

Wichtige Maßnahmen in der Zusammenfassung.

1. Dokumentation

Zunächst muss dokumentiert werden, welche Daten in welcher Form und wem sowohl innerbetrieblich und auch außerbetrieblich zugänglich gemacht werden. Ein Verarbeitungsverzeichnis ist zu erstellen.

2. Risikobewertung

Auf Grundlage des Verarbeitungsverzeichnisses ist eine Risikobewertung vorzunehmen: Wie könnten Daten in unbefugte Hände geraten und wie hoch ist hierfür die Wahrscheinlichkeit? Diese Risikobetrachtung ist Bestandteil des Verarbeitungsverzeichnisses. Bei Cloud-Diensten ist darauf entsprechende Vorkehrungen des Anbieters zu achten.

3. Sicherungsmaßnahmen

Entsprechend dem festgestellten Risiko besteht die Verpflichtung, "technische und organisatorische Maßnahmen" zu ergreifen. Das können Virenschutz, Passwörter, Löschfristen oder auch Einbruchschutzmaßnahmen sein. Maßnahmen welche die IT-Sicherheit eines Unternehmens garantieren sollen, müssen dem Stand der Technik entsprechen.

Die Datenverarbeitung über einen externen Dienstleister abzuwickeln, kann hier viel Erleichterung bringen.

4. Einwilligungserklärung / Auskunftsrecht / Löschungsrecht

Auch die Rechte der Betroffenen, also der Menschen, deren persönliche Daten verarbeitet werden, wurden gestärkt. Daher müssen Betriebe z.B. bei Versendung von Newsletter-Beiträgen von ihren Kunden Einwilligungserklärungen unterzeichnen lassen und aufbewahren. Zusätzlich ist die Zusendung von Informationen zur Datenerhebung an Kunden und potenzielle Kunden verpflichtend.

Insbesondere wenn es sich um Gesundheitsdaten handelt, ist höchste Sorgfalt beim Schutz der Daten gefordert. „Betroffene“ (Personen, deren Daten verarbeitet werden) haben zudem weitreichende Rechte auf Auskunft über die Datenweitergabe und das Recht auf Löschung der Daten gegenüber dem „Verantwortlichen“ (also dem „Datenverarbeiter“).

5. Anzeigepflicht

Unternehmen sind ab 25.05.2018 verpflichtet, Datenpannen innerhalb von 72 Stunden beim Landesdatenschutzbeauftragten Baden-Württemberg sowie den Betroffenen zu melden. Dies gilt für alle Arten von Daten.

6. Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn ein Betrieb zwar personenbezogene Daten für seine Zwecke nutzt, die tatsächliche Verarbeitung und Aufbereitung dieser Daten aber nicht selbst durchführt, sondern von einem Dienstleister vornehmen lässt. Der Dienstleister verarbeitet die Daten für und im Auftrag des Betriebs. Dies ist z.B. bei Anbietern von Cloud-Lösungen der Fall, die auf ihren Servern Daten für den Betrieb speichern. Dasselbe gilt für Steuerberater, die für den Betrieb die Steuerklärungen erstellen und dabei z.B. Rechnungen (Adressdaten der Kunden) verarbeiten.

7. Weitere Maßnahmen

Betriebe, die in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, benötigen einen betrieblichen Datenschutzbeauftragten. Dieser überwacht das vorgesehene Schutzniveau und kümmert sich um die Einhaltung der komplexen Vorgaben. Auch für kleinere Betriebe könnte es hilfreich sein, externe Beratung in Anspruch zu nehmen. Alternativ kann ein Mitarbeiter/eine Mitarbeiterin weiter qualifiziert werden.

Externe Datenschutzbeauftragte (nur die im BvD e.V. organisierten) finden sie [hier](#).

Bei Datenverarbeitungsdienstleistern sollte man zudem auf deutsche oder EU-weit tätige Anbieter zugreifen und die Einhaltung der EU-DSGVO im Vertrag absichern. Werden über andere Dienstleister Kundendaten ausgetauscht, wie z. B. über die US-amerikanischen Anbieter Whats-App oder Dropbox, liegt eine unerlaubte „Übermittlung an Drittstaaten“ vor, falls keine entsprechende Einwilligung der betroffenen Person vorliegt.

8. Datenschutzerklärung auf der Website

Jede Website muss eine [Datenschutzerklärung](#) aufweisen.

Erstellen Sie keine Datenschutzerklärung für Ihre Homepage, droht Ihnen eine Abmahnung. Dabei werden Ihnen die Abmahnkosten von ca. 100 bis 200 Euro in Rechnung gestellt.

Gemäß der deutschen und europäischen Rechtsprechung gilt eine fehlende oder unzureichende Datenschutzerklärung auf einer gewerblichen Website als Wettbewerbsverstoß. Das bedeutet, dass Konkurrenten (Mitbewerber) Abmahnungen versenden, Schadensersatz einfordern und auf Unterlassung pochen können.

Seit Anfang 2016 können nicht nur Mitbewerber, sondern auch Verbraucherschutzverbände Abmahnungen wegen fehlender Datenschutzerklärungen versenden.

Download wichtiger Dokumente und Mustervorlagen.

Nützliche Broschüren und links

- Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, C.H.Beck-Verlag, ISBN 978-3-406-71662-1, 5,50€, Bezug z.B. über den Buchhandel
- Alle Mustervorlagen und Infoblätter vom Zentralverband des Deutschen Handwerks ZDH: <https://www.zdh.de/fachbereiche/organisation-und-recht/datenschutz/datenschutz-fuer-handwerksbetriebe/>

Unsere Weiterbildungsangebote

- <https://www.hwk-ulm.de/dsgvo-workshops-2018/>