

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

Muster für ein Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO		Vorblatt
Angaben zum Verantwortlichen / ggf. Mitverantwortlichen / ggf. Vertreter		
Name/n	<i>Dr. Max Musterarzt/Musterpsychotherapeut</i>	
Straße	<i>Musterstraße 1</i>	
Postleitzahl	<i>12345</i>	
Ort	<i>Musterstadt</i>	
Telefon	<i>0123 456789</i>	
E-Mail-Adresse	<i>drmustermann@musterpraxis.de</i>	
Internet-Adresse	<i>www.musterpraxis.de</i>	
Angaben zur Person des Datenschutzbeauftragten (sofern gem. Artikel 37 DSGVO benannt)		
Anrede	<i>Frau</i>	
Titel	<i>-</i>	
Name, Vorname	<i>Musterfrau, Anna</i>	
Straße	<i>Musterstraße 1</i>	
Postleitzahl	<i>12345</i>	
Ort	<i>Musterstadt</i>	
Telefon	<i>0123 456789</i>	
E-Mail-Adresse	<i>datenschutzbeauftragte@musterpraxis.de</i>	

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

Verarbeitungstätigkeit Nr.: 1	
Bezeichnung: <u>Patientenbehandlung</u>	
Datum der Einführung: <i>05.04.2018</i>	Datum der letzten Änderung: <i>06.04.2018</i>
Zwecke der Verarbeitung:	
<i>Behandlung von Patienten, Erfüllung der Dokumentationspflichten (Führen der Patientenakte)</i>	
Beschreibung der Kategorien betroffener Personen	
<i>Patienten Unter Umständen weitere Betroffene (Familienangehörige, Pflegepersonal, andere Ärzte, etc.)</i>	
Beschreibung der Kategorien von personenbezogenen Daten	
<ul style="list-style-type: none">• <i>Name</i>• <i>Adressdaten</i>• <i>Kontakt Daten (Ansprechpartner, Telefon etc.)</i>• <i>Geburtsdatum</i>• <i>Gesundheitsdaten</i>• <i>Behandlungsdaten</i>• <i>ggf. Religionszugehörigkeit und andere behandlungsnotwendigen Daten</i>	
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden	
<i>Interne Zugriffsberechtigte</i>	<ul style="list-style-type: none">• <i>Angestellte Ärzte/Psychotherapeuten</i>• <i>Medizinische Fachangestellte</i>• <i>Medizinisch- technische Assistenten</i>• <i>Laborassistenten</i>• <i>etc.</i>
<i>Externe Empfänger</i>	<ul style="list-style-type: none">• <i>andere Ärzte/Psychotherapeuten</i>• <i>Krankenkassen</i>• <i>Medizinischer Dienst der Krankenversicherung</i>• <i>etc.</i>

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

(in der Regel) keine

Fristen für die Löschung

Die gesetzlichen Aufbewahrungsfristen werden eingehalten. D.h.:

In der Regel werden die Daten 10 Jahre nach Abschluss der Behandlung gelöscht (ggf. erst nach 30 Jahren, z. B. bei Strahlenbehandlung).

Weitere Infos siehe: Merkblatt der KVBW zu den Aufbewahrungsfristen.

U.U. bei haftungsrechtlichen Bedenken / mögl. Schadensersatzforderungen zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen wird nicht gelöscht. Allerdings werden in diesem Fall die betroffenen Patientenakten nach Ablauf der gesetzlichen Aufbewahrungsfrist gesperrt.

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO

Beispielhafte Aufstellung möglicher TOMs (kann je nach Praxis variieren)

Bitte ausführlich darstellen:

Die Musterbeispiele können als Checkliste zur Eigenkontrolle und zur Etablierung von weiteren Datenschutzmaßnahmen genutzt werden.

- *Arbeitsanweisung zur Patientenannahme ist vorhanden*
- *Datenschutz-Information zur Auslage, Aushang und für Internetseite vorhanden*
- *Einhaltung von Diskretionsspielregeln*
- *Verhaltensregeln für den Umgang mit dem Telefon und Fax*
- *Zugriffsschutz: abschließbare Schränke, Bildschirmsperre*
- *keine Nutzung/Beantwortung von unverschlüsselten E-Mails im Patientenkontakt*
- *regelmäßige Schulungen/Unterweisungen der Mitarbeiter*
- *Schutz vor unberechtigter Einsicht in das Patientenverwaltungssystem mittels abgetrenntem Empfangsbereich*
- *durch Tür abgetrennter Empfangs- und Wartebereich*
- *Löschkonzept liegt vor*
- *Meldekonzept liegt vor*
- *AV-Vertrag mit Softwarefirma (Name) liegt vor*
- *AV-Vertrag mit Schredderfirma (Name) liegt vor*
- *ggf. Datenschutzbeauftragter benannt und gemeldet*
- *Notfallkonzept vorhanden: z. B. Regelung zum Verhalten bei Ausfall des PVS*
- *etc.*

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

Das IT-Sicherheitskonzept beinhaltet:

- *automatische Updates im Betriebssystem aktivieren*
- *automatische Updates des Browsers aktivieren*
- *Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte*
- *Standard-Gruppenverwaltung (z. B. in Windows)*
- *aktueller Virens Scanner/Sicherheitssoftware*
- *Papieraktenvernichtung mit Spezial-Shredder mit Sicherheitsstufe 4*
- *PVS und Recherche-PC trennen*
- *Zugriffs- und Berechtigungskonzept*
- *Ende-zu-Ende und Transportverschlüsselung, z. B. bei Online-Terminbuchung, elektronischem Versand, Mitgliederportal der KVBW*
- *etc.*

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

Verarbeitungstätigkeit Nr.: 2	
Bezeichnung: <u>Lohnabrechnung, Personalakten</u>	
Datum der Einführung: <i>05.04.2018</i>	Datum der letzten Änderung: <i>06.04.2018</i>
Zwecke der Verarbeitung	
<ul style="list-style-type: none">• <i>Auszahlung der Löhne/Gehälter</i>• <i>Abfuhr Sozialabgaben u. Steuern</i>• <i>Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder Arbeitsverhältnisses</i>• <i>Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung oder des Personaleinsatzes</i>• <i>etc.</i>	
Beschreibung der Kategorien betroffener Personen	
<i>Personal</i>	
Beschreibung der Kategorien von personenbezogenen Daten	
<ul style="list-style-type: none">• <i>Name, Geburtsdatum</i>• <i>Adresse</i>• <i>Bankverbindungsdaten</i>• <i>Lohn-/Entgeltdaten</i>• <i>ggf. Religionszugehörigkeit</i>• <i>Sozialversicherungsdaten</i>• <i>Steuerdaten (Steuerklasse, Freibeträge)</i>• <i>Berufsgenossenschaftsangaben</i>• <i>etc.</i>	

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden

Interne Zugriffsberechtigte

- *Praxisverantwortlicher*
- *ggf. Buchhaltung*

Externe Empfänger

- *Finanzamt*
- *Sozialversicherungsträger*
- *etc.*

Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

(in der Regel) keine

Fristen für die Löschung

10 Jahre nach Beendigung des Arbeitsverhältnisses

Bitte holen Sie sich die notwendigen Informationen hierzu von Ihrem Steuerexperten ein.

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO

Beispielhafte Aufstellung möglicher TOMs (kann je nach Praxis variieren)

Bitte ausführlich darstellen:

- *Zugriffsschutz: abschließbare Schränke, Bildschirmsperre*
- *aktueller Virens scanner/Sicherheitssoftware*
- *Schutz vor unberechtigter Einsicht in die Personalverwaltungssoftware mittels eingeschränkter Berechtigungen*
- *Löschkonzept liegt vor*
regelmäßige Backups: z. B. wöchentlich auf einer externen Festplatte
- *Notfallkonzept vorhanden: z. B. Regelung zum Verhalten bei Ausfall des Personalverwaltungssystems*
- *siehe IT-Sicherheitskonzept*
- *etc.*

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

<p>Verarbeitungstätigkeit Nr.: 3</p> <p>Bezeichnung: <u>Betrieb der Webseite mit Möglichkeit der Online-Terminbuchung</u></p>	
Datum der Einführung: <i>05.04.2018</i>	Datum der letzten Änderung: <i>06.04.2018</i>
Zwecke der Verarbeitung	
<ul style="list-style-type: none">• <i>Betrieb einer Webseite</i>• <i>Terminbuchung</i>	
Beschreibung der Kategorien betroffener Personen	
Beschreibung der Kategorien von personenbezogenen Daten	
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden	
Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation	
Fristen für die Löschung	

Wichtiger Hinweis: Dies ist ein **Muster!**

Bitte die Inhalte auf Ihre **konkreten** Praxisverhältnisse anpassen.

D. h. die kursiv geschriebenen Eintragungsbeispiele verändern, ergänzen und/oder streichen.

**Technische und organisatorische Maßnahmen (TOM)
gemäß Art. 32 Abs. 1 DSGVO**

Weitere Verarbeitungstätigkeiten analog beschreiben:

- Verarbeitung von Patientendaten zur Abrechnung über die KV bzw. PVS
- etc.

.....
Verantwortlicher

.....
Datum

.....
Unterschrift