

Musterverzeichnis von Verarbeitungstätigkeiten

Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz -Grundverordnung (DSGVO)

Bitte berücksichtigen Sie, dass für jede identifizierte Verarbeitungstätigkeit je ein Verzeichnis zu führen ist! Das Muster beinhaltet mögliche Tätigkeiten, die individuell einzufügen sind.

Angaben zum Verantwortlichen

Name:
 Anschrift:
 Telefon:
 E-Mail:
 Internet -Adresse:

Angaben zur Person des Datenschutzbeauftragten (sofern gem. Art. 37 DSGVO benannt)

Vorname und Name:
 Anschrift:
 Telefon:
 E-Mail:

Verarbeitungstätigkeit

Datum der Anlegung:
 Datum der letzten Änderung:

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.:	* Verarbeitung besonderer Kategorien personenbezogener Daten, Gesundheitsdaten auf der Grundlage eines Behandlungsvertrages (Art. 9 Abs. 2 lit. h DSGVO) * 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)

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztchammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

Erhebung der Daten

Betroffene Personengruppen

z.B.: Patienten, Mitarbeiter, Bewerber

Beschreibung der Datenkategorien /
Art der gespeicherten Daten

z.B.:
* Name / Vorname / Anrede / Titel, Geburtsdatum, Adressdaten
* Gesundheitsdaten (besondere Kategorien personenbezogener Daten)
* Lohn- und Gehaltsdaten
* Zeiterfassungsdaten
* Sozialversicherungsdaten
* Vertragsdaten

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

Interne Empfänger
(innerhalb der Einrichtung des
Verantwortlichen)

z.B.:

Praxispersonal, Personalabteilung, Buchhaltung, Auftragsverarbeiter

Externe Empfänger und Dritte,
soweit nicht Auftragsverarbeiter

z.B.: externe andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern, privatärztliche Verrechnungsstellen

Datenübermittlung in Drittstaaten / internationale Organisationen (z. B. Cloud-Dienste)

Datenübermittlung in Drittstaaten

Sofern eine Datenübermittlung in Drittstaaten erfolgt, ist vorab zu klären, ob Datenübermittlungen in ein Drittland oder an eine internationale Organisation stattfinden. 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. (ggf. Auskunft von der Aufsichtsbehörde einholen)

Fristen für die Löschung der verschiedenen Datenkategorien

Daten sind zu löschen, wenn sie nicht
mehr benötigt werden; dabei sind ggf.
Aufbewahrungsfristen zu beachten

z. B.: §630 lit. f Abs. 3 BGB (Behandlungsdokumentation) § 28 Abs. 3 RÖV

Beurteilung der Angemessenheit technischer und organisatorischer Maßnahmen (TOM)

Allgemeine
Beschreibung der technischen

Maßnahmen müssen unter anderem Folgendes einschließen:
* die Pseudonymisierung und Verschlüsselung personenbezogener

Informationsblätter zum neuen Datenschutzrecht in der ambulanten Versorgung

und organisatorischen
Maßnahmen (Art. 32 Abs. 1 DSGVO)
Und des etwaigen verbleibenden
Risikos unter Berücksichtigung
der eingesetzten technisch
organisatorischen Maßnahmen

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 (Verantwortlicher)
