



# Sieben Schritte für Unternehmen



zur Vorbereitung auf die  
Datenschutz-Grundverordnung

## Wer ist angesprochen?

Diese Übersicht richtet sich an Unternehmen, die personenbezogene Daten nicht im Rahmen ihrer Kerntätigkeit verarbeiten, wie KMU, die hauptsächlich personenbezogene Daten ihrer Mitarbeiter verwenden oder Listen von Kunden oder Abnehmern führen. Dazu gehören beispielsweise auch Händler oder Geschäfte, wie eine Bäckerei oder Fleischerei, oder Dienstleister wie Architekten. In dieser Übersicht werden die wenigen Schritte vorgestellt, mit denen Ihr Unternehmen sich auf die Datenschutz-Grundverordnung vorbereiten kann.

Personenbezogene Daten sind alle Informationen, die sich auf eine lebende Einzelperson (keine juristischen Personen) beziehen. Dazu gehören zum Beispiel: Name, Vorname, Anschrift, E-Mail-Adresse oder Standortdaten vom Kartendienst auf dem Smartphone. Typischerweise sind das die Daten, die Sie von Ihren Mitarbeitern, Kunden oder Lieferanten speichern.

Je weniger  
Ihre Tätigkeit  
personenbezogene  
Daten gefährdet,  
desto weniger müssen  
Sie tun

### Anwendbare Grundsätze:

- 📌 **Sammeln Sie personenbezogene Daten zu einem klar definierten Zweck und verwenden Sie sie nicht anderweitig** (wenn Sie die E-Mail-Adresse Ihrer Kunden erfragen, um sie über Angebote oder Aktionen zu informieren, können Sie die Adresse nicht für andere Zwecke verwenden oder einem anderen Unternehmen verkaufen.)
- 📌 **Sammeln Sie nicht mehr Daten als nötig** (wenn Sie einen Lieferservice anbieten, brauchen Sie z. B. eine Adresse und einen Namen an der Klingel, aber Sie müssen nicht wissen, ob die Person verheiratet oder alleinstehend ist) – gehen Sie einfach achtsam mit den personenbezogenen Daten um, die Sie erhalten.

## SCHRITT 1

### PRÜFEN SIE DIE PERSONENBEZOGENEN DATEN, DIE SIE SAMMELN UND VERARBEITEN, DEN ZWECK UND DIE RECHTSGRUNDLAGE

Sie haben **Mitarbeiter**; Sie verarbeiten deren personenbezogenen Daten auf Grundlage des Arbeitsvertrags und gesetzlicher Verpflichtungen (z. B. Meldungen bei der Steuerbehörde oder ans Sozialsystem).

Sie können eine Liste von **Einzelkunden** führen, um ihnen zum Beispiel Ankündigungen für Sonderangebote/Aktionen zuzuschicken, wenn Sie von diesen Kunden ihre Einwilligung erhalten haben.

Die Einwilligung ist nicht immer nötig. In manchen Fällen erwarten die Personen, dass Sie ihre Daten verarbeiten. Zum Beispiel können Sie als

Pizzeria die Lieferadresse verwenden, um neue Produkte zu bewerben. Das nennt sich berechtigtes Interesse. Sie müssen aber die Person über die geplante Verwendung informieren und die Nutzung einstellen, sobald die Person das von Ihnen einfordert.

Bei der Verwaltung von **Lieferanten** oder **Geschäftskunden** arbeiten Sie auf Grundlage der jeweiligen Verträge. Die Verträge müssen nicht zwingend schriftlich geschlossen worden sein.

## SCHRITT 2

### INFORMIEREN SIE IHRE KUNDEN, ANGESTELLTEN UND DRITTE, WENN SIE DEREN PERSONENBEZOGENE DATEN SAMMELN

Personen müssen wissen, dass Sie deren personenbezogene Daten verarbeiten und zu welchem Zweck Sie dies tun.

Aber es ist nicht nötig, die Person zu informieren, wenn sie schon weiß wie Sie die Daten verwenden werden, zum Beispiel, wenn ein Kunde eine Lieferung frei Haus bestellt.

Sie müssen die Person außerdem darüber informieren, welche personenbezogenen Daten Sie von ihr haben, und ihr Zugang zu ihren Daten gewähren. Halten Sie Ordnung in Ihren Daten. Sollte Sie ein Mitarbeiter einmal fragen, welche Art von personenbezogenen Daten Sie haben, können Sie sie dann ohne zusätzlichen Aufwand angeben.

## SCHRITT 3

### BEWAHREN SIE DIE PERSONENBEZOGENEN DATEN NUR SO LANGE WIE NOTIG AUF

**Mitarbeiterdaten:** für die Dauer des Arbeitsverhältnisses und aller damit verbundenen rechtlichen Verpflichtungen.

**Kundendaten:** für die Dauer des Geschäftsverhältnisses und aller damit verbundenen rechtlichen Verpflichtungen (zum Beispiel für Steuerzwecke).

**Löschen Sie die Daten, wenn Sie sie nicht mehr für den Zweck benötigen, zu dem sie ursprünglich gesammelt wurden.**

## SCHRITT 4

### SCHÜTZEN SIE DIE PERSONENBEZOGENEN DATEN, DIE SIE VERARBEITEN

Wenn Sie die Daten in einem **IT-System** speichern, beschränken Sie den Zugang zu den entsprechenden Dateien, z. B. mit einem Passwort. Aktualisieren Sie regelmäßig die Sicherheitseinstellungen in Ihrem System. (Hinweis: die Datenschutz-Grundverordnung schreibt kein bestimmtes IT-System vor)

Wenn Sie gedruckte Dokumente mit personenbezogenen Daten lagern, stellen Sie sicher, dass Unbefugte keinen Zugriff auf sie erhalten; schließen Sie sie in einem Tresor oder einem Schrank ein.

## SCHRITT 5

### DOKUMENTIEREN SIE IHRE DATENVERARBEITUNG

Erstellen Sie ein kurzes Dokument, in dem Sie darlegen, welche personenbezogenen Daten Sie speichern und aus welchem Grund Sie dies tun. Möglicherweise müssen Sie Ihrer jeweiligen nationalen Datenschutzbehörde auf Anfrage die Dokumentation vorlegen.

Diese Dokumentation sollte die folgenden Angaben enthalten:

INFORMATION	BEISPIELE
Zweck der Datenverarbeitung	Information der Kunden über Sonderangebote/Lieferservice frei Haus; Bezahlung von Lieferanten; Gehälter und Sozialabgaben für Mitarbeiter
Arten personenbezogener Daten	Kontaktangaben von Kunden; Kontaktangaben von Lieferanten; Mitarbeiterdaten
Kategorien von betroffenen Personen, deren Daten gesammelt werden	Mitarbeiter; Kunden; Lieferanten
Kategorien von Empfängern	Arbeitsbehörden; Steuerbehörden
Aufbewahrungsfristen	Personenbezogene Daten von Mitarbeitern bis zum Ende des Arbeitsvertrags (und damit verbundenen rechtlichen Verpflichtungen); personenbezogene Daten von Kunden bis zum Ende des Geschäfts-/Vertragsverhältnisses
Technische und organisatorische Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten	IT-System wird regelmäßig aktualisiert; verschlossener Schrank/Tresor
Weiterleitung von personenbezogenen Daten an Empfänger außerhalb der EU	Verwendung eines Prozessors außerhalb der EU (z. B. zur Speicherung in einer Cloud)

## SCHRITT 6

### IHRE UNTERAUFTRAGNEHMER MÜSSEN DIE REGELN EBENFALLS EINHALTEN

Wenn Sie die Verarbeitung personenbezogener Daten in ein anderes Unternehmen auslagern, arbeiten Sie nur mit Dienstleistern, die Ihnen garantieren, dass sie bei der Verarbeitung die Vorgaben der Verordnung

beachten (zum Beispiel Sicherheitsmaßnahmen). Prüfen Sie vor der Vertragsunterzeichnung, ob der Anbieter bereits alle nötigen Änderungen im Sinne der Verordnung vorgenommen hat. Schreiben Sie das in den Vertrag.

## SCHRITT 7

### PRÜFEN SIE, OB SIE VON FOLGENDEN VORGABEN BETROFFEN SIND

> Um personenbezogene Daten besser zu schützen, kann von Organisationen verlangt werden, dass sie einen **Datenschutzbeauftragten ernennen**. **Sie müssen aber keinen Datenschutzbeauftragten ernennen**, wenn die Verarbeitung personenbezogener Daten nicht zu den Kerntätigkeiten Ihres Unternehmens gehört, keine riskante Verarbeitung stattfindet und die Verarbeitung nicht in großem Umfang stattfindet.

Wenn Ihr Unternehmen zum Beispiel nur Kundendaten für einen Lieferservice sammelt, ist kein Datenschutzbeauftragter nötig.

Selbst wenn Sie einen Datenschutzbeauftragten benötigen, kann er/sie auch ein Mitarbeiter sein, der diese Funktion zusätzlich zu seinen/

ihren anderen Aufgaben übernimmt. Oder ein externer Berater; so wie viele Firmen mit externen Steuerberatern arbeiten.

> **Normalerweise müssen Sie keine Datenschutz-Folgenabschätzung durchführen**

Solch eine Folgenabschätzung ist nur erforderlich, wenn eine größere Gefahr für die personenbezogenen Daten besteht, zum Beispiel bei Unternehmen, die öffentlich zugängliche Bereiche systematisch und umfangreich überwachen (z. B. Videoüberwachung).

Als kleines Unternehmen, das die Gehälter der Mitarbeiter und eine Liste seiner Kunden verwaltet, müssen Sie für diese Datenverarbeitung keine Datenschutz-Folgenabschätzung durchführen.

## Geldbußen

Die Datenschutzbehörden sind bevollmächtigt, Verstöße gegen die Datenschutzverordnung zu ahnden. Sie können Abhilfemaßnahmen ergreifen (wie eine Anordnung oder eine zeitweilige Aussetzung der Verarbeitung) und/oder eine Geldbuße verhängen.

Ihre Entscheidung für eine Geldbuße muss verhältnismäßig sein und auf Grundlage einer Bewertung aller Umstände des jeweiligen Einzelfalles getroffen werden.

Fällt die Entscheidung für eine Geldbuße, hängt die Höhe der Strafe auch von den Umständen des Falls ab, einschließlich der Schwere des Verstoßes und der Frage, ob der Verstoß vorsätzlich oder fahrlässig zustande kam. Die Behörde wird dabei auch Ihre Einstellung und Absichten berücksichtigen.

## Wenn Sie weitere Informationen dazu suchen:

### 1. Besuchen Sie den Online-Leitfaden der Europäischen Kommission zur Reform des Datenschutzes – verfügbar in allen EU-Sprachen:

[europa.eu/dataprotection/de](http://europa.eu/dataprotection/de)

### 2. Kontaktieren Sie Ihre nationale Datenschutzbehörde:

[edpb.europa.eu/about-edpb/board/members\\_de](http://edpb.europa.eu/about-edpb/board/members_de)

### WICHTIGER HINWEIS

Die Informationen in dieser Übersicht dienen einem besseren Verständnis der EU-Datenschutzvorschriften.

Sie dienen ausschließlich zur Orientierung. Nur der Wortlaut der Datenschutz-Grundverordnung ist rechtsverbindlich. Demzufolge begründet ausschließlich die Datenschutz-Grundverordnung Rechte und Pflichten für die betroffenen Personen. Diese Orientierungshilfe begründet weder durchsetzbare Rechte noch Ansprüche.

Die verbindliche Auslegung des EU-Rechts fällt in die ausschließliche Zuständigkeit des Gerichtshofs der Europäischen Union. Die in dieser Orientierungshilfe geäußerten Ansichten lassen den Standpunkt, den die Kommission gegebenenfalls vor dem Gerichtshof vertreten wird, unberührt.

Weder die Europäische Kommission noch irgendeine andere Person, die im Auftrag der Europäischen Kommission handelt, ist für die Nutzung der in dieser Orientierungshilfe enthaltenen Informationen verantwortlich.

Da dieses Dokument den aktuellen Stand zum Zeitpunkt seiner Ausarbeitung darstellt, sollte es als „dynamisches Instrument“ erachtet werden, das verbesserungsfähig ist. Die Inhalte können daher jederzeit ohne Vorankündigung geändert werden.

