Verfahrensanweisung **Praxisinterne Richtlinie zum Datenschutz** „Umsetzung des Datenschutz“	Praxisstempel

Diese Richtlinie dient als verbindliche Vorgabe für einen der DSGVO und dem BDSG entsprechenden Schutz der personenbezogenen Daten in unserer Zahnarztpraxis.

Dadurch sollen die Rechte und Freiheiten von Patienten, Mitarbeitern der Praxis und sonstigen Betroffenen, insbesondere der Schutz ihrer personenbezogenen Daten gewährleistet werden.

Die Richtlinie wird für alle Mitarbeiter und Berufsträger der Praxis jederzeit zugänglich gemacht.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter und Berufsträger unserer Zahnarztpraxis.

Die Vorgaben dieser Richtlinie gelten für den Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform erfolgt. Es werden sämtliche Daten von allen Arten von Betroffenen (Patienten, Mitarbeiter, Kontaktpersonen von Vertragspartnern der Praxis) in den Geltungsbereich der Richtlinie einbezogen.

Begriffsbestimmungen

Bei personenbezogenen Daten handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Dazu gehören unter anderem Daten der Patienten und der Beschäftigten der Zahnarztpraxis. Aber auch Kontaktdaten von Beschäftigten der Vertragspartner der Praxis können davon betroffen sein. Es ist ausreichend, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann.

Besondere Arten personenbezogener Daten sind in einer Zahnarztpraxis alle Informationen, die einen Gesundheitsbezug einer natürlichen Person aufweisen.

Datenverarbeitung ist jeder analoge oder automatisierte Vorgang. Dazu gehört das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten.

Verantwortlicher im Sinne des Datenschutzes sind in einer Zahnarztpraxis der oder die niedergelassenen Zahnärztinnen und Zahnärzte.
Auftragsverarbeiter ist in einer Zahnarztpraxis z.B. das externe Dentallabor, das im Interesse der Praxis personenbezogene Daten von Patienten oder Beschäftigten im Auftrag des Verantwortlichen verarbeitet.

Empfänger ist z.B. die Privatversicherung im Rahmen der privaten Abrechnung, der personenbezogene Daten offengelegt werden.
Dritter ist z.B. das externe Abrechnungsunternehmen, das im Interesse der Zahnarztpraxis personenbezogene Patientendaten zum Zwecke der Abrechnung erhält.

Eine Einwilligung des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sons-

tigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

Datenschutzorganisation

Für unsere Zahnarztpraxis wurde kein Datenschutzbeauftragter bestellt.

Optional:
Für unsere Zahnarztpraxis wurde ein Datenschutzbeauftragter bestellt. Diesen erreichen Sie unter folgenden Kontaktdaten: _____.

Der Datenschutzbeauftragte überwacht die Einhaltung der DSGVO sowie anderer gesetzlichen Vorgaben, einschließlich der Vorgaben dieser und anderer Richtlinien der Zahnarztpraxis. Der Datenschutzbeauftragte berät und unterrichtet die Praxisführung hinsichtlich bestehender Datenschutzpflichten und ist zuständig bei der Kommunikation mit Aufsichtsbehörden. Der Datenschutzbeauftragte überprüft stichprobenartig und in angemessenen Zeitabständen die Praxis bezüglich der datenschutzrechtlichen Bestimmungen. Bei der Erfüllung seiner Aufgaben ist er weisungsfrei und erstattet seinen Bericht unmittelbar der Praxisführung. Diese unterstützt ihn bei seinen Aufgaben.

Umgang mit personenbezogenen Daten

Die personenbezogene Datenverarbeitung ist grundsätzlich unzulässig und setzt eine gesetzliche Erlaubnis voraus. Personenbezogene Daten dürfen nach der DSGVO verarbeitet werden:

- wenn ein Vertragsverhältnis mit dem Betroffenen (z.B. Kontaktdaten des Ansprechpartners des Dentallabors) besteht,
- bei vorvertraglichen Maßnahmen auf Anfrage des Patienten sowie der Vertragsabwicklung mit dem Patienten (z.B. Patienten erscheint zum ersten Behandlungstermin in der Praxis und füllt den Anmeldebogen aus),
- aufgrund einer Einwilligung des Betroffenen (z.B. Patient wünscht die Teilnahme am Recall)
- aufgrund einer gesetzlichen Dokumentationspflicht (z.B. die nach dem Patientenrechtgesetz vorgeschriebene Dokumentation der Behandlungsinformationen)
- bei berechtigtem Interesse der Praxis (z.B. im Falle der Forderungsdurchsetzung des zahnärztlichen Honorars).

Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck (z.B. die Speicherung von Daten auf Vorrat) ist unzulässig.

Pseudonyme oder anonyme Datenverarbeitungen sind, soweit in der Zahnarztpraxis möglich, vorzuziehen.

Der Betroffene ist umfassend über die Datenverarbeitung nach den Vorgaben des Art. 13 DSGVO zu informieren. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen.

Werden personenbezogene Daten nicht beim Betroffenen erhoben, ist der Betroffene nachträglich und umfassend gem. Art. 14 DSGVO über den Umgang mit seinen Daten zu informieren.

Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, ver-

arbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport) zum Schutz besonderer personenbezogener Daten zu ergreifen.

Datenübermittlung

Personenbezogenen Daten dürfen nur an Dritte aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen überlassen werden. Befindet sich der Empfänger außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist.

Externe Dienstleister

Externe Dienstleister sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl sollte insbesondere folgendes berücksichtigen:

- Fachliche Eignung des Auftragnehmers für Umgang mit Daten
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Dienstleisters

Mit dem externen Dienstleister ist zwingend ein Vertrag zur Auftragsdatenverarbeitung abzuschließen.

Datenminimierung

Die Praxis soll so wenige Daten wie möglich von einem Betroffenen erheben, verarbeiten oder nutzen. Wenn möglich sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren.

Rechte von Betroffenen

Betroffene haben das Recht auf Auskunft über die in der Praxis über ihre Person gespeicherten personenbezogenen Daten. Die Auskunft durch die Praxis erfolgt schriftlich, wenn der Betroffene die Auskunft nicht in elektronischer Form verlangt. Der Umfang des Auskunftsanspruchs ergibt sich aus den Vorgaben des Art. 15 DSGVO. Auf Wunsch des Betroffenen werden die Daten in einem gängigen und maschinenlesbaren Format zur Verfügung gestellt.

Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.
Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich
- der Betroffene hat seine Einwilligung z.B. zum Recall widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung
- ihre Verarbeitung ist unzulässig
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt
- das Unternehmen die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt
- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

Spätestens innerhalb eines Monats muss der Betroffene über alle Maßnahmen informiert werden.

Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, z.B. zu Patientendaten, ist eine Herausgabe der Daten nur zulässig, wenn

- die anfragende Stelle ein berechtigtes Interesse darlegen kann und
- eine gesetzliche Norm die Praxis zur Auskunft verpflichtet sowie
- die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

Verzeichnis von Verarbeitungstätigkeiten

Es wird ein Verzeichnis über alle Datenverarbeitungen geführt. Hierfür ist der Praxisinhaber verantwortlich. Auf Anfrage wird der Datenschutzbehörde das Verzeichnis zur Verfügung gestellt. Dafür zuständig ist ebenfalls der Praxisinhaber.

Praxisinformationssystem

Ein Recall bzw. das Zusenden von Praxisflyern etc. an Betroffene ist grundsätzlich nur zulässig, wenn diese in die Verwendung ihrer Daten für diese Zwecke mittels einer schriftlichen Einwilligungserklärung eingewilligt haben.

Schulung

Es finden regelmäßige Schulungen für mit der Datenverarbeitung befasste Berufsträger und Beschäftigte der Praxis statt. Die Durchführung der Schulungen ist jeweils in einem Protokoll zu dokumentieren.

Datengeheimnis

Beschäftigten der Praxis ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Vor Aufnahme ihrer Tätigkeit werden sie auf das Datengeheimnis gemäß dem zugehörigen Formular verpflichtet.

Beschwerden

Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, wenn er eine Verletzung seiner Rechte behauptet. Ebenso können Mitarbeiter der Praxis Verstöße gegen diese Richtlinie jederzeit anzeigen.

Audits

Zur Sicherstellung des Datenschutzniveaus werden Prozesse der Datenverarbeitung regelmäßig intern überprüft. Sind Verbesserungen im Rahmen des Datenschutzes erforderlich, werden diese unverzüglich vorgenommen. Die Prüfungen sind zu dokumentieren.

Sicherheitskonzept für Datenverarbeitung

Eine unbefugte Nutzung von Daten der Praxis ist zu verhindern. Unbesetzte Räume müssen verschlossen werden, Zugangskontrollen für EDV-Stationen müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit immer zu sperren. Patientenakten dürfen nicht unbeaufsichtigt in der Praxis herumliegen.

Passwörter sind dem persönlichen Gebrauch der berechtigten Person vorbehalten. Sie müssen eine minimale Länge von zehn Zeichen aufweisen und aus einem Zeichenmix bestehen. Passwörter dürfen nicht aus leicht zu erratenden Begriffen gebildet werden.

Personenbezogene Daten dürfen nur von den Berufsträgern und Mitarbeitern der Praxis verwendet werden, die aufgrund der ihnen obliegenden Aufgaben die Daten verwenden müssen. Wer zum Zugriff berechtigt ist, muss festgelegt und dokumentiert sein.

Datenübertragungen durch das öffentliche Internet müssen, soweit wie möglich, verschlüsselt werden. Eine Verschlüsselung hat immer zu erfolgen, wenn es sich bei den Daten um solche mit sehr hohem Schutzbedarf handelt (z.B. Gesundheitsdaten).

Erfolgen Wartungsarbeiten dem praxiseigenen EDV- und Kommunikationssystem durch einen externen Dienstleister, ist dieses zu beaufsichtigen. Es muss gewährleisten sein, dass externe Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen.

Datenschutzverstoß

Erfolgt ein Datenschutzverstoß, ist unverzüglich nach dem Ablaufplan „Internes Vorgehen bei Datenschutzverstoß“ zu verfahren. Die Datenschutzbehörde und die Betroffenen werden durch den Praxisinhaber informiert.

Verstöße

Ein fahrlässiger oder vorsätzlicher Verstoß gegen Vorgaben dieser Richtlinie kann arbeitsrechtliche Sanktionen, wozu auch eine fristlose oder ordentliche Kündigung gehören kann, nach sich ziehen. Außerdem können Verstöße gegen den Datenschutz strafbewehrt sein und zivilrechtliche Folgen wie Schadenersatz drohen.

Nachweisbarkeit

Es ist eine transparente Nachweisbarkeit der Einhaltung dieser Richtlinie sichergestellt.

Aktualisierung

Diese Richtlinie ist unter Berücksichtigung der Weiterentwicklung des Datenschutzrechts sowie der technologischen oder organisatorischen Veränderungen in angemessenen Zeitabständen anzupassen. Änderungen an dieser Richtlinie sind formlos wirksam. Die Mitarbeiter der Praxis und Berufsträger sind umgehend über die geänderte Richtlinie zu informieren.

	Datum	**Unterschrift**
Verantwortliche/r für den Datenschutz		