen und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.
○	○	Haben Sie geeignete Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Patienten gemäß Art. 20 DSGVO zu erfüllen?
		Schritt 4: Bestimmung von Regelungen zwischen Aufsichtsbehörde, externen Dienstleistern und Dritten
○	○	Sind Externe zur Erledigung Ihrer Arbeiten (Auftragsverbearbeiter) eingebunden? Fall ja, sind folgende Punkte berücksichtigt worden?: • Erstellung einer Übersicht aller Auftragsverarbeiter • Mit allen Auftragsverarbeiter vertragliche Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DSGVO abschließen • Verpflichtung der Dritten zur Geheimhaltung
○	○	Wurde bereits geklärt, wer, wann und wie mit den Behörden kommuniziert wird?
		Schritt 5: Klärung von Verantwortlichkeiten und Umgang mit Risiken
○	○	Können Sie für jede Verarbeitungstätigkeit die Rechtmäßigkeit dieser Datenverarbeitung gemäß Art. 5 Abs. 2 DSGVO nachweisen, z.B. bezüglich Zweck der Verarbeitung?
○	○	Haben Sie Ihre derzeitigen Einwilligung auf die Bedingungen gemäß Art. 7 und Art. 8 DSGVO überprüft?
○	○	Dokumentieren Sie das Vorliegen der Einwilligungen bereits in geeigneter Form, damit diese später nachgewiesen werden kann?
○	○	Haben Sie Ihre aktuellen Prozesse an die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO angepasst? • Das Treffen und die Auswahl von technischen und organisatorischen Maßnahmen sollen sich auf Art. 32 Abs. 1 DSGVO stützen.

		Berücksichtigt dabei soll eine risikoorientierte Betrachtungsweise auf Basis o der Stand der Technik o der Implementierungsart o der Art/ des Umfangs/ der Umstände/ der Zwecke der Verarbeitung o der unterschiedlichen Eintrittswahrscheinlichkeit o der Schwere des Risikos für die Rechte und Freiheiten
		Schritt 6: Datenschutzverletzung
○	○	Ist sichergestellt worden, dass sich Datenschutzverletzungen in Ihrer Praxis erkennen lassen?
○	○	Haben geeignete Methoden festgelegt, um Risiken in Ihrer Praxis zu ermitteln?
○	○	Haben Sie sichergestellt, dass Datenpannen gemäß Art. 33 DSGVO innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden können?