Das neue Datenschutzrecht kommt zum 25. Mai 2018

WICHTIG: RELEVANTE REGELUNGEN UND GESETZLICHE NEUERUNGEN FÜR DIE ZAHNÄRZTLICHE PRAXIS – TEIL 1

Wie bereits in der Ausgabe 2/2018 des Rheinischen Zahnärzteblatts angekündigt, informiert die Zahnärztekammer (ZÄK) Nordrhein ihre Mitglieder über die rechtlichen Neuerungen im Datenschutzrecht. Am 25. Mai 2018 werden sowohl die Datenschutzgrundverordnung als auch daneben das neue Bundesdatenschutzgesetz in Kraft treten und zahlreiche verbindliche Änderungen für die Zahnärzteschaft mit sich bringen. Der vorliegende Artikel soll den Mitgliedern der ZÄK Nordrhein einen Überblick der relevanten gesetzlichen Neuregelungen des Datenschutzrechts verschaffen und zugleich über sie informieren. In Zusammenarbeit mit den anderen Heilberufskammern des Landes Nordrhein-Westfalen wurden die Vorgänge analysiert und nach aktuellem Kenntnisstand bewertet. Im nächsten Rheinischen Zahnärzteblatt (Ausgabe 4/2018) werden weitere Erläuterungen und Hilfestellungen sowohl zu den Informationspflichten des Zahnarztes, zu den Rechten der betroffenen Personen, zur Auftragsverarbeitung als auch zu den Folgen bei Verstößen gegen das Datenschutzrecht erfolgen.

A. RELEVANTE NORMEN

I. DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119, S. 1) wird ab dem **25.05.2018** unmittelbar geltendes Recht in allen Mitgliedsstaaten der Europäischen Union (EU) sein. Das bedeutet, dass die Verordnung nicht in nationales Recht umgewandelt werden muss. Erklärtes Ziel der DSGVO ist es, eine Harmonisierung der datenschutzrechtlichen Vorschriften innerhalb der EU zu schaffen, um so ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten zu erreichen.

II. BUNDESDATENSCHUTZGESETZ (BDSG-NEU)

Der Bundestag hat zudem im Rahmen von Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Anpassung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) mit Zustimmung des Bundesrats eine konstitutive Neuregelung des Bundesdatenschutzgesetzes beschlossen. Das Gesetz wurde am 30.06.2017 verkündet (BGBl. I. S. 2132 vom 05.07.2017) und tritt ebenfalls am **25.05.2018** in Kraft. Gleichzeitig tritt das Bundesdatenschutzgesetz (BDSG-alt) in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I. S. 66 vom 24.01.2003) außer Kraft.

Die DSGVO und das BDSG-neu schließen sich nicht aus und sind nebeneinander anzuwenden. Die entsprechenden Vorschriften sind auf der Webseite unter www.zahnaerztekammer nordrhein.de/fuer-die-praxis-beruf-wissen/datenschutz/ eingestellt.

B. Auswirkungen für die Zahnärzteschaft

Vorangestellt sei ausdrücklich, dass von den datenschutzrechtlichen Neuerungen auch Zahnärzte und Zahnärztinnen betroffen sind und die Verunsicherung hinsichtlich der Umsetzung derzeit allgemein groß ist. Nachfolgend werden die wesentlichen Auswirkungen durch das neue Datenschutzrecht dargestellt sowie erläutert. Der folgende Beitrag dient der Hilfestellung.

I. ADRESSAT DER DATENSCHUTZRECHTLICHEN BESTIMMUNGEN

Adressat der datenschutzrechtlichen Bestimmungen ist der sogenannte **Verantwortliche**, der die Rechte der **betroffenen Person** zu wahren hat. Der bzw. **alle Inhaber** einer zahnmedizinischen Einrichtung ist/sind der/die Verantwortliche/n im Sinne des Art. 4 Nr. 8 DSGVO. Betroffene Person im Sinne des Art. 4 Nr. 1 DSGVO sind in der Regel der Patient und der Mitarbeiter.

II. RECHTMÄßIGE DATENVERARBEITUNG

1. Verarbeitung personenbezogener Daten

Nur wenn mindestens einer der in Art. 6 Abs. 1 DSGVO erwähnten Umstände bzw. Rechtfertigungsgründe vorliegt, ist eine Verarbeitung personenbezogener Daten durch den Verantwortlichen rechtmäßig.

> Eine **Verarbeitung** ist *„jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Verände-*

rung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung" (Art. 4 Nr. 2 DSGVO). **Es wird nicht zwischen der Speicherung personenbezogener Daten in digitaler oder in Papierform unterschieden, da unter den Begriff der Verarbeitung sowohl automatisierte als auch manuelle Verarbeitungsvorgänge fallen.**

Personenbezogene Daten sind *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann"* (Art. 4 Nr. 1 DSGVO). Hierunter fallen als Identifizierungsmerkmale im vorgenannten Sinne z. B. Vor- und Nachname, Adresse, Geburtsdatum und Telefonnummer.

Im Bereich der zahnmedizinischen Einrichtung sind regelmäßig Art. 6 Abs. 1 lit. a DSGVO (Verarbeitung auf der Grundlage einer Einwilligung der betroffenen Person) sowie Art. 6 Abs. 1 lit. c DSGVO (Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung wie z. B. die Übermittlung von Leistungsdaten an Krankenkassen und die Kassenzahnärztliche Vereinigung, §§ 294 ff. SGB V) für die Verarbeitung personenbezogener Daten einschlägig.

Anders als noch § 4 a Abs. 1 S. 3 BDSG-alt bestimmt Art. 7 DSGVO kein Schriftformerfordernis mehr für eine erklärte Einwilligung. Es genügt fortan, wenn die informierte betroffene Person unmissverständlich bekundet, mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden zu sein (z. B. Nicken). Die Einwilligung kann aber auch weiterhin **schriftlich**, **elektronisch** oder **mündlich** erfolgen. Es ist – trotz des fehlenden Schriftformerfordernisses – zu Beweiszwecken dennoch zu empfehlen, eine schriftliche Einwilligung einzuholen oder eine unmissverständlich bekundete Einwilligung zu dokumentieren. Die betroffene Person ist vor Erklärung der Einwilligung umfassend nach Maßgabe des Art. 13 DSGVO zu informieren (Ausführungen zu den Informationspflichten werden in der Ausgabe 4/2018 des Rheinischen Zahnärzteblatts erfolgen). Eine erteilte Einwilligung kann durch die betroffene Person mit Wirkung für die Zukunft **widerrufen** werden (Art. 7 Abs. 3 DSGVO).

2. Verarbeitung besonderer Kategorien personenbezogener Daten (Gesundheitsdaten)

Die Verarbeitung personenbezogener Daten ist von der Verarbeitung besonderer Kategorien personenbezogener Daten zu unterscheiden. Beim Patienten erhobene Gesundheitsdaten fallen im zahnärztlichen Berufsalltag in diese besondere Kategorie.

Werden Gesundheitsdaten zur Durchführung eines Behandlungsvertrags verarbeitet, bedarf es keiner ausdrücklichen Einwilligung des Patienten in die Datenverarbeitung und somit auch keiner besonderen Nachweislegung. Die Verarbeitung der Gesundheitsdaten darf aber nur durch den Berufsgeheimnisträger oder durch unter seiner/ihrer Verantwortung tätiges Personal erfolgen (Art. 9 Abs. 2 lit. h und Abs. 3 DSGVO, § 22 Abs. 1 Nr. 1 b BDSG-neu).

Ist eine Verarbeitung von Gesundheitsdaten im Rahmen einer Behandlung erfolgt, bedeutet dies nicht, dass die Daten auch für andere Zwecke wie z. B. Werbung verwendet werden können. Erfolgt die Verarbeitung nicht zur Durchführung eines Behandlungsvertrages, sondern z. B. in der Form der Übermittlung an Dritte (z. B. an private Krankenversicherungen oder Seniorenheime), ist die Einholung einer Einwilligung erforderlich (vgl. B.II.1.).

Ist eine Einwilligung im Zusammenhang mit anderen Sachverhalten erfolgt (z. B. wird auf dem Anamnesebogen zugleich die Einwilligung zur Weitergabe von Gesundheitsdaten an ein Abrechnungsunternehmen erklärt), ist eine drucktechnische Hervorhebung der unterschiedlichen Inhalte zu empfehlen.

Im Falle der Datenübermittlung an einen Dritten zu Abrechnungszwecken muss auch weiterhin eine schriftliche Einwilligung des Patienten sowie eine Entbindungserklärung von der zahnärztlichen Schweigepflicht erfolgen (§ 10 Abs. 6 der Gebührenordnung für Zahnärzte).

3. Umsetzung von technischen und organisatorischen Maßnahmen

Rechtmäßig ist die Datenverarbeitung nur, wenn der Verantwortliche *„unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um[setzt], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt"* (Art. 24 Abs. 1 DSGVO). Weitere Konkretisierungen des Art. 24 DSGVO finden sich in Art. 32 DSGVO, welcher umfangreiche technische und organisatorische Maßnahmen auflistet.

Ergänzend dazu fordert § 22 Abs. 2 BDSG-neu zusätzlich vom Verantwortlichen *„angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person"*. Zu diesen Maßnahmen können u. a. gehören:

- Technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt
- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind
- Sensibilisierung der an Verarbeitungsvorgängen Beteiligten
- Benennung einer/eines Datenschutzbeauftragten (nähere Ausführungen unter B.III.2)
- Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern
- Pseudonymisierung und Verschlüsselung personenbezogener Daten im Falle rechtmäßiger Datenweitergabe an Dritte

III. WEITERE DATENSCHUTZRECHTLICHE PFLICHTEN DES VERANTWORTLICHEN

1. Verzeichnis von Verarbeitungstätigkeiten

Auch nach der bisherigen Rechtslage war der Verantwortliche zur Führung eines Verfahrensverzeichnisses verpflichtet (§ 4 g Abs. 2 und 2 a BDSG-alt). Art. 30 DSGVO verpflichtet den Verantwortlichen und ggf. seinen Vertreter, ein Verzeichnis **aller** Verarbeitungstätigkeiten zu führen. Die erstmalige Erstellung bzw. Aktualisierung eines vorhandenen Verzeichnisses bedeutet zunächst einmal eine Bestandsaufnahme aller Verarbeitungstätigkeiten (z. B. Behandlungsdokumentation, Buchhaltungssoftware, elektronische Terminvergabe, E-Mail-Programm, Personalangelegenheiten) anzufertigen. Es ist zu empfehlen, auf das bestehende Verarbeitungsverzeichnis zurückzugreifen und sich sodann einen Überblick zu verschaffen, bei welchen Abläufen welche Daten verarbeitet werden. In der zahnmedizinischen Einrichtung werden Daten primär im Empfangsbereich, aber auch im Behandlungsraum, im Röntgenraum sowie bei der Beauftragung eines Labors verarbeitet. Nicht zu vergessen ist dabei, dass auch bei der beruflichen Nutzung von Smartphones, Laptops und Tablets möglicherweise eine Datenverarbeitung erfolgt.

Das Verzeichnis muss schriftlich oder elektronisch geführt werden und auf Nachfrage der Aufsichtsbehörde (Kontaktdaten am Ende dieses Beitrages) zur Verfügung gestellt werden. Ein nicht vollständig oder nicht geführtes Verfahrensverzeichnis kann mit einem Bußgeld sanktioniert werden. Zwar ist bei Betrieben unter 250 Mitarbeitern eine Ausnahme von der Pflicht zur Führung eines Verarbeitungsverzeichniseses vorgesehen, die Ausnahme betrifft aber nicht den Bereich der Verarbeitung von Gesundheitsdaten (§ 30 Abs. 5 DSGVO). **In zahnmedizinischen Einrichtungen ist daher stets ein Verzeichnis über die Verarbeitungstätigkeiten zu erstellen.**

Welche Angaben im Verzeichnis zu vermerken sind, finden sich insbesondere in Art. 30 Abs. 1 DSGVO:

- Den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- die Zwecke der Verarbeitung (z. B. Lohnabrechnung)
- eine Beschreibung der Kategorien betroffener Personen (z. B. Patient oder Mitarbeiter) und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (z. B. Kassenzahnärztliche Vereinigung, Sozialversicherungsträger), einschließlich Empfänger in Drittländern oder internationalen Organisationen
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (z. B. Aufbewahrungsfristen nach § 630 f Abs. 3 BGB, § 28 Abs. 3 S. 2 und 3 RöV)
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO

Ein **Muster-Verfahrensverzeichnis** wird auf Seite 167 sowie über die Internetpräsenz der ZÄK Nordrhein unter www.zahnaerztekammernordrhein.de/fuer-die-praxis-beruf-wissen/datenschutz/ bereitgestellt. Darüber hinaus hat auch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI) ein **Muster-Verfahrensverzeichnis** nebst **Ausfüllhinweisen** zur Verfügung gestellt.

Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen auf das Kurzpapier **Nr. 1** der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK). Ein Link für den Abruf des Kurzpapiers **Nr. 1 sowie aller Kurzpapiere** über die LDI wird am Ende des Artikels angegeben.

2. Datenschutzbeauftragter

Ob und in welchen Fällen ein Datenschutzbeauftragter zu benennen ist, richtet sich sowohl nach Art. 37 Abs. 1 lit. c DSGVO als auch nach § 38 BDSG-neu.

„10-Personen-Regel“

Unabhängig von den noch nachfolgend zu erläuternden Merkmalen „Kerntätigkeit“ und „umfangreich“, ist vorab festzuhalten, dass ein Datenschutzbeauftragter gemäß § 38 Abs. 1 S. 1 BDSG-neu immer zu benennen ist, soweit der Verantwortliche in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Bei der Berechnung der Personenzahl werden alle Personen mitgezählt, die tatsächlich auf die automatisierte Datenverarbeitung zugreifen. Darunter fallen in der Regel alle Mitarbeiter (auch Auszubildende und Halbtagskräfte) einer zahnmedizinischen Einrichtung, ausgenommen z. B. einer Reinigungskraft. Ob der Verantwortliche bei der „10-Personen-Regel“ mitgezählt wird, ist derzeit noch unklar. Eine Stellungnahme der LDI steht aus. Die „10-Personen-Regel“ gilt unabhängig von der Form der zahnmedizinischen Einrichtung (Einzelpraxis, Praxisgemeinschaft, Berufsausübungsgemeinschaft, Medizinisches Versorgungszentrum).

Werden in einer zahnmedizinischen Einrichtung hingegen **weniger als zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, sind die nachfolgenden zwei Punkte zu beachten:

„Kerntätigkeit“
Ein Datenschutzbeauftragter ist gemäß Art. 37 Abs. 1 lit. c DSGVO dann zu benennen, wenn die „Kerntätigkeit“ des Verantwortlichen in der „umfangreichen“ Verarbeitung von Gesundheitsdaten besteht. Zu der „Kerntätigkeit“ zählen sämtliche Tätigkeiten, bei denen die Datenverarbeitung einen untrennbaren Bestandteil der Haupttätigkeit ausmacht. Zur Kerntätigkeit der Zahnärzteschaft zählt neben der Behandlung von Patienten auch die Verarbeitung von Gesundheitsdaten. Zur Führung einer Behandlungsdokumentation ist ein Heilberufler rechtlich verpflichtet (u. a. § 630 f BGB und § 3 Abs. 3 der Berufsordnung der ZÄK Nordrhein).

Das Merkmal der „Kerntätigkeit“ dürfte daher dem Grunde nach immer zu bejahen sein. Ob ein Datenschutzbeauftragter im konkreten Fall zu benennen ist, hängt aber zusätzlich davon ab, ob eine Verarbeitung von Gesundheitsdaten „umfangreich“ ist.

Das Tatbestandsmerkmal **„umfangreich“** ist von den Normgebern nicht näher konkretisiert worden, sodass derzeit noch umstritten ist, wann das Merkmal zu bejahen ist. Zur Beantwortung der Frage, wann eine Datenverarbeitung „umfangreich“ ist, wird der sogenannte Erwägungsgrund 91 der DSGVO herangezogen, der folgende Anknüpfungspunkte nennt:

- Verarbeitung großer Mengen personenbezogener Daten (Volumen)
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt)
- betrifft eine große Anzahl von Personen (Bezugsgröße)
- Dauer der Verarbeitung (zeitlicher Aspekt)

Die Angaben im Erwägungsgrund 91 tragen zu einer Beantwortung der Frage, wann eine „umfangreiche“ Datenverarbeitung vorliegt, leider nicht bei. Einzig der Leitlinie WP 243 der sogenannten „Artikel-29-Datenschutzgruppe“ (ein unabhängiges Beratungsgremium der EU) ist folgende Erwägung zu entnehmen: Eine Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines Krankenhauses ist „umfangreich“, die Verarbeitung von Patientendaten durch einen einzelnen (Zahn-)Arzt in der Regel hingegen nicht. Konkretere Angaben für den Einzelfall sind letztlich aber nicht möglich. Ausführungen der datenschutzrechtlichen Aufsichtsbehörde in NRW liegen aktuell nicht vor. Einschlägige Rechtsprechung bleibt ebenfalls abzuwarten.

Bezugnehmend auf die vorgenannte Leitlinie unterliegen jedenfalls in Einzelpraxis tätige Zahnärzte und Zahnärztinnen in der Regel nicht dem Merkmal der „umfangreichen“ Datenverarbeitung. Heilberufsträger, die sich lediglich organisatorisch zusammengeschlossen haben (Praxisgemeinschaft), dürften auch nicht unter das Merkmal „umfangreich“ fallen.

Ob Verantwortliche, die in Berufsausübungsgemeinschaften (Gemeinschaftspraxen), Partnerschaften oder auch Medizinischen Versorgungszentren tätig sind, einen Datenschutzbeauftragten aufgrund einer „umfangreichen“ Verarbeitung benennen müssen, ist nach aktuellem Stand aus den vorgezeichneten Gründen unklar und umstritten. Die Zahnärztekammer Nordrhein rät ihren Mitgliedern, sich im Zweifel an die zuständige Aufsichtsbehörde zu wenden. Die Kontaktdaten finden sich am Ende dieses Beitrags.

> Unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ist im Übrigen ein Datenschutzbeauftragter zu benennen, wenn eine Datenschutz-Folgenabschätzung durchzuführen ist. Nähere Erläuterungen dazu folgen unter B.III.3.

Ist aufgrund der vorherigen Erläuterungen ein **Datenschutzbeauftragter durch den Verantwortlichen zu benennen**, wird auf folgende Punkte hingewiesen:

- Der Verantwortliche kann auch nach neuem Recht nicht selber als Datenschutzbeauftragter fungieren.
- Es kann ein interner oder ein externer Datenschutzbeauftragter benannt werden, Art. 37 Abs. 6 DSGVO.
- Wird ein Datenschutzbeauftragter benannt, sind seine/ihre Kontaktdaten der zuständigen Aufsichtsbehörde mitzuteilen, Art. 37 Abs. 7 DSGVO. Die in Nordrhein-Westfalen für den Datenschutz zuständige Aufsichtsbehörde ist die **Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI)**, deren Kontaktdaten am Ende des Beitrages aufgelistet werden.

Die wahrzunehmenden Aufgaben sowie die Qualifikationsvoraussetzungen des Datenschutzbeauftragten richten sich nach Art. 37 Abs. 5 und 39 Abs. 1 DSGVO. Der Datenschutzbeauftragte ist hiernach auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzrechtspraxis zu benennen. Welche Mindestqualifikationen ein Datenschutzbeauftragter aufweisen muss, ist vom Normgeber nicht näher bestimmt worden. Festzuhalten ist dennoch, dass ein Datenschutzbeauftragter die vorgenannten Fähigkeiten besitzen muss, um die nachfolgend aufgeführten Mindestaufgaben erfüllen zu können (Art. 39 DSGVO):

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Datenverarbeitungen durchführen, hinsichtlich ihrer datenschutzrechtlichen Pflichten
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz

personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO
- Zusammenarbeit mit und Anlaufstelle für die Aufsichtsbehörde

Der Verantwortliche hat den Datenschutzbeauftragten bei seiner Aufgabenerfüllung zu unterstützen und muss insbesondere

- sicherstellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
- den Datenschutzbeauftragten unterstützen, z. B. in Form von Zurverfügungstellung der für die Erfüllung der Aufgaben sowie der zur Erhaltung des Fachwissens erforderlichen Ressourcen und Zugangsgewährung zu personenbezogenen Daten und Verarbeitungsvorgängen.
- sicherstellen, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der höchsten Managementebene des Verantwortlichen.

Hinzuweisen ist letztlich auf einen besonderen Kündigungsschutz des internen Datenschutzbeauftragten (§ 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG-neu).

Die grundsätzliche Pflicht zur Einhaltung datenschutzrechtlicher Bestimmungen entfällt nicht, wenn kein Datenschutzbeauftragter zu benennen ist.

Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen auf das Kurzpapier **Nr. 12** der DSK. Zudem wird auf das Informationsblatt der LDI **„Häufig gestellte Fragen zum Datenschutzbeauftragten“** unter www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Datenschutzbeauftragte_nach_der_DS-GVO_und_der_JI-RL/Inhalt/FAQ_zum_Datenschutzbeauftragten/FAQ_ein_Dokument.pdf Bezug genommen.

3. Datenschutz-Folgenabschätzung

Eine wesentliche datenschutzrechtliche Neuerung stellt die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) dar, die in Art. 35 DSGVO normiert ist. Da auch bei einer rechtmäßigen Datenverarbeitung Risiken für die Rechte und Freiheiten der betroffenen Person entstehen können, dient die DSFA der Bewertung von „hohen Risiken“ (Ursache, Art, Besonderheiten und Schwere) im Zusammenhang mit Datenverarbeitungsvorgängen. Nach Auswertung der Ergebnisse sollen geeignete Maßnahmen zur Risikominimierung ergriffen werden.

Bei der Verarbeitung von Gesundheitsdaten geht der Normgeber grundsätzlich von einem abstrakten Risiko für die Rechte und Freiheiten der Patienten aus, wenn sie **„umfangreich“** sind. Eine DSFA ist daher immer in einer zahnmedizinischen Einrichtung durchzuführen, wenn eine „umfangreiche“ Verarbeitung von Gesundheitsdaten erfolgt. Wie bereits unter Punkt B.III.2 erläutert, besteht keine Einigkeit darüber, wann von einer „umfangreichen“ Verarbeitung auszugehen ist. In der Regel gilt die Datenverarbeitung beim Betrieb einer Einzelpraxis und auch einer Praxisgemeinschaft nicht als „umfangreich“, sodass eine DSFA nicht erfolgen muss. Gleichwohl müssen auch in einem solchen Fall selbstverständlich die datenschutzrechtlichen Bestimmungen eingehalten werden. Wegen der aktuellen Unbestimmtheit des Begriffs „umfangreich“ ist jedem Verantwortlichen anzuraten, eigenverantwortlich die Erforderlichkeit einer DSFA zu prüfen und das Prüfungsergebnis zu dokumentieren. Hilfestellung kann die Aufsichtsbehörde geben, da diese auch eine Beratungsfunktion hat.

Die Aufsichtsbehörde erstellt und veröffentlicht eine Liste von Verarbeitungsvorgängen, für die eine DSFA erforderlich bzw. nicht erforderlich ist (Art. 35 Abs. 4 und 5 DSGVO). Nach bisherigem Stand hat die LDI eine solche Liste aber noch nicht veröffentlicht.

Folgende Punkte wären jedoch zumindest in einer DSFA zu berücksichtigen:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese datenschutzrechtlichen Bestimmungen eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Liegt eine „umfangreiche“ Verarbeitung von Gesundheitsdaten vor, hat die DSFA zu erfolgen und es ist gemäß § 38 Abs. 1 S. 2 BDSG-neu zwingend und unabhängig von der „10-Personen-Regel“ (vgl. B.III.2) ein Datenschutzbeauftragter zu benennen.

Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen auf das Kurzpapier **Nr. 5** der DSK. Die DSK hat zudem angekündigt, ein Kurzpapier zum Begriff des Risikos veröffentlichen zu wollen.

C. FAZIT

Für den Verantwortlichen einer zahnmedizinischen Einrichtung ist es wichtig, sich mit den Neuerungen des Datenschutzrechts umfassend vertraut zu machen und die bisherigen Datenverarbeitungsprozesse in der zahnmedizinischen Einrichtung einer kritischen Prüfung zu unterziehen sowie an das neue Datenschutzrecht anzupassen. Der Datenschutz ist weiterhin Chefsache. Insbesondere ist zu prüfen, ob ein Datenschutzbeauftragter zu benennen ist und ob eine Datenschutz-Folgenabschätzung durchzuführen ist. Darüber hinaus empfiehlt es sich, alle bisher verwendeten Formulare (z. B. Einwilligungserklärungen, Abtretungserklärungen etc.) an die Anforderungen des Datenschutzes anzupassen. Auch sind bestehende Verarbeitungsverzeichnisse zu sichten, ggf. zu aktualisieren und neue zu schaffen.

Nicht unberücksichtigt bleiben darf, dass auch die Mitarbeiter einer zahnmedizinischen Einrichtung für die neuen Vorgaben des Datenschutzes sensibilisiert und geschult werden müssen.

Verschwiegenheitspflichten, die aus der Berufsordnung der ZÄK Nordrhein sowie aus dem Strafgesetzbuch resultieren, sind auch im Rahmen des neuen Datenschutzrechts stets zu berücksichtigen.

Wie eingangs angekündigt, werden in Teil 2 des Artikels (Ausgabe 4/2018 des Rheinischen Zahnärzteblatts) weitere Erläuterungen und Hilfestellungen sowohl zu den Informationspflichten des Zahnarztes, zu den Rechten der betroffenen Personen, zur Auftragsdatenverarbeitung als auch zu den Folgen bei Verstößen gegen das Datenschutzrecht erfolgen.

Zusätzliche Informationen und aktuelle Entwicklungen zum Datenschutzrecht werden zudem bereits jetzt auf der Webseite der Zahnärztekammer Nordrhein unter www.zahnaerztekammernordrhein.de/fuer-die-praxis-beruf-wissen/datenschutz/ eingestellt werden.

Ass. iur. Katharina Gorontzi, LL.M.
Rechtsabteilung, ZÄK Nordrhein

Ansprechpartner bei der ZÄK Nordrhein

Ass. jur. Katharina Beckmann
Ressortleitung Berufsausübung
Tel. 0211 44704-330
beckmann@zaek-nr.de

Weitere Unterlagen

Für weitere umfassende Erläuterungen verweist die ZÄK Nordrhein auf die vollständige Sammlung der **Kurzpapiere** der DSK, insbesondere auf die Kurzpapiere Nr. 1, 5, 8 und 12 (Stand Februar 2018).
www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Kurzpapiere-der-Datenschutzkonferenz-zur-DS-GVO.html

Die LDI hat ein Muster-**Verfahrensverzeichnis** sowie hilfreiche **Ausfüllhinweise** bereitgestellt.
www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html

Die LDI hat zudem eine **Checkliste** mit den wichtigsten Punkten und Fragen zur Vorbereitung auf das neue Datenschutzrecht veröffentlicht.
www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Checkliste-fuer-KMU-zur-DS-GVO_LDI-NRW.pdf

Kontaktdaten der in NRW für den Datenschutz zuständigen Aufsichtsbehörde
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44 | 40102 Düsseldorf
Tel. 0211 38424–0 | Fax 0211 38424–10
poststelle@ldi.nrw.de

Übersicht der wichtigsten datenschutzrechtlichen Begrifflichkeiten

(in alphabetischer Reihenfolge)

AUFTRAGSVERARBEITER – ART. 4 NR. 8 DSGVO
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

BETROFFENE PERSON – ART. 4 NR. 1 DSGVO
Eine identifizierte oder identifizierbare natürliche Person.

BDSG-ALT
Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I. S. 66 vom 24.01.2003). Tritt am 25.05.2018 außer Kraft.

BDSG-NEU
Bundesdatenschutzgesetz. Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Anpassung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU). Das Gesetz wurde am 30.06.2017 verkündet (BGBl. I. S. 2132 vom 05.07.2017) und tritt am 25.05.2018 in Kraft.

BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN – ART. 9 DSGVO
Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

DSFA – ART. 35 DSGVO
Datenschutz-Folgenabschätzung.

DSGVO
Datenschutzgrundverordnung. Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119, S. 1).

DSK
Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

EINWILLIGUNG – ART. 4 NR. 11 DSGVO
Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

GESUNDHEITSDATEN – ART. 4 NR. 12 DSGVO
Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

LDI
Aufsichtsbehörde. Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

PERSONENBEZOGENE DATEN – ART. 4 NR. 1 DSGVO
Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

VERANTWORTLICHER – ART. 4 NR. 7 DSGVO
„Verantwortlicher“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werde.

VERARBEITUNG – ART. 4 NR. 2 DSGVO
Jeder – mit oder ohne Hilfe automatisierter Verfahren – ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Muster-Verfahrensverzeichnis gemäß Artikel 30 Datenschutzgrundverordnung (DSGVO)

Wichtiger Hinweis der Zahnärztekammer Nordrhein

Die Zahnärztekammer Nordrhein bietet ihren Mitgliedern ein Muster-Verfahrensverzeichnis gemäß Artikel 30 DSGVO zur Verwendung in der eigenen zahnmedizinischen Einrichtung an. **Das Muster erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit, sondern gibt lediglich unverbindliche Anhaltspunkte für ein mögliches Verfahrensverzeichnis.** Bitte beachten Sie, dass das Muster-Verfahrensverzeichnis eine individuelle Rechtsberatung oder Rücksprache mit der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen nicht ersetzen kann und die Zahnärztekammer Nordrhein daher **keine Haftung** übernimmt.

Verzeichnis der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO	*(Name, Kontaktdaten)*
Ggf. gemeinsamer Verantwortlicher	*(Name, Kontaktdaten)*
Interner oder externer Datenschutzbeauftragter, sofern gemäß Art. 37 DSGVO benannt	*(Name, Kontaktdaten)*
Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit	*Allgemeine Bezeichnung der dokumentierten Verarbeitungstätigkeit* ***z. B.:*** • *„Dokumentation der Behandlung“* • *„E-Mail-Verarbeitung“* • *„Lohn- und Gehaltsabrechnung“*
Zweckbestimmung	***z. B.:*** • *Verarbeitungstätigkeit: „Dokumentation der Behandlung“* → *Zweckbestimmung: sachgerechte therapeutische Behandlung und Weiterbehandlung; Erfüllung gesetzlicher Pflichten* • *Verarbeitungstätigkeit: „E-Mailverarbeitung“* → *Zweckbestimmung: Durchführung der elektronischen Kommunikation* • *Verarbeitungstätigkeit: „Lohn- und Gehaltsabrechnung“* → *Zweckbestimmung: Erstellung der Lohnabrechnung; Erfüllung gesetzlicher Pflichten* *Es können auch mehrere Zweckbestimmungen für eine Verarbeitung angegeben werden.*
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	***z. B.:*** • *Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7 DSGVO)* • *Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit. f DSGVO)* • *Verarbeitung besonderer Kategorien personenbezogener Daten, Gesundheitsdaten auf der Grundlage eines Behandlungsvertrages (Art. 9 Abs. 2 lit. h DSGVO)*
Erhebung der Daten	
Betroffene Personengruppen	***z. B.:*** *Patienten, Mitarbeiter, Bewerber*
Beschreibung der Datenkategorien/Art der gespeicherten Daten	***z. B.:*** • *Gesundheitsdaten (besondere Kategorien personenbezogener Daten)* • *Bankverbindungsdaten/Kreditkartendaten* • *Lohn- und Gehaltsdaten* • *Name/Vorname/Anrede/Titel, Geburtsdatum, Adressdaten* • *Sozialversicherungsdaten* • *Vertragsdaten* • *Zeiterfassungsdaten*
Herkunft der Daten:	*Woher stammen die Daten? Von Betroffenen selbst oder von einem Dritten?*

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der Einrichtung des Verantwortlichen)	***z. B.:*** *Personalabteilung, Buchhaltung, Auftragsverarbeiter*
Externe Empfänger und Dritte, soweit nicht Auftragsverarbeiter	***z. B.:*** *Kassenzahnärztliche Vereinigung, Krankenkasse, Steuerberater.*
Datenübermittlung in Drittstaaten/internationale Organisationen (z. B. Cloud-Dienste)	
Datenübermittlung in Drittstaaten	*Die Übermittlung von personenbezogenen Daten in Drittländer ist ausschließlich zulässig, wenn neben der Rechtmäßigkeit der Datenverarbeitung weiterführend das durch die DSGVO gewährleistete Schutzniveau in dem jeweiligen Drittland nicht untergraben wird (Art. 44 DSGVO).*
Angemessenes Datenschutzniveau durch	• *Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO oder* • *Garantien gem. Art. 46 DSGVO* - *Verbindliche interne Datenschutzvorschriften (BCR)* - *EU-Standardvertrag* *Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. Abs. 2 DSGVO)*
Fristen für die Löschung der verschiedenen Datenkategorien	
Speicherdauer, Fristen	***z. B.:*** *§ 630 f Abs. 3 BGB (Behandlungsdokumentation), § 28 Abs. 3 RöV*
Beurteilung der Angemessenheit technischer und organisatorischer Maßnahmen (TOM)	
Wenn möglich: Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 DSGVO) und des etwaigen verbleibenden Risikos unter Berücksichtigung der eingesetzten TOM	*Maßnahmen müssen unter anderem Folgendes einschließen:* • *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;* • *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen;* • *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;* • *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.* *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zweck der Datenverarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche geeignete TOM, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO).*
Prüfung durch den Verantwortlichen	
Prüfung	*Erfolgt/nicht erfolgt*
Datum, Unterschrift	

Das neue Datenschutzrecht kommt zum 25. Mai 2018

WICHTIG: RELEVANTE REGELUNGEN UND GESETZLICHE NEUERUNGEN FÜR DIE ZAHNÄRZTLICHE PRAXIS – TEIL 2

In der Ausgabe 3/2018 des Rheinischen Zahnärzteblatts hat die Zahnärztekammer (ZÄK) Nordrhein ihre Mitglieder über die relevanten rechtlichen Neuerungen im Datenschutzrecht zum 25. Mai 2018 informiert. Es wurden der Adressat der datenschutzrechtlichen Bestimmungen, die Begrifflichkeiten zur Verarbeitung von personenbezogenen Daten, die Pflicht zur Führung von Verarbeitungsverzeichnissen sowie die Benennung eines Datenschutzbeauftragten erläutert. Teil 2 des Artikels wird weitere Erläuterungen und Hilfestellungen zum neuen Datenschutzrecht geben.

Unter B.III. (RZB 3/2018, S. 163) wurden bereits die datenschutzrechtlichen Pflichten des Verantwortlichen wie das Führen eines Verarbeitungsverzeichnisses sowie die Benennung eines Datenschutzbeauftragten erläutert. Neben diesen Pflichten treffen den Verantwortlichen zusätzliche Pflichten, die nachfolgend erläutert werden.

4. Informationspflichten

Neu ist, dass **gegenüber der betroffenen Person** (z. B. Patient, Mitarbeiter) künftig **umfangreiche abstrakte Informationspflichten** über die Datenverarbeitung bestehen (Art. 13 DSGVO) und zwar ohne konkretes Anfragebegehren der betroffenen Person. Die Informationspflichten dienen der Datentransparenz und sind neben den noch zu erläuternden Auskunftsrechten der betroffenen Person (vgl. B.III.5) vom Verantwortlichen zu erfüllen. **Zum Zeitpunkt der Datenerhebung** (z. B. bei Neuaufnahme des Patienten oder Neueinstellung eines Mitarbeiters) muss der Verantwortliche der betroffenen Person Folgendes **unentgeltlich** und grundsätzlich **schriftlich** oder **elektronisch** mitteilen:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten
- Zwecke der Datenverarbeitung (z. B. Erfüllung des Behandlungsvertrags, Lohnbuchhaltung)
- Rechtsgrundlage für die Verarbeitung (z. B. § 630 a und f BGB)
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (z. B. Kassenzahnärztliche Vereinigung, Sozialversicherungsträger)
- ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln (z. B. Cloud-Dienste)
- Dauer der Datenspeicherung oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (z. B. Aufbewahrungsfristen nach § 630 f Abs. 3 BGB, § 28 Abs. 3 S. 2 und 3 RöV)
- Rechte der betroffenen Person auf Auskunft, Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit
- Recht der betroffenen Person, eine erklärte Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte
- sofern einschlägig: das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (in der zahnmedizinischen Einrichtung in der Regel nicht einschlägig)

Die betroffene Person muss „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ über die vorstehenden Punkte informiert werden (Art. 12 Abs. 1 DSGVO). Ein bloßer Aushang in den Räumen der zahnmedizinischen Einrichtung oder ein Verweis auf die eigene Internetpräsenz ist nicht ausreichend und kann allenfalls ergänzend erfolgen. Es empfiehlt sich, der betroffenen Person bei Datenerhebung ein allgemein verfasstes Informationspapier im vorgenannten Umfang zu überreichen und sich gegenzeichnen zu lassen.

Es empfiehlt sich zudem, jeden Betroffenen ab dem 25.05.2018 erstmalig nach den vorgezeichneten Grundsätzen zu informieren. Eine Wiederholung ist anschließend bei unveränderten Bedingungen nicht erforderlich (Art. 13 Abs. 4 DSGVO). Die Informationspflicht kann zudem im Rahmen der Dritterhebung von personenbezogenen Daten entfallen (Art. 14 Abs. 5 lit. d DSGVO).

Es ist vom Verantwortlichen zu prüfen, ob vorhandene Datenschutzerklärungen auf der Internetpräsenz der zahnmedizinischen Einrichtung angepasst werden müssen.

Ein **Muster zu den Informationspflichten** wird auf Seite 255sowie über die Internetpräsenz der ZÄK Nordrhein unter www.zahnaerztekammernordrhein.de/fuer-die-praxis-beruf-wissen/datenschutz/ bereitgestellt. Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen auf das Kurzpapier **Nr. 10** der DSK. Ein Link für den Abruf des Kurzpapiers **Nr. 10 sowie aller Kurzpapiere** über die LDI wird am Ende des Artikels angegeben.

5. Auskunftsrechte

Neben den vorgenannten abstrakten Informationspflichten des Verantwortlichen hat die betroffene Person ein Auskunftsrecht gegenüber dem Verantwortlichen. Der Verantwortliche hat **unentgeltlich** in **schriftlicher** oder **elektronischer** Form **spätestens binnen eines Monats** nach Anfrage der betroffenen Person eine Kopie der konkreten personenbezogenen Daten, die Gegenstand der Verarbeitung sind, der betroffenen Person zur Verfügung zu stellen (Art. 12 Abs. 3 i.V.m. Art. 15 Abs. 3 DSGVO).

Der Umfang des Auskunftsrechts ist ausweislich des Kurzpapiers **Nr. 6** der DSK wie folgt zu bestimmen:

„Nach Art. 15 Abs. 1 DSGVO steht der betroffenen Person ein abgestuftes Auskunftsrecht zu. Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Auch eine Negativauskunft ist erforderlich, wenn der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat. Zum anderen kann die betroffene Person ganz konkret Auskunft darüber verlangen, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).“

Folgende Auskünfte sind – je nach Auskunftsbegehren der betroffenen Person – zu tätigen:

- Verarbeitungszwecke (z. B. zur Durchführung des Behandlungs-, Arbeits- oder Dienstleistungsvertrages)
- Kategorien personenbezogener Daten, die verarbeitet werden (z. B. Gesundheitsdaten)
- Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen (z. B. Kassenzahnärztliche Vereinigung, Sozialversicherungsträger)
- die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (z. B. Aufbewahrungsfristen nach § 630 f Abs. 3 BGB, § 28 Abs. 3 S. 2 und 3 RöV)
- Betroffenenrechte hinsichtlich Berichtigung, Löschung oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
- Beschwerderecht bei einer Aufsichtsbehörde
- alle verfügbaren Informationen über die Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden
- sofern einschlägig: das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (in der zahnmedizinischen Einrichtung in der Regel nicht einschlägig).

Unklar ist derzeit noch, ob von dem Auskunftsrecht auch das **Recht des Patienten auf Einsichtnahme in die Behandlungsdokumentation** (§ 630 g BGB) umfasst wird. Dem Grunde nach ist § 630 g BGB neben dem Auskunftsrecht gemäß Art. 15 DSGVO anwendbar, die Normen widersprechen sich aber hinsichtlich des Herausgabezeitpunktes und der Kostentragung. Es bleibt daher abzuwarten, wie künftig der Zeitpunkt der Herausgabe sowie die Frage der Kostentragung in der Praxis umgesetzt und juristisch bewertet werden wird.

Ausnahmen vom Auskunftsrecht der betroffenen Person sind im BDSG-neu an verschiedenen Stellen zwar normiert, bestehen jedoch in der Regel in einer zahnmedizinischen Einrichtung nicht. Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen zu bestehenden Auskunftsrechten auf das Kurzpapier **Nr. 6** der DSK.

6. Sonstige Rechte der betroffenen Personen

Neben dem Recht auf Auskunft haben betroffene Personen auch das Recht auf **Berichtigung** (Art. 16 DSGVO) sowie auf **Einschränkung/Sperrung** der Datenverarbeitung (Art. 18 DSGVO).

Art. 17 DSGVO gewährt zudem ein Recht auf **Löschung** („Recht auf Vergessenwerden“), dem jedoch gesetzliche Aufbewahrungsfristen (z. B. § 630 f Abs. 3 BGB, § 28 Abs. 3 S. 2 und 3 RöV) entgegenstehen können (Art. 17 Abs. 3 DSGVO, § 35 Abs. 3 BDSG-neu). In einem solchen Falle kann zwar eine erbetene Löschung nicht erfolgen, wohl aber eine **Einschränkung/Sperrung** der Verarbeitung. Die ZÄK Nordrhein verweist für weitere

Informationen und Erläuterungen auf das Kurzpapier **Nr. 11** der DSK. Eine Übersicht der wesentlichen Aufbewahrungspflichten wird auf Seite 256 abgedruckt.

Erwähnenswert ist zudem das mit Art. 20 DSGVO eingeführte **Recht des Betroffenen auf Datenübertragbarkeit**, welches insbesondere beim Wechsel des Mitarbeiters einer zahnmedizinischen Einrichtung in Betracht kommen kann. Danach hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie hat das Recht, dass diese Daten durch den Verantwortlichen einem anderen Verantwortlichen ohne Behinderung unentgeltlich übermittelt werden. Folgende drei Voraussetzungen für das Recht auf Datenübertragbarkeit müssen nebeneinander erfüllt sein:

- Die personenbezogenen Daten wurden dem Verantwortlichen durch die betroffene Person selbst bereitgestellt,
- die Verarbeitung erfolgt
  - auf der Grundlage einer erklärten Einwilligung gemäß Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO oder
  - auf der Grundlage eines Vertrages gemäß Art. 6 Abs. 1 lit. b DSGVO,
- die Verarbeitung erfolgt mithilfe automatisierter Verfahren.

7. Auftragsverarbeitung

Neue Regelungen zur Auftragsverarbeitung finden sich in Art. 28 DSGVO sowie in § 62 BDSG-neu. Ein **Auftragsverarbeiter** ist nach Art. 4 Nr. 8 DSGVO *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“*. Auch die bisherige Rechtslage sah in § 11 BDSG-alt den Einsatz eines Auftragsdatenverarbeiters (z. B. Wartung der EDV-Systeme, Lohnabrechnung) und – in engen Grenzen – die Möglichkeit der Funktionsübertragung (z. B. Outsourcing) vor.

Grundsätzlich ist nunmehr zwar in weiterem Umfang als bisher der Einsatz von Dienstleistern als Auftragsverarbeiter möglich. Der **Verantwortliche** bleibt aber bei Beauftragung eines Dienstleisters auch weiterhin in der Pflicht, die bereits dargestellten datenschutzrechtlichen Bestimmungen einzuhalten, und unterliegt zudem Kontroll- und Dokumentationspflichten (Art. 32 Abs. 1 lit. d DSGVO).

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich **auf Weisung** des Verantwortlichen verarbeiten (Art. 29 DSGVO). Darüber hinaus bedarf die Beauftragung eines Dienstleisters zwingend eines Vertrages in schriftlicher oder elektronischer Form und muss die Mindestanforderungen des Art. 29 Abs. 3 DSGVO erfüllen. Bestehende Verträge können weiterhin Bestand haben, soweit sie den Anforderungen der DSGVO entsprechen. Als Beispiele für die Beauftragung externer Dienstleister im Rahmen einer Auftragsverarbeitung sind zu nennen: EDV-Wartungen, Lohn- und Gehaltsabrechnungen, Honorarabrechnungen, Marketingmaßnahmen, Vernichtung von Unterlagen etc. Nicht darunter dürfte hingegen in der Regel die Beauftragung eines gewerblichen Dentallabors fallen. Bei der Beauftragung des Dentallabors handelt es sich „im Kern“ um die Herstellung von Zahnersatz und nicht um die Durchführung bestimmter Datenverarbeitungsvorgänge im Auftrag. Gleichwohl bleibt eine Stellungnahme der LDI abzuwarten. Zumindest dürfte im Übrigen eine Übermittlung der Daten durch Art. 9 Abs. 2 lit. h DSGVO gedeckt sein.

> Auch beim Einsatz von Auftragsverarbeitern sind die Bestimmungen der Berufsordnung der ZÄK Nordrhein als auch des § 203 StGB zur zahnärztlichen Verschwiegenheitspflicht zwingend zu berücksichtigen (§ 1 Abs. 2 S. 3 BDSG-neu).

Bei datenschutzrechtlichen Verstößen kann der Verantwortliche sowie der Auftragsverarbeiter in die **Haftung** genommen werden (Art. 82 Abs. 1 DSGVO). Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen auf das Kurzpapier **Nr. 13** der DSK.

8. Beschäftigtendatenschutz

In Ergänzung zu den zuvor erwähnten Datenschutzrechten der Mitarbeiter einer zahnmedizinischen Einrichtung sei hier noch auf einen gesonderten Beschäftigtendatenschutz gemäß § 26 BDSG-neu hingewiesen, der bisher in § 32 BDSG-alt geregelt war. Die ZÄK Nordrhein verweist für ausführlichere Informationen und Erläuterungen zum Beschäftigtendatenschutz auf das Kurzpapier **Nr. 14** der DSK.

IV. HAFTUNG UND SANKTIONEN BEI DATENSCHUTZRECHTLICHEN VERSTÖßEN

1. Sanktionen

Als Aufsichtsbehörde überwacht die LDI die Einhaltung datenschutzrechtlicher Bestimmungen im Anwendungsbereich der DSGVO und des BDSG-neu. Insoweit wurden der LDI neben einem umfangreichen Aufgabenkatalog (Art. 57 DSGVO) zahlreiche Befugnisse zur Einhaltung und Durchsetzung der DSGVO sowie der Betroffenenrechte eingeräumt. Dazu zählen Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse sowie beratende Befugnisse (Art. 58 DSGVO, § 40 Abs. 6 BDSG-neu). Die Aufsichtsbehörde darf den Verantwortlichen sowie den Vertreter anweisen, Informationen zur Aufgabenerfüllung bereitzustellen. Im Rahmen ihrer Befugnisse hat die Aufsichtsbehörde im Übrigen grundsätzlich ein Zutrittsrecht zu den Geschäftsräumen des Verantwortlichen. Ohne Vorlage einer Schweigepflichtentbindungserklärung kann die Aufsichtsbehörde jedoch nicht Einsicht in die Patientendaten nehmen. Die LDI kann ihre Untersuchungsbefugnisse im Hinblick auf die Einhaltung allgemeiner datenschutzrechtlicher Bestimmungen (z. B. Führung des Verarbeitungsverzeichnisses) wahrnehmen.

Stellt die Aufsichtsbehörde Verstöße gegen datenschutzrechtliche Bestimmungen fest, kann sie eine **Geldbuße** bis zu 20 Millionen Euro verhängen. §§ 42 und 43 BDSG-neu beinhalten zudem **Straf-** als auch **Bußgeldvorschriften**.

Datenschutzverstöße sowie Datenverluste sind künftig der LDI durch den Verantwortlichen binnen 72 Stunden nach Bekanntwerden zu melden (Art. 33 DSGVO). Die für die Meldung erforderlichen Informationen finden sich in Art. 33 Abs. 3 DSGVO.

Die ZÄK Nordrhein verweist für weitere Informationen und Erläuterungen auf das Kurzpapier **Nr. 2** der DSK.

2. Haftung

Ausweislich Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen ein Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

D. Fazit

Wie die Erläuterungen und Hinweise zeigen, sind derzeit leider viele Punkte hinsichtlich der Umsetzung des neuen Datenschutzrechts in der täglichen Praxis noch ungewiss, sodass die Verunsicherung der Zahnärzteschaft nachvollziehbar groß ist. Es bleiben weitere Stellungnahmen der DSK und LDI als auch etwaige Rechtsprechung abzuwarten. Wie schon in Teil 1 des Artikels ausgeführt, ist es nunmehr von großer Bedeutung, sich mit den Neuerungen des Datenschutzrechts umfassend vertraut zu machen und die bisherigen Datenverarbeitungsprozesse in der zahnmedizinischen Einrichtung einer kritischen Prüfung zu unterziehen sowie bis zum 25. Mai 2018 an das neue Datenschutzrecht anzupassen. Nicht unberücksichtigt bleiben darf, dass auch die Mitarbeiter einer zahnmedizinischen Einrichtung für die neuen Vorgaben des Datenschutzes sensibilisiert und geschult werden müssen.

Es ist zudem dringend zu empfehlen, alle betroffenen Personen ab dem **25. Mai 2018** erstmalig über die abstrakten Informationspflichten nach Art. 13 DSGVO zu informieren.

Nochmals ist darauf hinzuweisen, dass Verschwiegenheitspflichten, die aus der Berufsordnung der ZÄK Nordrhein sowie aus dem Strafgesetzbuch resultieren, auch im Rahmen des neuen Datenschutzrechts stets zu berücksichtigen sind.

Die ZÄK Nordrhein wird die Entwicklungen im Datenschutzrecht für ihre Mitglieder selbstverständlich beobachten und über solche informieren. Es empfiehlt sich, für zusätzliche Informationen die Webseite der ZÄK Nordrhein regelmäßig unter www.zahnaerztekammernordrhein.de/fuer-die-praxis-beruf-wissen/datenschutz aufzusuchen, da dort insbesondere über aktuelle Entwicklungen im Datenschutzrecht informiert werden wird.

Ass. iur. Katharina Gorontzi, LL.M.
Rechtsabteilung, ZÄK Nordrhein

Ansprechpartner bei der ZÄK Nordrhein
Ass. jur. Katharina Beckmann
Ressortleitung Berufsausübung
Tel. 0211 44704-330
beckmann@zaek-nr.de

Weitere Unterlagen

Für weitere umfassende Erläuterungen verweist die ZÄK Nordrhein auf die vollständige Sammlung der **Kurzpapiere** der DSK, insbesondere auf die Kurzpapiere Nr. 1, 5, 8 und 12 (Stand März 2018).
www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Kurzpapiere-der-Datenschutzkonferenz-zur-DS-GVO.html

Die LDI hat ein Muster-**Verarbeitungsverzeichnis** sowie hilfreiche **Ausfüllhinweise** bereitgestellt.
www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html

Die LDI hat zudem eine **Checkliste** mit den wichtigsten Punkten und Fragen zur Vorbereitung auf das neue Datenschutzrecht veröffentlicht.
www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Checkliste-fuer-KMU-zur-DS-GVO_LDI-NRW.pdf

Kontaktdaten der in NRW für den Datenschutz zuständigen Aufsichtsbehörde
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44 | 40102 Düsseldorf
Tel. 0211 38424–0 | Fax 0211 38424–10
poststelle@ldi.nrw.de

Übersicht der wichtigsten datenschutzrechtlichen Begrifflichkeiten

(in alphabetischer Reihenfolge)

AUFTRAGSVERARBEITER – ART. 4 NR. 8 DSGVO
Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

BETROFFENE PERSON – ART. 4 NR. 1 DSGVO
Eine identifizierte oder identifizierbare natürliche Person.

BDSG-ALT
Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I. S. 66 vom 24.01.2003). Tritt am 25.05.2018 außer Kraft.

BDSG-NEU
Bundesdatenschutzgesetz. Artikel 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Anpassung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU). Das Gesetz wurde am 30.06.2017 verkündet (BGBl. I. S. 2132 vom 05.07.2017) und tritt am 25.05.2018 in Kraft.

BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN – ART. 9 DSGVO
Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

DSFA – ART. 35 DSGVO
Datenschutz-Folgenabschätzung.

DSGVO
Datenschutzgrundverordnung. Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119, S. 1).

DSK
Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

EINWILLIGUNG – ART. 4 NR. 11 DSGVO
Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

GESUNDHEITSDATEN – ART. 4 NR. 12 DSGVO
Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

LDI
Aufsichtsbehörde. Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

PERSONENBEZOGENE DATEN – ART. 4 NR. 1 DSGVO
Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

VERANTWORTLICHER – ART. 4 NR. 7 DSGVO
„Verantwortlicher“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werde.

VERARBEITUNG – ART. 4 NR. 2 DSGVO
Jeder – mit oder ohne Hilfe automatisierter Verfahren – ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Muster-Informationsblatt
gemäß Artikel 13 Datenschutzgrundverordnung (DSGVO)

Wichtiger Hinweis der Zahnärztekammer Nordrhein

Die Zahnärztekammer Nordrhein bietet ihren Mitgliedern ein Muster-Informationsblatt gemäß Artikel 13 DSGVO zur Verwendung in der eigenen zahnmedizinischen Einrichtung an. **Das Muster erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit, sondern gibt lediglich unverbindliche Anhaltspunkte für ein mögliches Informationsblatt.** Bitte beachten Sie, dass das Muster-Informationsblatt eine individuelle Rechtsberatung oder Rücksprache mit der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen nicht ersetzen kann und die Zahnärztekammer Nordrhein daher **keine Haftung** übernimmt.

Datenverarbeiter, Verantwortlicher	
Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters	*Name, Kontaktdaten*
Interner oder externer Datenschutzbeauftragter, sofern gemäß Art. 37 DSGVO benannt	*Name, Kontaktdaten*
Verarbeitungsrahmen	
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung	***z. B.** zur Erfüllung des Behandlungsvertrages sowie zur Dokumentation der Behandlung (§§ 630 a und 630 f BGB); zur Lohnbuchhaltung*
Wenn die Verarbeitung auf Artikel 6 Abs. 1 lit. f DSGVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden	***z. B.** zur Durchsetzung zivilrechtlicher Ansprüche*
Die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten	***z. B.** Kassenzahnärztliche Vereinigung, Krankenkasse, Factoring-Unternehmen*
Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer	***z. B.** 10 Jahre Behandlungsdokumentation (§ 630 f Abs. 3 BGB)*
Die Bereitstellung der personenbezogenen Daten ist gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich.	***z. B.** zur Durchführung der Behandlung erforderlich*
Die betroffene Person ist verpflichtet/nicht verpflichtet, die personenbezogenen Daten bereitzustellen; mögliche Folgen der Nichtbereitstellung	***z. B.** ohne Bereitstellung kann keine Behandlung erfolgen*
Sofern einschlägig: Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person	*Beim sog. Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO werden Daten analysiert und ausschließlich einer automatischen Verarbeitung beruhenden Entscheidung unterworfen (z. B. automatisierte Ablehnung eines Online-Kreditvertrages).* *In der zahnmedizinischen Einrichtung in der Regel nicht einschlägig, so dass das Feld nicht ausgefüllt werden muss.*
Weitergabe und Auslandsbezug	
Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Art. 46 oder Art. 47 DSGVO oder Art. 49 Abs. 1 Unterabs. 2 DSGVO einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.	***z. B.** einschlägig bei der Nutzung von Cloud-Diensten, bei denen regelmäßig eine Datenspeicherung auf Servern im Ausland erfolgt.*
Betroffenenrechte	
Als betroffene Person werden Sie darüber informiert, dass Sie ein Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung bzw. Einschränkung (Art. 18 DSGVO) der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung (Art. 21 DSGVO) sowie des Rechts auf Datenübertragbarkeit (Art. 20 DSGVO) haben. Zudem haben Sie das Recht, die Einwilligung im Sinne von Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Weiter besteht ein Beschwerderecht bei der Aufsichtsbehörde (Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Postfach 20 04 44, 40102 Düsseldorf).	

Zur Kenntnis genommen am: _____ **Unterschrift der betroffenen Person:** _____

Übersicht über Aufbewahrungsfristen mit datenschutzrechtlicher Relevanz

Unterlagen	Aufbewahrungsfrist	Rechtsgrundlage
PATIENTENBEHANDLUNG		
Betäubungsmittelbuch	3 Jahre nach der letzten Eintragung	§ 13 Abs. 3 BtMVV
Betäubungsmittelrezept	3 Jahre	§ 8 Abs. 5 BtMVV
Dokumentation über die zahnärztliche Patientenbehandlung	10 Jahre Achtung: In Ausnahmefällen kann es zu einer Verjährung von Schadensersatzansprüchen erst nach 30 Jahren kommen (§ 199 Abs. 2 BGB). Insofern kann eine Aufbewahrung von 30 Jahren sinnvoll sein.	§ 630 f Abs. 3 BGB (§ 12 Abs. 1 MBO-Zahnärzte)
MITARBEITERUNTERLAGEN UND ARBEITNEHMERSCHUTZ		
Arbeitsmedizinische Vorsorge/Vorsorgekartei	Die Angaben sind bis zur Beendigung des Beschäftigungsverhältnisses aufzubewahren und anschließend in der Regel zu löschen.	§ 3 Abs. 4 ArbMedVV
Arbeitszeitnachweise/ Überstundendokumentation	2 Jahre	§ 16 Abs. 2 ArbZG
Aufzeichnung zu Beschäftigung werdender und stillender Mütter	2 Jahre	§ 27 Abs. 5 MuSchG
Unfallanzeige	5 Jahre	§ 24 Abs. 6 DGUV V1
Verbandbuch	5 Jahre	§ 24 Abs. 6 DGUV V1
Verzeichnis der im Betrieb beschäftigten Jugendlichen	2 Jahre nach der letzten Eintragung	§ 50 Abs. 2 JArbSchG
RÖNTGEN		
Einweisung bei der ersten Inbetriebnahme	für die Dauer des Betriebs	§ 18 Abs. 1 RöV
Mitarbeiterunterweisung	5 Jahre	§ 36 Abs. 4 RöV
Röntgenaufnahmen	10 Jahre nach Abschluss der Behandlung, bei Kindern/Jugendlichen bis zu deren 28. Lebensjahr	§ 28 Abs. 3 RöV
STEUERN*		
Aufzeichnungen steuerlicher Art, Buchungsbelege	10 Jahre	§ 147 Abs.3 AO
Bestell- und Auftragsunterlagen	6 Jahre	§ 147 Abs. 3 AO
Gehaltslisten und -quittungen	10 Jahre	§ 147 Abs. 3 AO
Kassenbücher und -berichte	10 Jahre	§ 147 Abs. 3 AO
Rechnungen	10 Jahre	§ 147 Abs. 3 AO; § 14 b Abs. 1 UStG
Reisekostenabrechnung	6 Jahre	§ 147 Abs. 3 AO

* Die ZÄK Nordrhein empfiehlt in Zweifelsfällen eine Rücksprache mit einem Steuerberater.

(Aufbewahrungsfristen aus dem vertragszahnärztlichen Bereich (z. B. SGB V, BMV-Z, EKV-Z) sind in dieser Tabelle nicht aufgeführt. Zudem erhebt die Übersicht keinen Anspruch auf Vollständigkeit und Richtigkeit.)