DATENSCHUTZ – D11

Stand: März 2018

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

Verzeichnis von Verarbeitungstätigkeiten

Werden personenbezogene Daten im Unternehmen verarbeitet, ist darüber ein Verzeichnis von Verarbeitungstätigkeiten anzufertigen. Das Verzeichnis der Verarbeitungstätigkeiten löst das aus dem BDSG bekannte Verfahrensverzeichnis ab. Das Verzeichnis umfasst sämtliche automatisierte Verarbeitungen sowie nicht-automatisierte Verarbeitungen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. In der Praxis besteht das Verzeichnis in der Regel aus mehreren einzelnen Verfahrensbeschreibungen, die in der Summe ein Verfahrensverzeichnis ergeben.

Das Verfahrensverzeichnis spielt eine wichtige Rolle beim **Aufbau eines Datenschutzmanagements**. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können. Das Verzeichnis hilft zudem dem Unternehmen dabei seinen **Dokumentations- und Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO** nachzukommen. Aus diesem Grund ist es auch aus eigenem Interesse ratsam, ein vollständiges Verzeichnis zu erstellen. **Aber**: Mit der Erstellung des Verzeichnisses ist nur ein erster Schritt getan, um seinen Verpflichtungen nach der DSGVO nachzukommen. Darüber hinaus muss die Ordnungsgemäßheit der gesamten Verarbeitung oder auch das Vorhandensein von Einwilligungen nachgewiesen werden.

Muss mein Unternehmen ein Verfahrensverzeichnis erstellen?

Art 30 DSGVO schreibt vor, wann ein Verzeichnis erstellt werden muss. Eine Pflicht zur Erstellung besteht danach, wenn das Unternehmen

- mehr als 250 Mitarbeiter beschäftigt;
- die Verarbeitungen ein Risiko für die Rechte und Freiheiten der Betroffenen darstellt (z. B. Videoüberwachung, Ortung von Mitarbeitern mittels GPS);
- besondere Kategorien von Daten verarbeitet (z. B. Religionsdaten, Gesundheitsdaten) oder
- nicht nur gelegentlich personenbezogene Daten verarbeitet.

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

Die letzte Alternative wird wohl auf die allermeisten Unternehmen zutreffen, da in der Regel zumindest Kunden- und/oder Beschäftigtendaten verarbeitet werden.

Beispiel: *Das Unternehmen A verkauft Sportartikel in seinem Ladengeschäft. Dazu hat es drei Mitarbeiter angestellt. Für die Anstellung benötigt das Unternehmen verschiedene Daten (z.B. Name, Anschrift, Sozialversicherungsnummer) seiner Mitarbeiter. Kunde B möchte gerne eine Hose bestellen, die im Ladengeschäft nicht mehr verfügbar ist. Zu diesem Zweck notiert sich Mitarbeiter C die Daten des Kunden, um ihn bei Erhalt der Ware informieren zu können. A muss ein Verzeichnis über die Beschäftigtendaten und eines über die Kundendaten anlegen.*

Die Verpflichtung, ein Verfahrensverzeichnis zu erstellen besteht künftig auch für den **Auftragsverarbeiter**, Art. 30 Abs. 2 DSGVO.

Welche Angaben muss das Verzeichnis enthalten?

Art. 30 DSGVO nennt die Angaben, die das Verzeichnis enthalten muss:

- den Namen und die Kontaktdaten des **Verantwortlichen** und gegebenenfalls des Vertreters;

  Beispiel: Max Mustermann GmbH
  Geschäftsführer: Max Mustermann
  Mustermannstr. 1
  66123 Musterstadt
  Tel: 0681-1234-0
  Fax: 0681-1234-1
  E-Mail: info@maxmustermann.de

- den Namen und die Kontaktdaten des **Datenschutzbeauftragten,** soweit einer bestellt wurde;

  Beispiel: Eva Musterfrau
  Musterfraustr. 1,66123 Musterstadt (wenn extern)
  Tel: 0681-1234-2
  Fax: 0681-1234-3
  E-Mail: info@evamusterfrau.de

- die **Zwecke der Verarbeitung,** z. B.:
  - Lohn-, Gehalts- und Bezügeabrechnung
  - Arbeitszeiterfassung
  - Videoüberwachung
  - Kundendatenbank
  - Lieferantenliste
  - Internetseite

- eine Beschreibung der **Kategorien betroffener Personen,** z. B.:
  - Mitarbeiter
  - Kunden
  - Lieferanten
  - Bewerber
- eine Beschreibung der **Kategorien personenbezogener Daten,** z. B.:
  - Kontaktdaten
  - Steuernummer
  - Mitarbeiter-Stammdaten
  - Kontoverbindung
  - Bonitätsdaten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen: *Hier sind externe aber auch interne Stellen zu nennen, die die Daten erhalten, z. B.:*
  - Steuerberater
  - Paketdienstleiter
  - Auftragsverarbeiter
  - Banken
  - Personalrat/Betriebsrat
- die **Angabe von Drittländern** oder internationale Organisationen, an die die Daten übermittelt werden sowie die Dokumentierung geeigneter Garantien: *Eine Übermittlung in Drittländer findet auch statt, wenn sich dort der Server befindet oder Supportdienstleistungen aus diesem erbracht werden.*
- wann die **Daten gelöscht** werden: *Es existieren teilweise gesetzliche Aufbewahrungspflichten, die zu beachten sind. In allen Fällen sollte ein Löschkonzept entworfen werden.*
- eine **Beschreibung der technischen und organisatorischen Maßnahmen:** *Wie bisher auch müssen die technischen und organisatorischen Maßnahmen beschrieben werden, die zum Schutz der Rechte und Freiheiten der Betroffenen eingerichtet wurden. Dies kann z. B. durch ein Sicherheitskonzept erfolgen.*
  - Pseudonymisierung/Verschlüsselung personenbezogener Daten;
  - Gewährleistung der Integrität und Vertraulichkeit, der Verfügbarkeit und Belastbarkeit der Systeme und Dienste;
  - Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen

Wichtig: *Die gemachten Angaben müssen die Verarbeitungstätigkeiten aussagekräftig beschreiben.*

Wichtig: *Unternehmen, die bereits in der Vergangenheit ein Verfahrensverzeichnis geführt haben, sollten Ihr Verzeichnis überprüfen und dieses gegebenenfalls an die neuen Vorgaben anpassen.*

Wer hat das Verzeichnis zu erstellen und wie muss es geführt werden?

Die Erstellung des Verfahrensverzeichnisses ist laut DSGVO Chefsache. Der „Verantwortliche“ kann diese Aufgabe an einen Dritten delegieren. Aber: Verantwortlich bleibt weiterhin der Unternehmer!

Das Verzeichnis ist **schriftlich** zu führen. Dies kann auch in einem **elektronischen Format** erfolgen. Anders als bisher besteht kein Einsichtsrecht für jedermann in das Verzeichnis. Ebenfalls weggefallen ist die Meldepflicht an die Aufsichtsbehörde. Die **Aufsichtsbehörde** hat aber das Recht, **auf Anfrage Einsicht** in das Verfahrensverzeichnis zu nehmen. Verlangt die Aufsichtsbehörde Einsicht, kann sie verlangen, dass das elektronische Verzeichnis ausgedruckt wird.

Das Verzeichnis ist regelmäßig **in deutscher Sprache** zu führen (Art. 30 Abs. 4 DSGVO, ErwGr. 82, Working Paper 243 der Art. 29-Gruppe, Ziff. 2.3).

Bei Änderungen des einzelnen Verfahrens ist das Verzeichnis anzupassen. Die Änderungen sind zu dokumentieren.

Rechtsfolgen bei Verstoß

Fehlt ein Verfahrensverzeichnis oder wird dieses nicht vollständig geführt bzw. der Aufsichtsbehörde auf Anfrage nicht vorgelegt, kann eine Geldbuße verhängt werden.

Muster-Vorlage für ein Verzeichnis

Die Aufsichtsbehörde des Saarlandes stellt ein Muster für ein Verarbeitungsverzeichnis zur Verfügung. Einen Link dazu finden Sie auf unserer Internetseite unter www.saarland.ihk.de unter der **Kennzahl 2158** unter dem Stichwort Verweise.