

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	<i>(Name, Kontaktdaten)</i>
Ggf. gemeinsamer Verantwortlicher	<i>(Name, Kontaktdaten)</i>
Interner oder externer Datenschutzbeauftragter, sofern gemäß Art. 37 DSGVO benannt	<i>(Name, Kontaktdaten)</i>
Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit	<i>Allgemeine Bezeichnung der dokumentierten Verarbeitungstätigkeit z. B.:</i> <ul style="list-style-type: none"> • „Dokumentation der Behandlung“ • „E-Mail-Verarbeitung“ • „Lohn- und Gehaltsabrechnung“
Zweckbestimmung	<i>z. B.:</i> <ul style="list-style-type: none"> • 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 <p><i>Es können auch mehrere Zweckbestimmungen für eine Verarbeitung angegeben werden.</i></p>
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	<i>z. B.:</i> <ul style="list-style-type: none"> • 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	<i>z. B.:</i> <i>Patienten, Mitarbeiter, Bewerber</i>
Beschreibung der Datenkategorien/Art der gespeicherten Daten	<i>z. B.:</i> <ul style="list-style-type: none"> • Gesundheitsdaten (besondere Kategorien personenbezogener Daten) • Bankverbindungsdaten/Kreditkartendaten • Lohn- und Gehaltsdaten • Name/Vorname/Anrede/Titel, Geburtsdatum, Adressdaten • Sozialversicherungsdaten • Vertragsdaten • Zeiterfassungsdaten
Herkunft der Daten:	<i>Woher stammen die Daten? Von Betroffenen selbst oder von einem Dritten?</i>

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der Einrichtung des Verantwortlichen)	z. B.: <i>Personalabteilung, Buchhaltung, Auftragsverarbeiter</i>
Externe Empfänger und Dritte, soweit nicht Auftragsverarbeiter	z. B.: <i>Kassenzahnärztliche Vereinigung, Krankenkasse, Steuerberater.</i>
Datenübermittlung in Drittstaaten/internationale Organisationen (z. B. Cloud-Dienste)	
Datenübermittlung in Drittstaaten	<i>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).</i>
Angemessenes Datenschutzniveau durch	<ul style="list-style-type: none"> • <i>Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO oder</i> • <i>Garantien gem. Art. 46 DSGVO</i> <ul style="list-style-type: none"> - <i>Verbindliche interne Datenschutzvorschriften (BCR)</i> - <i>EU-Standardvertrag</i> <p><i>Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. Abs. 2 DSGVO)</i></p>
Fristen für die Löschung der verschiedenen Datenkategorien	
Speicherdauer, Fristen	z. B.: <i>§ 630 f Abs. 3 BGB (Behandlungsdokumentation), § 28 Abs. 3 RöV</i>
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	<p><i>Maßnahmen müssen unter anderem Folgendes einschließen:</i></p> <ul style="list-style-type: none"> • <i>die Pseudonymisierung und Verschlüsselung personenbezogener Daten;</i> • <i>die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen;</i> • <i>die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;</i> • <i>ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.</i> <p><i>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).</i></p>
Prüfung durch den Verantwortlichen	
Prüfung	<i>Erfolgt/nicht erfolgt</i>
Datum, Unterschrift	