digitalcourage

# Wichtige Punkte, die ein Datenschutzkonzept beachten sollte

- Ein gutes Datenschutzkonzept hält die gesetzlichen Bestimmungen ein und ermöglicht allen, für die es geschrieben wurde, verantwortungsvollen Umgang mit den eigenen Daten. Es ist nicht nur vernünftig, sondern auch ein Zeichen von Respekt, mit den Daten von Kund.innen und Mitarbeiter.innen sorgsam umzugehen.
    - **Opt-in** bedeutet, dass Kund.innen bewusst einen Haken setzen oder ihre Zustimmung per E-Mail bekunden müssen, wenn sie zum Beispiel einen Newsletter beziehen möchten.
    - **Datensparsamkeit**: Erheben Sie nur Daten, die Sie für die Dienstleistung und zur Abrechnung brauchen. Löschen Sie alle Daten, die nicht mehr nötig sind.
    - **Verarbeitungsverzeichnis**: Schreiben Sie genau auf, wie Sie persönliche Daten verarbeiten. Näheres bei den Datenschutzbeauftragten.
    - **Datenschutzfreundliche Gestaltung** ist nicht nur für Websites vorgeschrieben, sondern auch für Apps. Achten Sie bei den Anwendungen, die Sie bereitstellen, ebenfalls auf „Datenschutz per Voreinstellung“ (*privacy by design*).
- Ermöglichen Sie **anonymes Bezahlen**, also nicht nur mit Kreditkarte, Bankeinzug oder gar Paypal. Vielleicht ist sogar Barzahlung beziehungsweise Nachnahme eine Option, nach dem alten Grundsatz „Erst die Ware, dann das Geld".
- Vertrauliche Kommunikation **darf Geld kosten**. Es muss ja nicht gleich ein eigener Server sein. Vertrauenswürdige E-Mail-Dienstanbieter sind nicht teuer. Sie sind ihr Geld wert.
- **Achtung mit kostenlosen Diensten**. Speichern Sie Kund.innendaten und Informationen über die Belegschaft nicht in Googletabellen oder ähnlichen Vorlagen.
- Verlangen Sie nicht, dass Ihre Mitarbeiter.innen für den **dienstlichen Account persönliche Daten** verwenden. Schließlich durchschnüffelt Facebook jeden Browser und kann berufliche und private Daten zusammenführen. Auch wer für Dienstliches kein Extragerät hat und sich mit dem Privatrechner in den Dienstaccount einloggt, kann auf diese Weise ausspioniert werden.
- Überwachen Sie Ihre Mitarbeiter.innen **nicht mit Video**.
- **Schulen** Sie die Belegschaft im sensiblen Umgang mit Daten und Passwörtern.
- Geben Sie die **Daten von Kund.innen** nicht weiter. Auch nicht unabsichtlich, zum Beispiel durch Ihren E-Mail- oder den Internetanbieter.
- Verfassen Sie eine kurze, verständliche **Datenschutzerklärung**. Ein vorbildliches Beispiel finden Sie bei Posteo.
- Dieses Datenschutzkonzept und weitergehende Tipps finden Sie auf unserer Website auch online: `https://digitalcourage.de/selbstverteidigung`

*Spätestens jetzt sollten Sie sich übrigens überlegen, ob Sie uns nicht zum Dank für unseren Service eine Spende zukommen lassen wollen. Denn die Recherche und Aktualisierung für diese Artikel ist viel Aufwand und wir sind ein gemeinnütziger Verein.*

Wir dürfen keine Rechtsberatung leisten. Wenn etwas unklar ist, fragen Sie Ihre.n Datenschutzbeauftragte.n oder Ihre IHK.

**Digitalcourage e.V.** | Marktstraße 18 | 33602 Bielefeld
Tel: 0521-16391639 | mail@digitalcourage.de | https://digitalcourage.de

Spenden bitte auf unser Konto mit der IBAN: DE66 4805 0161 0002 1297 99
oder spenden Sie online `https://digitalcourage.de/spende`