Top 10 der wichtigsten Punkte

- ☑ *Eigene Beschäftigte sensibilisieren und unterrichten*
- ☑ *Kundschaft über die Verarbeitung informieren*
- ☑ *Datenschutzerklärung auf der Webseite einbinden*
- ☑ *Verzeichnis der Verarbeitungstätigkeiten erstellen*
- ☑ *Regelmäßige Datensicherungen durchführen*
- ☑ *Betroffenenrechte beachten (Auskunft, Löschung)*
- ☑ *Verträge zur Auftragsverarbeitung abschließen*
- ☑ *Webseite überprüfen und sicher halten*
- ☑ *Videoüberwachung kennzeichnen*
- ☑ *Datenpannen einfach online melden*

Erläuterungen hierzu finden Sie auf
www.lda.bayern.de/top10

Zentrale Datenschutzthemen

Unser Webangebot für Sie:

Mehr Informationen unter
www.lda.bayern.de

HERAUSGEBER
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Bayerisches Landesamt für Datenschutzaufsicht

Datenschutz für Bayern

DS-GVO einfach umgesetzt in Unternehmen

Zielgruppe dieses Flyers

Der Fokus dieses Flyers liegt auf **kleineren Unternehmen mit bis zu 50 Beschäftigten**.

Die genannten Datenschutzanforderungen betreffen daher viele Unternehmen aus dem Handwerks-, Einzelhandels-, Dienstleistungs- und freiberuflichen Bereich.

INFORMATIONSPFLICHTEN

Jedes Unternehmen hat seiner Kundschaft und seinen Beschäftigten schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss es darauf hinweisen, wo die Informationen leicht zugänglich sind.

Bestellt jemand eine Ware online, sind die Informationen im Bestellprozess **auf der Webseite** zu erteilen. Erfolgt die Bestellung im Ladengeschäft, sollten die wichtigsten Informationen in einem **Bestellformular** oder Beiblatt enthalten sein – detailliertere Informationen können z. B. auf der Homepage oder in einem Aushang erteilt werden.

SICHERHEIT DER VERARBEITUNG

Um die Daten der Kundschaft angemessen zu schützen, müssen kleinere Unternehmen meist nur die **Standard-sicherheitsmaßnahmen** nutzen. Darunter fällt bspw. der Einsatz aktueller Betriebssysteme, Passwortschutz an den Arbeitsplätzen und regelmäßige Backups.

Damit Unbefugte nicht an die schutzwürdigen Daten herankommen, sind die Datenbanken selbst besonders abzusichern. CRM-Systeme zur Verwaltung der Daten der Kundinnen und Kunden unterstützen meist eine **verschlüsselte Speicherung**.

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Unternehmen gehen im Alltag mit vielen personenbezogenen Daten um, insbesondere mit den Daten ihrer Kundschaft und ihrer Beschäftigten.

Deshalb besteht meist auch für kleine Unternehmen die **gesetzliche Verpflichtung**, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Aus diesem ist dann ersichtlich, welche Daten (Kategorien) zu welchem Zweck verarbeitet werden.

Wie so etwas aussehen kann, zeigt das BayLDA auf seiner Webseite für typische Branchen in **Muster-Verzeichnissen**.

EINWILLIGUNGEN

Für die Bearbeitung von **Warenbestellungen** oder **Dienstleistungen** ist i. d. R. **keine Einwilligung** der Kundschaft nötig.

Wenn Einwilligungen eingeholt werden müssen, z. B. für Telefonwerbung, muss dazu verständlich informiert werden. Für eine Einwilligung ist eine **aktive Zustimmung** notwendig. Aus Beweisgründen ist eine schriftliche bzw. elektronisch dokumentierte Form empfehlenswert.

Bestehende Einwilligungstexte sind an die DS-GVO anzupassen und müssen auch einen Hinweis der **Widerrufbarkeit** der Einwilligung beinhalten.

DATENSCHUTZVERLETZUNGEN

Kommt es im Unternehmen zu Sicherheitsvorfällen im Umgang mit personenbezogen Daten, so besteht eine **gesetzliche Meldepflicht** beim BayLDA als Aufsichtsbehörde.

Beispiele solcher Datenschutzverletzungen:

- Diebstahl oder Verlust eines Notebooks
- Verschlüsselungstrojaner per E-Mail
- Hacking-Angriff auf die Unternehmenswebsite

Die Kundschaft und die Beschäftigten sind übrigens nur zu informieren, wenn ein hohes Datenschutzrisiko für diese besteht (was die Ausnahme ist).

RECHTE DER KUNDSCHAFT UND DER BESCHÄFTIGTEN

In der DS-GVO werden Personen, deren Daten verarbeitet werden, eine Reihe von Rechten eingeräumt.

Diese Personen können vom Unternehmen jederzeit **Auskunft** über die Verarbeitung ihrer Daten verlangen.

Sobald keine gesetzliche Grundlage mehr für die Speicherung der Daten besteht, sind sie zu **löschen** – z. B. wenn nach zehn Jahren die steuerlichen Aufbewahrungsfristen abgelaufen sind.

WERBUNG

Briefwerbung ist für Unternehmen nach DS-GVO grundsätzlich ohne Einwilligung erlaubt. Für E-Mail-Werbung gilt dies dagegen nur bei Bestandskundinnen und -kunden.

Dabei ist jeweils auf das **Recht zum Widerspruch** gegen eine werbliche Nutzung der Kontaktdaten hinzuweisen.

Für die werbliche Nutzung von Telefonnummern (Verbraucherinnen und Verbraucher) sowie bei der Verwendung von E-Mail-Adressen bei neuer Kundschaft ist stets deren vorherige Einwilligung nötig.

DATENSCHUTZBEAUFTRAGTE/R (DSB)

Bei kleineren Unternehmen besteht häufig keine Pflicht, eine(n) DSB zu benennen.

Nur wenn in der Regel **mindestens zehn Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (**Schwerpunkt ihrer Tätigkeit**), wäre dies der Fall.

Zu den zehn Personen können Beschäftigte im Personal- und Vertriebsbereich zählen, nicht jedoch Reinigungskräfte.