Dokumentationspflicht
Hinweise für Handwerksbetriebe

Weshalb ist eine Dokumentation nötig?

Handwerksbetriebe, die personenbezogene Daten verarbeiten, sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden. Auf Grundlage dieser Übersicht sollen sich Betriebsinhaber über das Ausmaß und die Intensität der betrieblichen Datenverarbeitung bewusst werden.

Die Pflicht zur Dokumentation der Datenverarbeitungsprozesse sowie die konkreten Anforderungen an die Dokumentation sind in Artikel 30 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt.

Was ist zu dokumentieren?

Nach Art. 30 DSGVO sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in den unterschiedlichsten betrieblichen Situationen vorkommen (z.B. Erstellung und Veränderung der Kundendatei, Verwaltung der Mitarbeiterakten, Verwendung einer Kamera im Betrieb).

Wie ist der Ablauf der Dokumentation?

Schritt 1: Risikobewertung

Im ersten Schritt ist zu bewerten, ob die Datenverarbeitung ein hohes oder geringes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind (z.B. betriebliche Videoüberwachung mit Blick auf eine öffentliche Straße). Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten, ethnische Herkunft, religiöse Zugehörigkeit) umfangreich verarbeitet werden. Dies ist bei Handwerksbetrieben gewöhnlich nicht der Fall. Ausnahmen sind in der Regel jedoch Betriebe der Gesundheitshandwerke oder große Betriebe mit vielen Mitarbeitern, die in der Personalabteilung solche Daten umfangreich verarbeiten.

Sollte ausnahmsweise ein hohes Risiko bestehen, ist eine „Datenschutz-Folgenabschätzung“ vorzunehmen. Die Anforderungen dieser Folgenabschätzung richten sich nach Art. 35 DSGVO und umfassen folgende Prüfungspunkte:

- eine Beschreibung der geplanten Verarbeitungsvorgänge,
- eine Beschreibung der Zwecke der Verarbeitung,
- eine Bewertung der Notwendigkeit der Verarbeitungsvorgänge,
- eine Bewertung der Risiken für die Personen, deren Daten verarbeitet werden sollen,
- eine Beschreibung der Maßnahmen, die zur Bewältigung der Risiken vorgesehen werden.

Schritt 2: Erstellen des Verarbeitungsverzeichnisses

Art. 30 DSGV zählt die Punkte auf, die in einem Verarbeitungsverzeichnis enthalten sein müssen. Dies sind im Einzelnen:

- **Name und die Kontaktdaten des Betriebs** (bei juristischen Personen zudem Name des Vertreters, z.B. Name des Geschäftsführers)

- **Name und Kontaktdaten des Datenschutzbeauftragten** (DSB): Nur erforderlich, wenn ein DSB bestellt wurde (zur Frage wann DSB zu bestellen ist, siehe *Praxis Datenschutz* zum betrieblichen DSB).

- **Zwecke der Verarbeitung**: Z.B. für Werbemaßnahmen oder zur Abwicklung eines Vertrags.

- Beschreibung der **Kategorien betroffener Personen**: Z.B. Kunden, Mitarbeiter, Zulieferer etc.

- Beschreibung der **Kategorien personenbezogener Daten**: Werden z.B. einfache Adressdaten oder besonders sensible Daten wie z.B. Gesundheitsdaten erhoben?

- **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden: Gilt nur, wenn die Daten an Dritte weitergeleitet werden (z.B. Weitergabe von Daten an die Creditreform).

- Wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien: In der Regel gilt, dass Daten zu löschen sind, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden.

- Wenn möglich, eine Beschreibung der **technischen und organisatorischen Maßnahmen** (siehe hierzu nachfolgend).

Technische und organisatorische Maßnahmen

Betriebe sind verpflichtet, Maßnahmen auf dem Stand der Technik zu ergreifen, um den Risiken zu begegnen, die mit der Datenverarbeitung einhergehen. § 64 Bundesdatenschutzgesetz zählt zahlreiche Maßnahmen auf, die zu berücksichtigen sind. Diese lassen sich thematisch auf folgende Kernmaßnahmen zusammenfassen:

- **Vertraulichkeit der Datenverarbeitung**
  (u.a. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle) Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden (z.B. Abschließen des Serverraums).

- **Integrität der Datenverarbeitung**
  (u.a. Eingabekontrolle/ Verarbeitungskontrolle) Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (z.B. Verwendung individueller Benutzernamen).

- **Verfügbarkeitskontrolle**
  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können (z.B. Installierung von Geräten zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen).

- **Trennungsgebot**
  Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (z.B. Trennung von Daten verschiedener Auftraggeber).

Muster eines Verarbeitungsverzeichnisses

Ein Muster für ein Verarbeitungsverzeichnis ist als Anlage 1 beigefügt. Anlage 2 enthält ein ausgefülltes Beispiel. Zudem befindet sich in Anlage 3 eine Checkliste möglicher heranzuziehender technischer und organisatorischer Maßnahmen.