EU-Datenschutz-Grundverordnung (DSGVO): Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten

Pflicht und Umfang von Verzeichnissen von Verarbeitungstätigkeiten

Allgemeines

Die DSGVO verpflichtet zum Führen von Verzeichnissen über die Verarbeitung von Daten. Diese Pflicht trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter (siehe dazu auch „Verantwortlicher und Auftragsverarbeiter"). Der Umfang der Dokumentationspflicht ist für den Auftragsverarbeiter geringer als für den Verantwortlichen.

Was muss das Verzeichnis enthalten?

Der **Verantwortliche** hat ein Verzeichnis sämtlicher Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen, zu führen. Dieses Verzeichnis hat Folgendes zu enthalten:

- Namen und Kontaktdaten des bzw. der Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- Zweck der Datenverarbeitung,

> **Tipp:**
> Selbst wenn es nicht zwingend vorgesehen ist, empfiehlt sich aus Beweisgründen auch die Angabe der Rechtsgrundlage (z.B. Einwilligungserklärung) für den Datenverarbeitungszweck.

- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (z.B. Kunden und Lieferanten; Rechnungsdaten, Adressdaten),
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (z.B. Sozialversicherung, Finanzamt, Rechtsanwalt, Steuerberater), einschließlich Empfänger in Drittländern oder internationalen Organisationen (z.B. Konzernmutter in USA),
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland (z.B. USA) oder an eine internationale Organisation, einschließlich der Angaben des betreffenden Drittlands oder der betreffenden internationalen Organisation (uU ist auch die Dokumentierung geeigneter Garantien erforderlich),
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (nach Möglichkeit),
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit).

Über alle im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten hat der **Auftragsverarbeiter** ein Verzeichnis zu führen. Dieses Verzeichnis hat Folgendes zu enthalten:

- Name und Kontaktdaten des Auftragverarbeiters und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragverarbeiters und eines etwaigen Datenschutzbeauftragten,
- Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder eine internationalen Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation (uU ist auch die Dokumentierung geeigneter Garantien erforderlich).
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit).

Form der Verzeichnisse

Diese Verzeichnisse sind schriftlich zu führen, wobei dies auch in einem elektronischen Format erfolgen kann. Musterverzeichnisse mit Anwendungsbeispielen finden Sie im Downloadbereich.

Pflichten gegenüber der Aufsichtsbehörde

Jeder Verantwortliche, jeder Auftragsverarbeiter sowie die jeweiligen Vertreter haben bei der Erfüllung ihrer Aufgaben mit der Aufsichtsbehörde zusammenzuarbeiten. Auf Anfrage sind die Verzeichnisse der Behörde vorzulegen. Anhand dieser Verzeichnisse ist es für die Aufsichtsbehörde möglich, die betreffenden Verarbeitungsvorgänge zu kontrollieren.

Hinweis:
Jedes Unternehmen, das eine Lohnverrechnung und/oder Kundendateien führt, benötigt ein Verarbeitungsverzeichnis (diese Verarbeitungen erfolgen nicht „nur gelegentlich").

Wen trifft die Pflicht zur Führung dieser Verzeichnisse?

Die Pflicht zur Führung des Verarbeitungsverzeichnisses gilt für Unternehmen mit weniger als 250 Mitarbeitern – nur - dann nicht, wenn

- die Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt,
- die Verarbeitung nur gelegentlich erfolgt und
- die Verarbeitung keine sensiblen Daten bzw. keine Daten über strafrechtliche Verurteilungen beinhaltet.

Geldstrafen

Die Verletzung der Dokumentationspflicht ist mit bis zu EUR 10 Mio. oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

Relevante Artikel der DSGVO: Art 30-31
Relevante Erwägungsgründe: 13, 75, 76, 82, 89

Stand: 03.03.2021