Checkliste: Wie können die Prozesse im Praxisalltag an die Anforderungen der DSGVO angepasst werden?

Die Gültigkeit der Datenschutzgrundverordnung (DSGVO) ab Mai 2018 wirft einige Fragen bei Praxisinhabern auf. Die Gesundheitsdaten sind „personenbezogene Daten besonderer Kategorie“, denen nach der DSGVO ein erhöhter Schutzbedarf zukommt. 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 erforderlichen Prozessschritte der Umsetzung der DSGVO in einer Arztpraxis dar.

Auszüge aus dem Gesetzestext sind *kursiv* gestellt. Auffassungen der „Artikel-29-Datenschutzgruppe“ sind mit einem „*“ versehen. Unterstreichungen stammen von der Verfasserin des Textes und dienen ausschließlich dem besseren Verständnis.

Hinweis:

Die Checkliste dient lediglich der ersten Orientierung bei der Umsetzung der Anforderungen der DSGVO in einer Arztpraxis. Sie enthält daher keine Darstellungen zum Profiling oder zur Übermittlung von Daten an ein Drittland. Wir empfehlen, sich bei der Umsetzung der DSGVO durch entsprechend geschultes Personal oder die Inanspruchnahme eines externen Beratungsdienstleiters unterstützen zu lassen.

Das Kompetenzzentrum für Telemedizin und E-Health Hessen bietet eine unentgeltliche Beratung an, sofern sich die Praxis im Bundesland Hessen befindet. Kontaktieren Sie uns diesbezüglich unter info@ehealth-zentrum.de.

12 Schritte zur Umsetzung der DSGVO in Ihrer Praxis:

JA	NEIN	Schritt 1: Vorbereitung / Ist-Stand-Analyse
❍	❍	Haben Sie sich einen Überblick über alle datenschutzrechtlich relevanten Verarbeitungsvorgänge in Ihrer Praxis verschafft?
❍	❍	Haben Sie eine Bestandsaufnahme gemacht, die beinhaltet welche Daten auf welcher Rechtsgrundlage und von wem verarbeitet werden?
❍	❍	Ist in der Praxis ein generelles Bewusstsein über Datenschutzrisiken vorhanden?
JA	**NEIN**	**Schritt 2: Verzeichnis von Verarbeitungstätigkeiten**
❍	❍	Ist ein Verzeichnis mit den Verarbeitungstätigkeiten gemäß Art. 30 DSGVO angelegt worden? (Die Pflicht hierzu besteht bei Arztpraxen nach Art. 30 V i.V.m. Art. 9 I DSGVO wegen der Verarbeitung von Gesundheitsdaten.)
❍	❍	Sind darin alle unter „Schritt 1: Vorbereitung / Ist-Stand-Analyse“ aufgelisteten Verarbeitungsprozesse genannt?
❍	❍	Haben Sie dabei auch an die Besonderheiten der Verarbeitung von Daten von Kindern gedacht (Einwilligungsfähigkeit)?
❍	❍	Haben Sie dafür gesorgt, dass das Verzeichnis regelmäßig aktualisiert wird?
❍	❍	Haben Sie hierfür Zuständigkeitsregelungen mit den entsprechenden Vertretungsregelungen aufgestellt?
❍	❍	Können Sie die Rechtmäßigkeit für jede Verarbeitungstätigkeit gemäß Art. 5 II DSGVO nachweisen, z.B. bezüglich des Zwecks der Verarbeitung?
❍	❍	Existiert eine Dokumentation des Verzeichnisses, der entnommen werden kann wann welches Verzeichnis erstellt oder aktualisiert wurde und von wem?

JA	NEIN	Schritt 3: Datenschutzbeauftragter
❍	❍	Haben Sie bereits einen (internen / externen) Datenschutzbeauftragten bestimmt? Dieser ist nach Art. 37 Abs. 1 DSGVO grundsätzlich in den folgenden Situationen zu benennen: • *Der Verantwortliche (natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und* • *Mittel der Verarbeitung von personenbezogenen Daten entscheidet) ist eine Behörde oder öffentliche Stelle* oder: • *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* (zum Beispiel bei der Überwachung von gesundheitsbezogenen Daten über in Kleidung integrierte Geräte (Wearables)*) oder: • *Die Kerntätigkeit Ihrer Praxis besteht in der umfangreichen Verarbeitung von besonderen Kategorien von Daten gemäß Art. 9 DSGVO*, worunter u.a. die Gesundheitsdaten fallen (Nicht gegeben bei der Verarbeitung von Patientendaten durch einen einzelnen Arzt*) oder: • *In Ihrer Praxis sind mindestens zehn Personen ständig (d.h. nicht nur gelegentlich, sondern regelhaft) mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt* (§ 38 BDSG) z.B. Mitarbeiter am Empfang, Auszubildende, Ärzte
❍	❍	Haben Sie die Kontaktdaten Ihres Datenschutzbeauftragten gemäß Art. 37 VII DSGVO bei der zuständigen Aufsichtsbehörde gemeldet?
❍	❍	Ist der Datenschutzbeauftragte fachlich qualifiziert?
❍	❍	Kann die fachliche Qualifikation zum Beispiel durch Zertifikate belegt werden?

❍	❍	Für den Fall, dass ein externer Datenschutzbeauftragter engagiert wurde: Haben Sie diesen zur Geheimhaltung verpflichtet?
JA	**NEIN**	**Schritt 4: Datenschutzfolgenabschätzung**
❍	❍	Haben Sie überprüft, ob eine Datenschutzfolgenabschätzung (Art. 35 DSGVO) in Ihrer Praxis notwendig ist? Diese ist immer vorzunehmen, *wenn die Verarbeitung unter Verwendung neuer Technologien* erfolgt (z.B. Cloud Dienste, Videosprechstunde) oder *wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person* besteht. Das ist im Gesundheitsbereich vor allem dann der Fall, wenn eine umfangreiche Verarbeitung von Gesundheitsdaten stattfindet. Nicht umfangreich ist die Verarbeitung personenbezogener Daten von Patienten durch einen einzelnen Arzt*. Davon unabhängig kann ein hohes Risiko bestehen, wenn mindestens zwei* der nachstehenden Kriterien erfüllt sind und die Verarbeitung zu • Diskriminierung, • Finanziellem Verlust, • Rufschädigung, • Verlust der Vertraulichkeit des Patientengeheimnisses, • Verhinderung der Kontrolle über die eigenen Daten oder • Erstellung von Profilen durch Analysen und Prognosen (genetische Analysen) führen könnte oder die • Verarbeitung von personenbezogenen Daten schutzbedürftiger natürlicher Personen (Kinder oder psychisch Erkrankte), • Verarbeitung sensibler Daten (genetische Daten, Gesundheitsdaten, Daten über das Sexualleben) oder • Verarbeitung einer großen Menge von Patientendaten, die wiederum von einer großen Menge von Patienten stammt, betrifft. Die Notwendigkeit für eine Datenschutzfolgenabschätzung kann entfallen, wenn das Risiko durch geeignete technische und organisatorische

		Maßnahmen sog. TOMs (siehe unten unter „Schritt 9 Technische und organisatorische Maßnahmen (TOMs)“) wirksam eingedämmt wurde. Wenn das Risiko wirksam eingedämmt wurde: Haben Sie die Erwägung in die Dokumentation zur Risikoanalyse aufgenommen? Wenn Sie unsicher sind ob das Risiko wirksam eingedämmt wurde, dann kontaktieren Sie die zuständige Datenschutzbehörde.
❍	❍	Wenn die Datenschutzfolgenabschätzung notwendig ist: Haben Sie (1.) *eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung […],* (2.) *eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,* (3.) *eine Bewertung der Risiken* für die Patienten sowie *die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen* […] vorgenommen?
❍	❍	Zu 1.: Umfasst diese: • *Die Art, den Umfang, die Umstände und Zwecke der Verarbeitung* (Erwägungsgrund 90), • die personenbezogenen Daten, die Empfänger und die Speicherfrist für die personenbezogenen Daten*, • eine funktionale Beschreibung der Verarbeitungsvorgänge*, • die Ermittlung der Wirtschaftsgüter, auf die sich die personenbezogenen Daten stützen (Hardware, Software, Netzwerke, Personen, Papiere oder Übertragungsmedien für Papiere)* und die • *Berücksichtigung der Einhaltung genehmigter Verhaltensregeln* (Art. 35 VIII DSGVO)?
❍	❍	Zu 2.: Umfasst diese: • *Festgelegte, eindeutige und legitime Zwecke* (Art. 5 I b) DSGVO), • die *Rechtmäßigkeit der Verarbeitung* (Art. 6),

		• die *Daten, die dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind* (Art. 5 I c) DSGVO) und • eine *Begrenzung der Speicherfrist* (Art. 5 I e) DSGVO)? • Maßnahmen im Sinne der Betroffenen (Informationspflichten, Auskunftsrecht, Recht auf Datenübertragbarkeit, Widerspruchsrecht, Recht auf Einschränkung der Verarbeitung, Verhältnis zu Auftragsverarbeitern, Garantien in Bezug auf die internationale Übermittlung von Daten, vorherige Konsultation)*
❍	❍	Zu 3.: Umfasst diese: • *Ursache, Art, Besonderheit und Schwere der Risiken* (für jedes Risiko: unrechtmäßiger Datenzugriff, unerwünschte Änderung und Verschwinden von Daten einzeln nach Risikoquelle, potentieller Auswirkung auf die Rechte und Freiheiten der Betroffenen, Bedrohung, Eintrittswahrscheinlichkeit und Schwere)*, • eine *Maßnahmenermittlung zur Risikobewältigung* (Art. 35 VII DSGVO), • die *Einbeziehung der betroffenen Parteien* (Art. 35 IX DSGVO) und • die *Einholung des Rates des Datenschutzbeauftragten* (Art. 35 II DSGVO)?

❍	❍	Wenn sich das Restrisiko nach allem immer noch als hoch erweist, zum Beispiel: • wenn die Betroffenen erheblichen oder unumkehrbaren und nicht zu bewältigenden Folgen ausgesetzt sind, also etwa, wenn ein unrechtmäßiger Datenzugriff das Leben der Betroffenen bedroht* <u>oder</u> • eine Gefahr für ihre Arbeitsstelle oder ihre finanzielle Situation darstellt* <u>oder</u> • das Eintreten des Risikos unausweichlich erscheint, weil etwa eine bekannte Sicherheitslücke in der Datenweitergabe nicht behoben wird*: Haben Sie die zuständige Datenschutzbehörde hierüber informiert?
❍	❍	Haben Sie festgelegt wer für die Durchführung der Datenschutzfolgenabschätzung zuständig ist (Achtung: Das entbindet Sie als Praxisinhaber dennoch nicht von der Rechtfertigungspflicht)?
❍	❍	Ist ein Verfahren implementiert worden, das die Aktualität der Datenschutzfolgenabschätzung sicherstellt?
❍	❍	Sind hierin sowohl eine regelmäßige Prüfung enthalten, als auch eine Prüfung bei Änderungen in Verarbeitungsvorgängen, die wiederum zu Änderungen in der Risikobewertung führen können?
❍	❍	Haben Sie hierfür Zuständigkeiten und Vertretungsregelungen festgelegt?
❍	❍	Gibt es eine Dokumentation über die Abwägungsprozesse und getroffenen Entscheidungen im Rahmen der Aktualitätsprüfungen?

JA	NEIN	Schritt 5: Interne Datenschutzrichtlinie
❍	❍	Verfügen Sie über eine interne Datenschutzrichtlinie zur Definition von klaren Verhaltensregeln im Umgang mit Patientendaten und zur Stärkung des Bewusstseins für den Datenschutz? Diese Themen könnte die interne Datenschutzrichtlinie enthalten (nicht abschließend): • Verhaltensweisen bei der Erfassung von Patientendaten • Verantwortlichkeiten bzgl. einzelner Verarbeitungstätigkeiten • Zugriffsbeschränkungen für Mitarbeiter • Dokumentation des Nachweises über die einschlägigen Rechtsgrundlagen zur Verarbeitung personenbezogener Daten (z.B. Wo und in welcher Form die Einwilligung dokumentiert wird), • Verfahren und Zuständigkeiten, um Auskunftsrechtanträge von betroffenen Patienten nach Art. 15 DSGVO zu erfüllen, • Verfahren und Zuständigkeiten, um Anträge auf Berichtigung aus Art. 16 DSGVO zu erfüllen, • Verfahren und Zuständigkeit zur Löschung von Daten nach Wahrnehmung der Rechte aus Art. 17 DSGVO durch einen Patienten oder nach Fristablauf der jeweiligen Aufbewahrungsfristen, • Verfahren und Zuständigkeiten, um Anträge auf Einschränkung der Verarbeitung aus Art. 18 DSGVO zu erfüllen, • Verfahren und Zuständigkeiten, um die Mitteilungspflichten im Zusammenhang mit den vorgenannten Rechten aus Artt. 15 – 18 DSGVO zu erfüllen, • Verfahren und Zuständigkeiten, um Anträge auf Datenübertragbarkeit betroffener Patienten gemäß Art. 20 DSGVO zu erfüllen (nur soweit Daten verarbeitet werden, die nicht unter Art. 9 II 1 DSGVO fallen, sondern rein auf vertraglicher Ebene genutzt werden, z.B. Zahlungsdaten bei IGeL),

		• Verfahren und Zuständigkeit im Falle einer Datenpanne oder eines Datenschutzverstoßes, • Vertretungsregelungen für die oben genannten Zuständigkeiten, • Zugriffsmöglichkeiten für den Datenschutzbeauftragten und dessen Vertreter auf die oben genannten Verfahrensbeschreibungen, • Verbindlichkeitserklärung (zu unterzeichnen durch die Mitarbeiter).
JA	**NEIN**	**Schritt 6: Erfüllung von Informationspflichten**
❍	❍	Sind Ihre Texte zur Information über die Erhebung von personenbezogenen Daten und Auskunftsrechten der betroffenen Personen bereits an Art. 13 DSGVO angepasst worden? Sind dabei insbesondere die folgenden Punkte aufgenommen worden: Aus Art. 13 I DSGVO: • *Name und Kontaktdaten des Verantwortlichen der Praxis sowie ggf. dessen Vertreter*, • *Kontaktdaten des ggf. benannten Datenschutzbeauftragten*, • *Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und die Rechtsgrundlage(n) für die Verarbeitung*, • *Das berechtigte Interesse, sofern die Datenerhebung auf Ihrem berechtigten Interesse oder dem eines Dritten beruht* (Art. 6 I f DSGVO), • *Ggf. die Empfänger bzw. Kategorien von Empfängern der personenbezogenen Daten*, • Sofern die personenbezogenen Daten in Drittländer oder internationale Organisation übermittelt werden sollen: 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* Aus Art. 13 II DSGVO:

		• Geplante *Dauer der Speicherung*. Sofern dies nicht möglich sein sollte, die *Kriterien für die Festlegung dieser Dauer*, • Hinweis bezüglich der Betroffenenrechte auf: o *Auskunft über die betreffenden personenbezogenen Daten* (Art. 15 DSGVO), o *Berichtigung, Löschung oder Einschränkung der Verarbeitung* (Art. 16, 17 DSGVO), o *Widerspruch gegen die Datenverarbeitung* aufgrund besonderer Situation des Patienten (Art. 21 DSGVO), o *Datenübertragbarkeit* (Art. 20 DSGVO), • *Recht zum jederzeitigen Widerruf einer Einwilligung, ohne dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Wiederruf erfolgten Verarbeitung berührt wird* (Art. 13 II c) DSGVO, • *Recht zur Beschwerde bei der Aufsichtsbehörde* (Art. 77 DSGVO), • *Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und ob die betroffene Person verpflichtet ist die Daten bereitzustellen und welche möglichen Folgen eine Nichtbereitstellung hätte* (Art. 13 II e) DSGVO), • 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 die betroffene Person* (Art. 13 II f) DSGVO)?
❍	❍	Bei einer *Zweckänderung* (Art. 13 III DSGVO): Ist gewährleistet, dass die oben genannten Informationen (Art. 13 II DSGVO) der betroffenen Person vor der Weiterverarbeitung für den geänderten Zweck mitgeteilt werden?
❍	❍	Sofern die Daten nicht bei der betroffenen Person erhoben worden sind (Dritterhebung, Art. 14 DSGVO):

		Sind der betroffenen Person die oben genannten Informationen (Erhebung der personenbezogenen Daten bei der betroffenen Person) und zusätzlich die folgenden Informationen erteilt worden: • Angabe über die Kategorien der verarbeiteten Daten (Art. 14 I d) DSGVO), • Angabe der Datenquelle (ersetzt die Angabe, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsschluss erforderlich ist; Art. 14 II f) DSGVO), • Herkunft aus öffentlich zugänglichen Quellen (Art. 14 II f) DSGVO)? Dies ist nicht notwendig, soweit eine der folgenden Ausnahmen greift: • Wenn und soweit *die betroffene Person bereits über die Daten verfügt* (Art. 14 V a) DSGVO) oder, • wenn sich *die Erteilung der Information als unmöglich erweist oder einen unverhältnismäßig hohen Aufwand erfordern würde* (Insbesondere im Zusammenhang mit im öffentlichen Interesse liegenden Archivzwecken und wissenschaftlicher und historischer Forschung; Art. 14 V b) DSGVO) oder, • wenn *die Erlangung oder Offenlegung durch Unionsrecht […] geregelt und geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorgesehen wurden* (Art. 14 V c) DSGVO) oder, • wenn personenbezogene Daten vertraulich behandelt werden müssen, weil sie *dem Berufsgeheimnis* nach Unionsrecht oder dem Recht eines Mitgliedstaates *unterliegen* (Hierunter fallen zum Beispiel Informationen über Krankheiten von Familienangehörigen bei der Anamnese, vgl. Art. 14 V d DSGVO i.V.m. § 29 I 1 BDSG)
❍	❍	Wurde die Überschrift des Informationsblattes an die Empfehlung des Hessischen Landesdatenschutzbeauftragten angepasst („Informationen nach Art. 13 DS-GVO“)?

❍	❍	Erfolgt die Information auf einem separaten Papier getrennt von der Einwilligung?
❍	❍	Haben Sie sichergestellt, dass ihre Mitarbeiter wissen, dass eine Unterschrift auf dem Informationsblatt nicht notwendig ist?
❍	❍	Haben Sie die Empfänger der Daten konkret benannt, also nicht lediglich als „Kassenärztliche Vereinigung“, sondern z.B. als „Kassenärztliche Vereinigung Hessen“?
❍	❍	Enthält Ihre Information den Hinweis, dass die Daten nur mit Einwilligung an andere, als die genannten Stellen übermittelt werden?
❍	❍	Dokumentieren Sie die Übergabe des Informationsblattes? (Dies kann nach dem Hessischen Datenschutzbeauftragten auch in der Form erfolgen, dass ein genereller Verfahrensablauf mit Übergabe des Informationsblattes implementiert und dokumentiert wird und dies dann auf Verlangen der Aufsichtsbehörde vorgelegt wird.)
❍	❍	Haben Sie sichergestellt, dass ihre Mitarbeiter wissen, dass eine Behandlung nicht aus dem Grund abgelehnt werden darf, weil das Informationspapier nicht unterzeichnet wurde?
❍	❍	Enthält das Informationsblatt den Hinweis auf das Recht auf Beschwerde bei einer Aufsichtsbehörde? Wenn es sich hierbei um den „Hessischen Beauftragten für Datenschutz und Informationsfreiheit“ handelt: Haben Sie diesen genau so benannt und haben Sie auch an die Anschrift gedacht?
❍	❍	Enthält Ihr Informationsblatt nur dann einen Hinweis auf das Recht auf Datenübertragbarkeit, wenn kein klassisches Behandlungsverhältnis zugrunde liegt (bei einem klassischen Behandlungsverhältnis ist dies gerade nicht notwendig, vgl. Art. 20 DSGVO i.V.m. Art. 9 II h DSGVO)?
JA	**NEIN**	**Schritt 7: Einwilligung**
❍	❍	Haben Sie Ihre derzeitigen Einwilligungsbögen an Art. 7 DSGVO angepasst? Insbesondere:

		• Bei Einwilligung für mehrere Sachverhalte: Klare Abgrenzbarkeit der Sachverhalte und *verständliche und leicht zugänglicher Form und einfache Sprache*, • *jederzeitiges Widerrufsrecht für die Zukunft*, • *Widerruf, der so einfach ist, wie die Erteilung*.
❍	❍	Haben Sie dabei auch auf die erweiterte Informationspflicht aus Artt. 13 und 14 DSGVO s.o. geachtet?
❍	❍	Haben Sie sichergestellt, dass dem Patienten diese Informationen (nach Art. 13 DSGVO - Erhebung beim Betroffenen), *zum Zeitpunkt der Erhebung* erteilt werden und nicht erst im Nachhinein?
❍	❍	Wenn Sie auch personenbezogene Daten von Kindern im Hinblick auf Dienste der Informationsgesellschaft (gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf erbrachte Dienstleistung, zum Beispiel Fernbehandlungen) verarbeiten: Haben Sie sichergestellt, dass für Kinder unter 16 Jahren die Personensorgeberechtigten einwilligen (Art. 8 I 2 DSGVO)?
❍	❍	Dokumentieren Sie das Vorliegen der Einwilligungen bereits in geeigneter Form (schriftlich), damit diese später nachgewiesen werden kann?
JA	**NEIN**	**Schritt 8: Auftragsverarbeitung**
❍	❍	Sind Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter; Art. 28 DSGVO) eingebunden (z.B. IT-Dienstleister)?
❍ ❍ ❍	❍ ❍ ❍	Falls ja: • Haben Sie eine Liste aller Auftragsverarbeiter erstellt? • Bieten die Auftragsverarbeiter *hinreichende Garantien* dafür, dass die *Verarbeitung im Einklang mit der DSGVO erfolgt*? • Verwenden Sie hierfür *geeignete technische und organisatorische Maßnahmen*?

❍	❍	• Haben Sie mit allen Auftragsverarbeitern eine vertragliche Vereinbarung mit dem Mindestinhalt nach Art. 28 III DSGVO geschlossen? Insbesondere: o Verpflichtung *keine Unterauftragsverarbeitung ohne vorherige Unterrichtung des Verantwortlichen und Genehmigung durch den Verantwortlichen* zu bestellen und dabei die gemeinsamen Bedingungen über die Unterauftragsverarbeitung einzuhalten (Art. 28 II, III 2 d), IV DSGVO), o *Gegenstand und Dauer der Verarbeitung* (Art. 28 III 1 DSGVO) o *Art der personenbezogenen Daten* (Art. 28 III 1 DSGVO), o *Kategorien betroffener Personen* (Art. 28 III 1 DSGVO), o *Pflichten und Rechte der Verantwortlichen* (Art. 28 III 1 DSGVO), o Verarbeitung der Daten nur auf *dokumentierte Weisung* des Verantwortlichen hin oder aufgrund rechtlicher *Verpflichtung* (Art. 28 III 2 a) DSGVO), o Gewährleistung der *Verpflichtung zur Vertraulichkeit* der Mitarbeiter durch den Auftragsverarbeiter (oder vergleichbare *gesetzliche Verpflichtung*) (Art. 28 III 2 b) DSGVO), o *Technische und organisatorische Maßnahmen*, die notwendig sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 28 III 2 c) DSGVO), o Verpflichtung zur *Unterstützung des Verantwortlichen seiner Pflicht zur Beantwortung von Anträgen der Betroffenen u.a. auf Löschung nachzukommen (z.B. durch geeignete technische und organisatorische Maßnahmen)* (Art. 28 III 2 e) DSGVO), o Verpflichtung zur *Unterstützung des Verantwortlichen* seinen übrigen Pflichten, z.B. der Meldung von Datenschutzverletzungen, der Benachrichtigung des

		Betroffenen im Falle einer Datenschutzverletzung, der Konsultation des Datenschutzbeauftragten und bei der Datenschutzfolgenabschätzung *unter Berücksichtigung der Art der Verarbeitung nachzukommen z.B. durch geeignete technische und organisatorische Maßnahmen* (Art. 28 III 2 f) DSGVO), o *Pflicht nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht* (Art. 28 III 2 g) DSGVO), o *Pflicht dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung zu stellen und Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen* (Art. 28 III 2 h) DSGVO) und o Mit Blick auf Art. 28 III 2 h) DSGVO: *Verpflichtung den Verantwortlichen unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt* (Art. 28 III 3 DSGVO).

JA	NEIN	Schritt 9: Technische und organisatorische Maßnahmen (TOMs)
❍	❍	*Haben Sie unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten* (Sicherheit der Verarbeitung, Art. 32 I DSGVO)? Insbesondere: • Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 I a) DSGVO), • *Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste, die die Daten verarbeiten* (Art. 32 I b) DSGVO), • *Fähigkeit bei einem physischen oder technischen Zwischenfall die Verfügbarkeit oder den Zugang zu den personenbezogenen Daten rasch wiederherzustellen* (Art. 32 I c) DSGVO).
❍	❍	Haben Sie bei der *Bewertung der Angemessenheit des Schutzniveaus besondere Risiken beachtet, wie die unbeabsichtigte oder unrechtmäßige Vernichtung, den Verlust, die Veränderung oder die unbefugte Offenlegung von personenbezogenen Daten oder den unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet* wurden (Art. 32 I II DSGVO)*?*
❍	❍	Haben Sie und hat der Auftragsverarbeiter *sichergestellt, dass die Ihnen/ihm unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen oder aufgrund einer zwingenden Rechtsvorschrift der Union oder eines Mitgliedstaates verarbeiten* (Art. 32 IV DSGVO)*?*
❍	❍	Gibt es ein *Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen*

		Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 I d) DSGVO)?
❍	❍	Werden alle Überprüfungen, Bewertungen und Evaluierungen dokumentiert?
❍	❍	Haben Sie hierfür jeweils Zuständigkeiten und Vertretungen vergeben?
JA	**NEIN**	**Schritt 10: Meldung von Datenschutzverletzungen**
❍	❍	Haben Sie geeignete Methoden festgelegt, um Datenschutzrisiken in Ihrer Praxis zu ermitteln?
❍	❍	Ist sichergestellt worden, dass sich Datenschutzverletzungen (z.B. versehentlicher Verlust von Datenträgern) in Ihrer Praxis erkennen lassen?
❍	❍	Haben Sie sichergestellt, dass Datenpannen gemäß Art. 33 I DSGVO *unverzüglich und möglichst innerhalb von 72 Stunden* nachdem die Verletzung bekannt wurde, an *die Aufsichtsbehörde gemeldet werden*? (Ausnahme: Wenn voraussichtlich (Prognose) kein Risiko für die Rechte und Freiheiten der Patienten besteht, weil bereits entsprechend geeignete Gegenmaßnahmen ergriffen wurden, Art 33 I DSGVO.)
❍	❍	Enthält die Meldung an die Aufsichtsbehörde mindestens die folgenden Punkte (Art. 33 III a) - d) DSGVO: • *eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;* • *den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;* • *eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;* • *eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls*

		Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen?
❍	❍	Wenn voraussichtlich (Prognose) ein *hohes Risiko für die Rechte und Freiheiten der betroffenen Person* besteht: Haben Sie auch an die unverzügliche *Benachrichtigung des Betroffenen in klarer einfacher Sprache gedacht, die die Art der Verletzung und die in Art. 33 III b, c, d DSGVO genannten Informationen und Maßnahmen enthält* (Art. 34 DSGVO)?
❍	❍	Wenn die Meldung später als 72 Stunden nachdem sie dem Verantwortlichen bekannt wurden ergeht: Haben Sie der Meldung eine *Begründung für die Verzögerung beigefügt* (Art. 33 I 2 DSGVO)?
❍	❍	Haben Sie sichergestellt, dass jegliche Datenschutzverletzungen und die dazugehörigen Meldungen dokumentiert werden (Art 33 V DSGVO)?
❍	❍	Haben Sie hierfür jeweils Zuständigkeiten und Vertretungen vergeben?
JA	**NEIN**	**Schritt 11: Mitarbeiter**
❍	❍	Werden die Mitarbeiter regelmäßig (etwa im 2 Jahres Rhythmus) geschult und im sicheren Umgang mit personenbezogenen Daten angeleitet?
❍	❍	Werden neue Mitarbeiter außerturnusmäßig geschult und angeleitet?
❍	❍	Wird die konsequente Umsetzung des Datenschutzes in der Praxis regelmäßig überprüft?
❍	❍	Erfolgt eine Dokumentation der Überprüfung?
❍	❍	Werden die Ergebnisse der internen Überprüfung besprochen und ggf. Hinweise erteilt?
JA	**NEIN**	**Schritt 12: Internetseite**
❍	❍	Verfügt ihre Internetseite über eine aktuelle Datenschutzerklärung?

Weitergehende Informationen / Hilfreiche Links:

Die **Datenschutzgrundverordnung** finden Sie unter:

https://dejure.org/gesetze/DSGVO

Ein Musterbeispiel für ein **Verzeichnis der Verarbeitungstätigkeiten** finden Sie unter: https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Verarbeitungsverzeichnis_Muster.docx

Hier finden Sie ein **beispielhaft ausgefülltes Verarbeitungsverzeichnis**, ebenfalls von der KBV:
https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Verarbeitungsverzeichnis_Ausfuellbeispiel.pdf

Ein **Patienteninformationsblatt zum Datenschutz in der Arztpraxis** der KBV finden Sie unter:
https://www.laekh.de/fileadmin/user_upload/Aerzte/Rund_ums_Recht/Publikationen_und_Merkblaetter/Informationspflichten_DSGVO.pdf

Ein Muster der GDD zur **Vertragsgestaltung mit dem Auftragsdatenverarbeiter** finden Sie unter:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/FormulierungshilfeAuftragsverarbeitungsvertrag%20nach%20DSGVO.pdf

oder ein vergleichendes Muster unter:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

Zur **Einwilligung** gibt es eine Ausführliche Darstellung der GDD unter: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_13.pdf

Ein Muster für eine **Einverständniserklärung für den Recall-Service** (Zahnärzte) finden Sie unter:
https://www.zaekmv.de/fileadmin/Redaktion/Downloads_Datenschutz/EinwilligungRecall_Muster.doc

Die **Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung** in der Arztpraxis der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung finden Sie unter:
https://www.kbv.de/media/sp/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

Zur Konkretisierung der „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ hat die Bundesärztekammer zusammen mit der Kassenärztlichen Bundesvereinigung eine **Technische Anlage** herausgegeben. Diese finden Sie unter:
https://www.kbv.de/media/sp/Technische_Anlage_Datenschutz.pdf

„Leitlinie Risikobewertung“: Leitlinie zur **Datenschutzfolgenabschätzung und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“** der Artikel 29 Datenschutzgruppe (genehmigt von dem Europäischen Datenschutzausschuss und damit weiterhin gültig) finden Sie unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

(Auf der gleichen Website ist unter dem Link „Available Language Versions“ als vierte Datei von oben auch die deutsche Version abrufbar.)

Die **Meldung der Kontaktdaten des Datenschutzbeauftragten** für Ihre Praxis in Hessen können Sie online vornehmen unter:
https://datenschutz.hessen.de/service/benennung-eines-datenschutzbeauftragten

Von dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit wird ein **Formular zur Meldung von Verletzungen des Schutzes personenbezogener Daten** unter folgendem Link bereitgestellt:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formular%20Art%2033_0.docx

Zum Thema Datensicherheit steht unsere Checkliste „**Datensicherheit und sicherer Umgang mit Patientendaten in der Arztpraxis“** zum Download bereit. Diese bietet wertvolle Tipps und Informationen zur praktischen Gestaltung des Umgangs mit Patientendaten in der Arztpraxis.
Sie finden diese auf der Internetseite des Kompetenzzentrums unter:
https://www.ehealth-zentrum.de/Downloads

Hinweis:

Alle Links wurden zuletzt am 07.10.2020 auf ihre Erreichbarkeit geprüft.

Soweit im Text die männliche Form genutzt wird, sind selbstverständlich auch immer die weibliche und diverse Form mit gemeint.

Haftungsausschluss:

Für die Richtigkeit und Vollständigkeit der Angaben wird keine Haftung übernommen. Auch wird hinsichtlich der Richtigkeit und Vollständigkeit des Inhaltes der verlinkten Dokumente oder Webseiten keine Haftung übernommen. Diese sollen lediglich als Arbeitshilfe dienen und zu einem ersten Überblick verhelfen.

Version: CL_Datenschutz_v01.9
Datum der Veröffentlichung: 15.03.2019
Letzte Änderung: 07.10.2020