Was kommt auf Sie zu?

Zulässigkeit der Datenverarbeitung

Eine Datennutzung ist **ohne Einwilligung** des Betroffenen erlaubt wenn diese:

- für die Erfüllung eines Vertrages,
- die Durchführung vorvertraglicher Maßnahmen oder
- die Wahrnehmung berechtigter Interessen des Betriebes

  erforderlich ist. Typischerweise also in den Fällen, in denen Sie die Adresse des Kunden verwenden, um einen Auftrag vor Ort auszuführen. Weitere Fälle der Datenerhebung zum Zwecke der Vertragsabwicklung wären das Nutzen einer Emailadresse, um wunschgemäß ein Angebot zuzusenden oder das Auswerten Ihrer Kundendatei, um den Kunden zielgerichtet mit Werbung anzusprechen.
  Achtung: Direktwerbung per Email oder Telefon ist weiterhin nur bei ausdrücklichem Einverständnis des Kunden zulässig!

Betriebe der **Gesundheitshandwerke** sind nach dem Bundesdatenschutzgesetz zusätzlich berechtigt, z.B Dioptrienzahl, Gehörschädigung etc. als **besonders schutzwürdige** Daten zu verarbeiten, wenn diese

- zum Zweck der Gesundheitsvorsorge,
- zur Versorgung oder Behandlung im Gesundheits-oder Sozialbereich,
- zur Abwicklung eines Vertrages zwischen dem Betroffenen und dem Gesundheitshandwerksbetrieb

  notwendig sind.

Die **Verarbeitung von Mitarbeiterdaten** ist zulässig, wenn diese:

- zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses (Bsp. Speicherung von Lohnunterlagen und Krankheitstagen) oder
- zur Ausübung der Interessensvertretung der Arbeitnehmer notwendig sind (Weiterleiten der Daten an den Betriebsrat).
-

Für die **Datennutzung zu anderen** als den oben genannten **Zwecken** benötigen Sie die **Einwilligung** des Betroffenen.

Muster Einwilligung

Pflichten für alle Betriebe

I. Dokumentationspflicht

Alle Betriebe haben ein Verzeichnis zu führen über alle Tätigkeiten, bei denen personenbezogene Daten verarbeitet werden (Erstellung/Veränderung einer Kundenkartei, Verwaltung von Mitarbeiterakten, Verwendung von Kameras). Dies soll in zwei Schritten erfolgen:

1. **Erstellen des Verzeichnisses mit folgendem Inhalt:**
   - Name und Kontaktdaten des Betriebes (bei juristischen Personen Geschäftsführer/-in oder Vertreter)
   - Name und Kontaktdaten des Datenschutzbeauftragten (soweit einer zu bestellen ist)
   - Zweck der Verarbeitung bspw. Werbung oder Abwicklung des Vertrages
   - Kategorie betroffener Personen (Kunden, Mitarbeiter, Zulieferer)
   - Kategorie personenbezogener Daten (nur Adressdaten oder evtl. auch Gesundheitsdaten)
   - (bei Weitergabe) Kategorie von Empfängern
   - Wenn möglich: Fristen für die Löschung und Beschreibung der technischen und organisatorischen Maßnahmen zur Abwehr der Risiken

2. Es ist zudem eine **Risikobewertung durchzuführen**, welche nach Anzahl der Betroffenen und Schutzwürdigkeit der erhobenen Daten differenziert. Wenn Sie lediglich Kunden- und Mitarbeiterdaten zum Zwecke der Vertragsabwicklung erheben, besteht kein erhöhtes Risiko für die Betroffenen (siehe Punkt 2. des Muster- Verarbeitungsverzeichnisses; hier kann in der Regel „nein“ angekreuzt werden).

   Bei Betrieben der Gesundheitshandwerke, die besonders schutzwürdige Daten verarbeiten, ist eine Datenschutzfolgeabschätzung Art. 35 DSGVO durchzuführen. Für diese Daten ist eine besondere Sicherung gegen den unbefugten Zugriff zu gewährleisten. Hierzu empfiehlt sich eine gesonderte individuelle Beratung durch Ihren IT- Anbieter.

Muster für ein **Verarbeitungsverzeichnis**

II. Informationspflicht bei Datenerhebung

Wenn Sie die Daten **direkt bei dem Betroffenen** erheben (zum Beispiel durch Abfragen der Adresse oder Emailadresse), sind Sie verpflichtet, demjenigen folgende Informationen zur Verfügung zu stellen:

- Identität des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zweck der Datennutzung, Rechtsgrundlage der Datenerhebung (alternativ Einwilligung)
- Dauer der Verarbeitung

- bei der regelmäßigen Weitergabe der Daten (Creditreform); über die Identität des Empfängers
- seine Rechte (Auskunftsrecht, Widerspruchsrecht Recht auf Vergessen werden / Löschung etc.)
- Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde
- Hinweis, ob die Bereitstellung der Daten für Abwicklung des Vertrages erforderlich ist

Ausnahmefall:
Weitere besondere Informationspflichten entstehen, wenn die **Erhebung der Daten bei Dritten** stattfindet (Adressenkauf).
Auch wenn Sie die Daten zu anderen Zwecken nutzen wollen, als bei der ursprünglichen Erhebung angegeben, müssen Sie Ihren Kunden hierüber informieren.

Achtung: Hier dürfte regelmäßig zusätzlich die Einwilligung des Betroffenen erforderlich sein.

Praxistipp:

Um etwaige Abmahnungen zu vermeiden, fügen Sie Ihrem Angebot oder Ihrer Auftragsbestätigung einen kurzen Text mit den nötigen Angaben bei.

Muster Informationserteilung

III. Technische und organisatorische Maßnahmen, die Betriebe zu ergreifen haben

Betriebe sind verpflichtet Maßnahmen zu ergreifen, um Risiken der Datenverarbeitung zu begegnen. Dies sind beispielsweise Maßnahmen, die garantieren, dass:

- Unbefugte keinen Zugang zu den Datenverarbeitungsanlagen haben
- nachträglich überprüft werden kann, von wem die Daten eingegeben, verändert oder entfernt wurden
- die Daten gegen Zerstörung und Verlust gesichert sind
- Daten die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden können

Es empfiehlt sich die gesonderte Beratung durch Ihren IT-Anbieter.

Beispielliste für mögliche technische und organisatorische Maßnahmen

Welche Betriebe müssen einen Datenschutzbeauftragten benennen?

Betriebe bei denen mehr als **9 Personen ständig** mit der automatisierten **Verarbeitung personenbezogener Daten** beschäftigt sind, müssen zusätzlich einen Datenschutzbeauftragten (DSB) benennen. Als automatisierte Verarbeitung gelten beispielsweise die Nutzung digitaler Kundendaten, Verwendung von Kundendaten auf dem Tablet oder Smartphone. Der Zugriff auf die Kundendatei vom Smartphone/ Tablet wäre hiervon umfasst, das bloße Zusenden von Kundenadressen zur Auftragsabwicklung per Email oder Whatsapp nicht.

Folgendes ist bei der Auswahl des DSB zu beachten:

- Kann sowohl Mitarbeiter als auch ein externer Dienstleister sein
- für mehrere Filialen reicht ein DSB
- fachliche Qualifikation (Recht, IT)
- kein Interessenskonflikt (Vorstand/Geschäftsführung/ Leiter EDV/ Personalwesen)
- die Kontaktdaten des DSB sind zu veröffentlichen und der Aufsichtsbehörde zu melden (namentliche Nennung nicht zwingend)
- es drohen Bußgelder bei Nichtbestellung

Muster für die **Bestellung eines Datenschutzbeauftragten**

Pflichten der Betriebe auf Antrag/Nachfrage des Betroffenen

Auf Anfrage des Betroffenen treffen alle Betriebe folgende Pflichten:

- Auskunftspflicht über gespeicherte Daten
- Pflicht die Verarbeitung einzuschränken, wenn die Datenverarbeitung unrechtmäßig ist (zum Beispiel ohne gesetzliche Grundlage oder Einwilligung geschieht) oder wenn Richtigkeit der Daten überprüft werden muss
- Wenn der Betroffene der Datennutzung zum Zwecke der Direktwerbung widerspricht, müssen Sie diese unterlassen.
- Pflicht zur Berichtigung (wenn der Betroffenen Ihnen mitteilt, dass seine Daten zum Teil falsch sind)
- Pflicht zur Löschung, sofern die Daten nicht mehr gebraucht werden. Zum Beispiel nach Ende der Gewährleistungsfrist.
- Beachten Sie hierbei die Aufbewahrungsfristen für Rechnungen.
- Transparenzgebot: die Anfragen des Betroffenen sind präzise, transparent, verständlich und in leicht zugänglicher Weise, sowie in einer klaren und einfachen Sprache unverzüglich zu bearbeiten.