Teil 3

Wer, was, wie und warum?

Beitragsserie „DS-GVO kompakt", Teil 3: Verzeichnis von Verarbeitungstätigkeiten

1. Einführung

Die DS-GVO verpflichtet nunmehr den Verantwortlichen (vgl. KVWL DS-GVO kompakt Nr. 1), ein Verzeichnis von Verarbeitungstätigkeiten (VVT) zu erstellen und fortlaufend zu aktualisieren.[1] Mit dem Verzeichnis führt der Verantwortliche den Nachweis, dass in seinem Verantwortungsbereich Daten DS-GVO-konform verarbeitet werden. Insofern ist das Verzeichnis auch auf Anfrage der Aufsichtsbehörde vorzulegen, damit die Verarbeitungsvorgänge beim Verantwortlichen anhand der Dokumentation durch die Behörde kontrolliert werden können. Ein Einsichtsrecht für jedermann – also auch Betroffene einer Datenverarbeitung – besteht beim VVT jedoch nicht. Patienten werden über Informationen zum Datenschutz (vgl. KVWL DS-GVO kompakt Nr. 2) über die Umstände der Datenverarbeitung informiert.

Die DS-GVO sieht im Falle von klein- oder mittelständischen Unternehmen Ausnahmen von der Erstellung eines VVT vor, die jedoch für Arztpraxen nicht greifen, weil dort die besonders zu schützenden Gesundheitsdaten verarbeitet werden.[2]

Das Verzeichnis ist vom Verantwortlichen (z. B. Einzelarzt oder Gemeinschaftspraxis) zu erstellen; eine Übertragung auf den Datenschutzbeauftragten ist aber auch möglich. Das Verzeichnis kann schriftlich oder in einem elektronischen Format (z. B. in Word oder Excel) geführt werden.

Das VVT beschreibt alle Verarbeitungstätigkeiten mit personenbezogenen Daten bei einem Verantwortlichen. Verarbeitungstätigkeiten bestehen häufig aus einer Vielzahl von Teilverarbeitungsschritten, die jedoch nicht jeweils einzeln dokumentiert werden müssen. Geklammert werden diese Teilschritte durch die übergeordnete Zweckbestimmung, die mit der Datenverarbeitung verfolgt wird. Insofern reicht es aus, nur solche übergeordneten Verarbeitungstätigkeiten im VVT zu dokumentieren und zu beschreiben.

Für Arztpraxen sind insbesondere die Verarbeitungsaktivitäten der Patientenverwaltung sowie die Personalverwaltung relevant. Aber auch das Inkasso kann eine eigenständige Verarbeitungstätigkeit darstellen, vorausgesetzt es werden privatärztliche Leistungen erbracht. Nach alter Rechtslage zu erstellende Verfahrensverzeichnisse decken bereits eine Vielzahl der gesetzlichen Vorgaben der DS-GVO für ein VVT ab. Daher können sie – sofern vorhanden – als Grundlage für die nach der DS-GVO geforderten Beschreibungen des VVT dienen und so die Basisarbeit erleichtern.

Hinweis: Ergeben sich im Laufe der Zeit wesentliche Änderungen bei der Datenverarbeitung (z. B. eine neue Zweckbestimmung tritt hinzu oder die Offenlegung von Daten an neue Empfänger ist erfolgt), muss eine Aktualisierung der Dokumentation erfolgen.

2. Inhalt des Verzeichnisses

Das Verzeichnis muss elementare Angaben zur Verarbeitung personenbezogener Daten machen, hierzu zählen beispielsweise die Zwecke der Verarbeitung, die Kategorien betroffener Personen sowie die hierbei verarbeiteten Datenkategorien. Ebenso zählen Empfänger von Daten sowie die Beschreibung technisch-organisatorischer Maßnahmen zur Datensicherheit zu den pflichtigen Inhalten. Wie detailliert die Beschreibung der technisch-organisatorischen Maßnahmen sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen. Maßnahmen zur Erfüllung der Schutzziele der Informationssicherheit in Gestalt der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der eingesetzten Systeme sollten jedoch dargestellt werden, wobei hier auch auf Angaben eines Herstellers zurückgegriffen werden kann. Jedenfalls sollte die Beschreibung der Maßnahmen nach Art. 32 DS-GVO so konkret erfolgen, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.

---

[1] Art. 30 DS-GVO.

[2] Art. 30 Abs. 5 DS-GVO i.V.m. Art. 9 Abs. 1 DS-GVO.

Muster

Verzeichnis von Verarbeitungstätigkeiten

Hinweis: *Das nachfolgende Muster wurde auf Basis der Hilfestellung der Kassenärztlichen Bundesvereinigung (KBV) erstellt. Es wurde jedoch durch die KVWL an aufsichtsbehördliche Empfehlungen angepasst.*[3]

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Rechtliche Grundlage: Artikel 30 Absatz 1 DS-GVO

Angaben zum Verantwortlichen

Name: Praxis Mustermann

Anschrift: Musterstraße 1a, 23456 Musterhausen

Telefon: 0123 456789

E-Mail: praxis@mustermann.de

Internet-Adresse: www.praxis-mustermann.de

Angaben zur Person des Datenschutzbeauftragten (falls vorhanden)

Vorname und Name: Sabine Mustermann

Anschrift: Musterstraße 1a, 23456 Musterhausen

Telefon: 0123 456788

E-Mail: datenschutzbeauftragter@praxis-mustermann.de

VERARBEITUNGSTÄTIGKEIT – Patientenverwaltung

Datum der Anlegung: 20. März 2018
Datum der letzten Änderung: 21. März 2018

Bezeichnung der Verarbeitungstätigkeit

Patientenverwaltung

Zwecke der Verarbeitung

Behandlung von Patienten, Abrechnung der ärztlichen Leistungen, Qualitätssicherung, Terminmanagement

Beschreibung der Kategorien betroffener Personen

Patienten

Beschreibung der Datenkategorien

Name, Adressen, Gesundheitsdaten, ggf. genetische Daten

[3] http://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Verarbeitungsverzeichnis_Ausfuellbeispiel.pdf.

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

Intern (Zugriffsberechtigte): Praxispersonal
Extern (Empfängerkategorie): Andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern, privatärztliche Verrechnungsstellen

Fristen für die Löschung

10 Jahre (gesetzliche Aufbewahrungsfrist)

Beschreibung der technisch-organisatorischen Maßnahmen

Siehe IT-Sicherheitskonzept

VERARBEITUNGSTÄTIGKEIT – Personalverwaltung

Datum der Anlegung: 18. März 2018
Datum der letzten Änderung: 20. März 2018

Bezeichnung der Verarbeitungstätigkeit

Personalverwaltung

Zwecke der Verarbeitung

Auszahlung der Löhne/Gehälter, Abfuhr von Sozialabgaben und Steuern

Beschreibung der Kategorien betroffener Personen

Beschäftigte

Beschreibung der Datenkategorien

Name, Geburtsdatum, Adresse, Bankverbindungsdaten, Lohn-/Entgeltdaten, ggf. Religionszugehörigkeit, Sozialversicherungsdaten, Steuerdaten (Steuerklasse, Freibeträge), Berufsgenossenschaftsangaben

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

Intern: Dr. Max Mustermann, ggf. Praxispersonal
Extern: Finanzamt, Krankenkassen, Rentenversicherer, ggf. externe Dienstleister zur Lohnabrechnung

Fristen für die Löschung

10 Jahre (gesetzliche Aufbewahrungsfrist)

Beschreibung der technisch-organisatorischen Maßnahmen

Siehe IT-Sicherheitskonzept

Muster

VERARBEITUNGSTÄTIGKEIT – Webseite

Datum der Anlegung: 18. März 2018
Datum der letzten Änderung: 20. März 2018

Bezeichnung der Verarbeitungstätigkeit
Webseite

Zwecke der Verarbeitung
Betrieb der Webseite, ggf. Terminbuchung

Beschreibung der Kategorien betroffener Personen
Webseitenbesucher, ggf. Patienten

Beschreibung der Datenkategorien
IP-Adresse, Name und Kontakt, ggf. Terminwunsch

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden
Intern: Dr. Max Mustermann, ggf. Praxispersonal
Extern: Ggf. Dienstleister zum Betrieb der Webseite

Fristen für die Löschung
IP-Adresse nach 7 Tagen

Beschreibung der technisch-organisatorischen Maßnahmen
Siehe IT-Sicherheitskonzept

Auszug aus einem IT-Sicherheitskonzept
(enthält technische und organisatorische Maßnahmen):

☑ Schlüssel, elektrische Türöffner, Alarmanlage	☑ Automatische Updates im Betriebssystem aktivieren	☑ Wöchentliche Backups (z. B. auf eine externe Festplatte)
☑ Sichere Passwörter (Zeichenmix einschl. Sonderzeichen)	☑ Automatische Updates des Browsers aktivieren	☑ Aktueller Virenscanner/Sicherheitssoftware
☑ Standard-Gruppenverwaltung (z. B. in Windows	☑ Zugriffs- und Berechtigungskonzept	☑ Papieraktenvernichtung mit Spezial-Shredder
☑ Abrechnungs- und Recherche-PC trennen	☑ Ende-zu-Ende und Transportverschlüsselung bei Onlineterminbuchung	☑ Verschlüsselte VPN-Verbindung bei Fernzugriff