

Checkliste

Datenschutz in der ärztlichen Praxis

Die nachfolgende Checkliste dient als erster Selbst – Check für die die Datenschutzkonformität Ihrer Arztpraxis.

Praxis (Raumorganisation)	
Empfangsbereich	
Ist sichergestellt, dass der Zutritt zur Praxis kontrolliert wird (Zutrittskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Existiert eine Diskretionszone vor dem Empfangsbereich?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Wurden im Empfangsbereich sonstige organisatorische Maßnahmen getroffen, um auszuschließen, dass Dritte Patientendaten zur Kenntnis erlangen?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Werden Patientendaten (persönliche Daten, Anliegen) im Rahmen der Anmeldung so erhoben, dass Dritte diese nicht mithören- oder mitlesen können?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind Faxgeräte, Bildschirme oder sonstige Endgeräte so plziert, dass Dritte keine Kenntnis von etwaigen Patientendaten nehmen können?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind Datenverarbeitungssysteme im Empfangsbereich so gesichert, dass ein unberechtigter Zugang nicht möglich ist (Zugangskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind physische und digitale Patientenakten, Kalender oder Karteikarten im Empfangsbereich vor dem Zugriff Unbefugter geschützt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Werden die Patienten darauf hingewiesen, dass sie ein Anamneseformular freiwillig individuell ausfüllen können?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Wartebereich	
Ist der Wartbereich vom Empfangsbereich- und Behandlungsbereich räumlich so getrennt, dass wartende Patienten keine Patientendaten aus dem Empfangs- und Behandlungsbereich zur Kenntnis erhalten?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Behandlungsbereich	
Ist der Behandlungsbereich / sind die unterschiedlichen Behandlungsräume so ausgestaltet, dass die Kenntniserlangung von fremden Patientendaten durch wartende, untersuchte oder behandelte Patienten ausgeschlossen ist?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist etwaig im Behandlungsbereich vorhandene EDV bei Abwesenheit des Arztes gesperrt, so dass Patienten keinen Zugang zu fremden Patientendaten haben?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig

Praxis (Elektronische Datenverarbeitung, Verwaltung)	
Sind sämtliche Datenverarbeitungssysteme der Praxis so gesichert, dass ein unberechtigter Zugang nicht möglich ist (Zugangskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind EDV – Arbeitsplätze durch Passwörter geschützt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind die Passwörter den aktuellen Sicherheitsstandards angelehnt (BSI Empfehlung: mind. 8 Zeichen, bestehend aus Buchstaben, Zahlen, Sonderzeichen)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Besteht eine Routine, die Passwörter nach gewissen Zeitabläufen zu ändern?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist bei jedem EDV – Arbeitsplatz ein passwortgeschützter Bildschirmschoner eingerichtet?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist nur dem betreffenden Mitarbeiter das Passwort für den jeweiligen EDV – Arbeitsplatz bekannt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Für den Fall, dass das EDV – System auch mit dem Internet verbunden ist: Existiert eine ausreichende Firewall?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist ein Backup – System für die EDV – Systeme, insbesondere die Patientendaten, implementiert (Verfügbarkeitskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind sämtliche Datenverarbeitungssysteme so eingerichtet, dass die Praxismitarbeiter nur auf diejenigen Daten zugreifen können, für die sie eine Zugriffsberechtigung haben (Zugriffskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist sichergestellt, dass Patientendaten im Rahmen der elektronischen Übertragung oder während des Transports z.B. von Akten, Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt (u.a. durch Verschlüsselungsverfahren) werden können (Weitergabekontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden (Eingabekontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Wird das Patientengeheimnis gewahrt, sofern externe Dienstleister mit der Administration und Wartung des der Praxis – EDV beauftragt sind?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist gewährleistet, dass Patientendaten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind physische und digitale Patientenakten, Kalender oder Karteikarten in der Praxis vor dem	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt

Zugriff Unbefugter geschützt?	<input type="checkbox"/> Nicht einschlägig
Werden physische Patientenakten in abschließbaren Aktenschränken aufbewahrt? Werden diese Aktenschränke außerhalb der Öffnungszeiten verschlossen?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sind die Praxisräume ausreichend gegen Einbruch geschützt (Zutrittskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist sichergestellt, dass externe Dienstleister (u.a. Reinigungspersonal) keinen Zugang zu Patientendaten haben?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist das Patientenaktenarchiv datenschutzkonform abgelegt (Zutrittskontrolle Zugangskontrolle)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist sichergestellt, dass physische Patientenakten oder Datenträger mit digitalen Patientendaten datenschutzkonform entsorgt werden (nach DIN 66399 zur Datenvernichtung)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist sichergestellt, dass die Praxismitarbeiter über die Verschwiegenheitspflicht belehrt wurden? Wurde die Belehrung schriftlich festgehalten?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Wurden die Praxismitarbeiter gemäß § 5 BDSG schriftlich auf das Datengeheimnis verpflichtet?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Werden die Praxismitarbeiter regelmäßig zu den Themen Verschwiegenheitspflicht und Datenschutz sensibilisiert und geschult?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Patientenrechte in der Praxis	
Findet eine Aufklärung der Patienten über die bestehenden Datenschutzrechte statt oder werden diese auf Wunsch mitgeteilt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Ist in der Praxis ein Ablauf definiert, wie mit datenschutzrechtlichen Anfragen von Betroffenen (Patienten) umgegangen wird?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Werden die gesetzlichen Fristen für die Löschung von Patientendaten und -akten (10 bzw. 30 Jahre) umgesetzt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Werden die Ansprüche der Patienten aus dem Patientenrechtegesetz (Anspruch auf Kopie der Patientenakte, Zurverfügungstellung der im Rahmen der Patientenaufklärung oder -einwilligung unterzeichnete Unterlagen) umgesetzt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Übermittlung von Patientendaten	
Wird sichergestellt, dass Empfänger von Patientendaten nur diejenigen Daten erhalten, die zur Erfüllung ihrer jeweiligen Aufgaben benötigt werden (Zurverfügungstellung auf „Need to know Basis“)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Werden Patientenauskünfte an Dritte zunächst an den Patienten weitergeleitet, bevor sie (nach Einwilligung des Patienten) von der Praxis herausgegeben werden?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig

Erfolgt eine Abrechnung über private Versicherungen oder privatärztliche Verrechnungsstellen ausschließlich nach ausdrücklicher Einwilligung des Patienten?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sofern es sich um eine Hausarztpraxis handelt: Werden Patientendaten von anderen behandelnden Ärzten nur mit schriftlicher Einwilligung des Patienten erhoben?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Sofern es sich um eine Facharztpraxis handelt: Werden Patientendaten an den Hausarzt nur mit schriftlicher Einwilligung des Patienten übermittelt?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Wir bei Übersendung von Patientendaten per Fax oder Email sichergestellt, dass nur der Patient oder Berechtigte Empfänger der Daten sind?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig
Wird eine ausreichend gesicherte Anlage für die Telefon Kommunikation genutzt (z.B. <u>nicht</u> bei Internet – Telefonie)?	<input type="checkbox"/> Erfüllt <input type="checkbox"/> Nicht erfüllt <input type="checkbox"/> Nicht einschlägig

Eine verbindliche Feststellung, ob eine Praxis datenschutzkonform eingerichtet ist und arbeitet, kann allerdings nur im Rahmen einer vollständigen Datenschutzprüfung getroffen werden.

Kontakt

Peer Fischer, Rechtsanwalt

BBP Rechtsanwälte

Mommsenstr. 11

10629 Berlin

W: www.bbp-legal.com

E: fischer@bbp-legal.com