

Datenschutz im Gesundheitswesen Modul 1

Verzeichnis der Verarbeitungstätigkeiten/
Sicherheit der Verarbeitung



Agenda

- I. Verzeichnis der Verarbeitungstätigkeiten
- II. Sicherheit der Verarbeitung

Agenda

Verzeichnis der Verarbeitungstätigkeiten

1. Funktionen
2. Verpflichtete und Ausnahmen
3. Pflichten des Verantwortlichen
4. Pflichten des Auftragsverarbeiters

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

1. Funktionen

- Im Hinblick auf Verantwortlichen/Auftragsverarbeiter:
 - Überblick, strukturierte Dokumentation, Datenschutz-Compliance
- Im Hinblick auf die zuständige Datenschutz-Aufsichtsbehörde:
 - „Accountability“ (des Verantwortlichen, Art. 5 Abs. 2 DSGVO), Kontrolle (Art. 30 Abs. 4 DSGVO), Vermeidung von Bußgeldern (Art. 83 Abs. 4 lit. a DSGVO)

§ Fehlendes VVT führt nicht zur Rechtswidrigkeit der Datenverarbeitung (EuGH, Urteil vom 04.05.2023 – Rs. C-60/22)



Erwägungsgrund Nr. 82 DSGVO:

„Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten [...] führen.

Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.“

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

2. Verpflichtete und Ausnahmen

- Verantwortliche (Art. 30 Abs. 1 DSGVO) und Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO)
 - Der Verantwortliche hat auch Verarbeitungen in seinem VVT zu dokumentieren, die Auftragsverarbeiter nach seiner Weisung ausführt.
- „Vertreter“ nur ausnahmsweise relevant (Art. 27 und Art. 3 Abs. 2 DSGVO)

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

2. Verpflichtete und Ausnahmen

Ausnahmen: Unternehmen mit weniger als 250 Mitarbeitern sind gemäß Art. 30 Abs. 5 DSGVO von der Pflicht zur Führung eines VVT befreit, „es sei denn,

- die von ihnen vorgenommene Verarbeitung birgt ein (qualifiziertes) Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nicht nur gelegentlich,
- es erfolgt eine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10“.



Stets Pflicht zur Führung eines VVT bei der Verarbeitung von Gesundheitsdaten

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

3. Pflichten des Verantwortlichen

- Nicht: Auflistung jeder einzelnen Verarbeitung (z.B. Erhebung, Speicherung, Verwendung etc.) gemäß Art. 4 Nr. 2 DSGVO
- „Verarbeitungstätigkeit“ = eine Reihe von aufeinanderfolgenden Vorgängen, in denen personenbezogene Daten verarbeitet werden (Rs. „Fashion-ID“ des EuGH)
- Mit anderen Worten: ein Prozess in einem Unternehmen/einer Einrichtung

☀ Bündelung aller Vorgänge, die denselben Zweck verfolgen

- Bsp.: Terminvergabe, Anamnese/Behandlung, Begutachtung, Videosprechstunde, Überweisung, Qualitätssicherung, MDK-Prüfungen, Abrechnungen, Personalverwaltung etc.



Art 30 Abs. 1 Satz 1 DSGVO:

„Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen“.

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

3. Pflichten des Verantwortlichen

 Tipps zur Erfassung der Verarbeitungstätigkeiten:

- Prozesse sollten dezentral als Verarbeitungsmeldungen (mittels Fragebögen oder in Form von Interviews) erfasst und an eine zentrale Stelle mit dem Ziel der Zusammenführung im VVT gemeldet werden
- Einheitliches, elektronisches VVT, Empfehlung: in Excel-Datei oder Software
- Plausibilitätsprüfung und regelmäßige Prüfroutinen (Change-Management)

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

- (1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
- a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
 - b) die Zwecke der Verarbeitung;
 - c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
 - d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
 - e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
 - f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
 - g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

hierzu sogleich



Pflichtinhalte des VVT des Verantwortlichen:

- Jeweilige Prozessbezeichnung (ungeschriebenes Tatbestandsmerkmal)
- Die übrigen (Pflicht-)Inhalte des VVT ergeben sich aus Art. 30 Abs. 1 Satz 2 DSGVO

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

3. Pflichten des Verantwortlichen

- VVT als Werkzeug für Datenschutz-Compliance:
- Datenschutz-Folgenabschätzung, Art. 35 DSGVO
- Datenschutzinformationen, Art. 13 und 14 DSGVO
- Datenübermittlungen in Drittländer, Art. 44 ff. DSGVO
- Löschkonzepte, Art. 17 DSGVO
- Gewährleistung der Sicherheit der Verarbeitung, Art. 32 DSGVO
- Ggf. Auskunftsanspruch gemäß Art. 15 Abs. 3 DSGVO
 - § Bei Protokolldateien handelt es sich „um Verzeichnisse von Verarbeitungstätigkeiten im Sinne von Art. 30 DSGVO“ (EuGH, Urteil vom 22.06.2023, Rs. C-579/21), können vom Auskunftsanspruch umfasst sein

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

4. Pflichten des Auftragsverarbeiters

- Erstellung des VVT grundsätzlich aus Sicht des Dienstleisters, orientiert an seinen Standardleistungen, d.h. Dienstleistungen oder Produkten
- Hieraus Ableiten von „Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden“
- Primärer Zweck: Übersicht, welche Leistungen für welchen Verantwortlichen erbracht werden



Art 30 Abs. 1 Satz 2 DSGVO:

„Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung“.

I. Verzeichnis der Verarbeitungstätigkeiten („VVT“)

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die ~~Dokumentierung geeigneter Garantien~~;
- d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Ohnehin Bestandteil des jeweiligen AVV



Pflichtinhalte des VVT des Auftragsverarbeiters

ergeben sich aus Art. 30 Abs. 2 DSGVO

Agenda

Sicherheit der Verarbeitung

1. Art. 32 DSGVO und risikobasierter Ansatz
2. Identifizieren von Risiken
3. Bewertung von Risiken „Eintrittswahrscheinlichkeit und Schadensschwere“
4. Bewältigung von Risiken

II. Sicherheit der Verarbeitung



1. Art. 32 und risikobasierter Ansatz

Artikel 32

Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

II. Sicherheit der Verarbeitung

Art. 32 Abs. 1 DSGVO

Umsetzung geeigneter technischer und organisatorischer Maßnahmen...

- unter Berücksichtigung der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken
- für die Rechte und Freiheiten natürlicher Personen
- um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

Das Risiko skaliert die bestehende Pflicht

z.B. Art. 30 Abs. 5 DSGVO

Pflicht zur Führung eines VVT...

- wenn die Verarbeitung ein Risiko
- für die Rechte und Freiheiten der betroffenen Personen birgt

Das Risiko entscheidet über das Bestehen der Pflicht

II. Sicherheit der Verarbeitung



2. Identifizieren von Risiken

- Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses
 - das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder
 - zu einem weiteren Schaden (Folgeschaden) für eine oder mehrere natürliche Personen führen kann (Def. nach Datenschutzkonferenz, Kurpapier Nr. 18)
- Perspektive: betroffene Person

II. Sicherheit der Verarbeitung



2. Identifizieren von Risiken

- ② Welche Schäden können potentiell entstehen?
 - Sämtliche rechtlich geschützte Interessen des Betroffenen
 - z.B.: physische, materielle, immaterielle Schäden, insb. Diskriminierung/Rufschädigung, gesellschaftliche Nachteile, Identitätsdiebstahl, finanzieller Verlust, Erschwerung der Rechtsausübung/Kontrolle

- ② Durch welche Ereignisse kann es in einem Worst-Case Szenario zu dem Schaden kommen?
 - Jegliche (potentielle) Nichteinhaltung von Vorschriften der DSGVO
 - z.B.: Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten (vgl. hierzu Art. 32 Abs. 2 DSGVO), Verwendung der Daten zu inkompatiblen Zwecken, (Weiter)Verarbeitung unrichtiger Daten
 - Konkrete Bsp.: Veröffentlichung von Gesundheitsdaten im Internet durch unbefugten Zugang oder Offenlegung; Verlust von Gesundheitsdaten, die für Behandlung eines Patienten notwendig sind

II. Sicherheit der Verarbeitung



2. Identifizieren von Risiken

- ② Durch welche Handlungen und Umstände (Risikquellen) kann es zum Eintritt dieser Ereignisse kommen?
- Menschliche Risikoquellen (vorsätzlich böswillige oder fahrlässige): Mitarbeiter des Verantwortlichen, Hacker, Auftragsverarbeiter, der Staat
 - Nicht-menschliche Risikoquellen: Höhere Gewalt, technisches Versagen

II. Sicherheit der Verarbeitung



3. Bewertung von Risiken „Eintrittswahrscheinlichkeit und Schadensschwere“

- Zwei Faktoren – Eintrittswahrscheinlichkeit x Schadensschwere
- Eintrittswahrscheinlichkeit
 - Nicht quantifizierbar, es gibt nicht zwingend ein richtiges Ergebnis
 - Einfließen können: Umfang der Verarbeitung (Art. 32 Abs. 1 DSGVO), Präsenz von Gefährdungslagen, statistische Erhebungen/Studien (wie oft kam es zu Vorfällen?), Missbrauchsinteresse eines Schädigers, Risiko, beim Missbrauch entdeckt zu werden, sonstige Folgen für den Schädiger

II. Sicherheit der Verarbeitung



3. Bewertung von Risiken „Eintrittswahrscheinlichkeit und Schadensschwere“

– Schadensschwere

- Nicht quantifizierbar, es gibt nicht zwingend ein richtiges Ergebnis
- Einfließen können:
 - Wertungen des Ordnungsgebers in Art. 32 Abs. 1 DSGVO: Art, Umstände, Zwecke der Verarbeitung
 - Wertungen des Ordnungsgebers an anderen Stellen: Besonders schützenswerte Personen und Daten (Kinder, Beschäftigte, Art. 9, 10 DSGVO); Profiling, Anzahl der Personen, Datensätze, Merkmale in Datensatz oder geographische Abdeckung etc.



Stets schwerer Schaden bei Gesundheitsdaten gemäß Art. 9 Abs. 1 DSGVO:

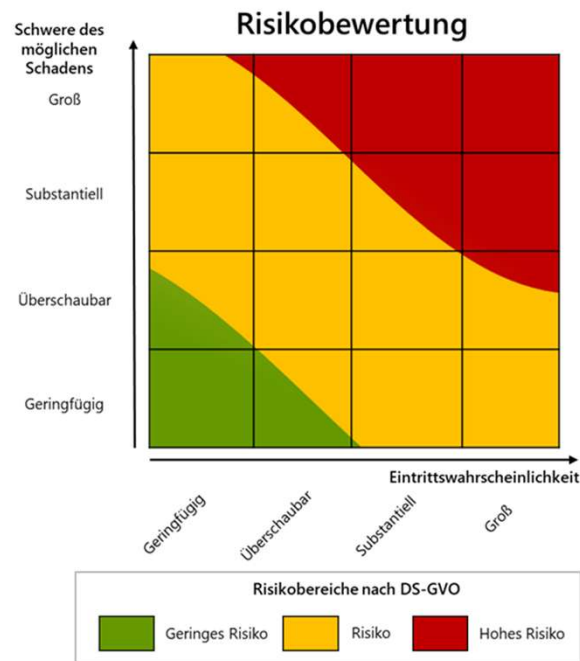
Gemäß LfD Niedersachsen: „Personenbezogene Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz“).“

II. Sicherheit der Verarbeitung



3. Bewertung von Risiken „Eintrittswahrscheinlichkeit und Schadensschwere“

Der Risikowert ergibt sich aus der Eintrittswahrscheinlichkeit und der Schwere des möglichen Schadens:



Quelle: DSK, Kurzpapier Nr. 18

II. Sicherheit der Verarbeitung



4. Bewältigung von Risiken

- Umsetzung von Abhilfemaßnahmen, die ein angemessenes Schutzniveau herstellen
- Die Auswahl der Maßnahmen orientiert sich an:
 - Ermittelttem Risikowert
 - Stand der Technik
 - Implementierungskosten (eher Vorsicht bei der Verarbeitung von Gesundheitsdaten)
- Die Auswahl der Maßnahmen ist eine technische Frage
- Beispiele:
 - Verschlüsselung, Pseudonymisierung (Art. 32 Abs. 1 Satz 2 lit. a DSGVO)
 - Standard-Datenschutzmodell
 - BSI – IT-Grundschutz-Kompendium

Vielen Dank!



Dr. Stefanie Schulz-Große

Leipziger Platz 3, 10117 Berlin

Tel +49 30 885665-248

schulz-grosse@redeker.de

REDEKER | SELLNER | DAHS

Berlin

Leipziger Platz 3

10117 Berlin

Tel +49 30 885665-0

Fax +49 30 885665-99

berlin@redeker.de

Bonn

Willy-Brandt-Allee 11

53113 Bonn

Tel +49 228 72625-0

Fax +49 228 72625-99

bonn@redeker.de

Leipzig

Petersstraße 39-41

04109 Leipzig

Tel +49 341 21378-0

Fax +49 341 21378-30

leipzig@redeker.de

London

4 More London Riverside

London SE1 2AU

Tel +44 20 77882555

london@redeker.de

Brüssel

172, Av. de Cortenbergh

1000 Brüssel

Tel +32 2 74003-20

Fax +32 2 74003-29

bruessel@redeker.de

München

Maffeistraße 4

80333 München

Tel +49 89 2420678-0

Fax +49 89 2420678-69

muenchen@redeker.de