

KOMPAKT. VERSTÄNDLICH. PRAXISNAH.



DEIN DATENSCHUTZPARTNER

DATENSCHUTZ-BASICS FÜR UNTERNEHMEN

Die wichtigsten Grundlagen, Sofortmaßnahmen
und häufigsten Fehler auf einen Blick

**Schaffe Klarheit, setze Prioritäten
und komm direkt ins Umsetzen.**

www.DEINDATENSCHUTZPARTNER.de



Warum Datenschutz für Dein Unternehmen wichtig ist

Datenschutz ist längst kein Randthema mehr. Jedes Unternehmen verarbeitet personenbezogene Daten – von Kundendaten über E-Mails bis hin zu Bewerber- und Mitarbeiterinformationen.

Wer Datenschutz im Alltag vernachlässigt, riskiert nicht nur Beschwerden, Bußgelder und Abmahnungen, sondern auch den Verlust von Vertrauen bei Kunden, Geschäftspartnern und Mitarbeitenden.

Die gute Nachricht:

Mit den richtigen Grundlagen, klaren Zuständigkeiten und wenigen praxistauglichen Maßnahmen lassen sich viele Risiken bereits deutlich reduzieren.

Was Du in unserem Leitfaden lernst

In diesem Praxis-Leitfaden erfährst:

- warum Datenschutz **Chiefsache** ist,
- was personenbezogene Daten überhaupt sind,
- welche **Pflichten** Unternehmen beachten müssen,
- welche **typischen Fehler** in der Praxis passieren,
- wie Du mit wenigen Maßnahmen schnell mehr Datenschutz im Unternehmen schaffst,
- und was Du bei **Betroffenenfragen** oder einer **Datenpanne** tun musst.



1. WARUM DATENSCHUTZ CHEFSACHE IST

Datenschutz betrifft **jedes Unternehmen** – unabhängig von Branche oder Größe.

Sobald Du mit Kundendaten, Mitarbeiterdaten, Bewerberdaten, E-Mail-Adressen oder Website-Tracking arbeitest, gelten datenschutzrechtliche Pflichten.

Warum das für die Geschäftsleitung wichtig ist

Die Verantwortung für die datenschutzkonforme Organisation liegt nicht bei der IT allein und auch nicht nur bei externen Beratern. Datenschutz ist eine **Führungsaufgabe**.

Wer Datenschutz nicht ernst nimmt, riskiert:

- Bußgelder,
- Abmahnungen,
- Vertrauensverlust,
- Reputationsschäden,
- und unnötigen Zeit- und Kostenaufwand.

Wer Datenschutz dagegen strukturiert angeht, schafft:

- Vertrauen,
- Rechtssicherheit,
- bessere interne Prozesse,
- und einen echten Wettbewerbsvorteil.



2. DIE WICHTIGSTEN GRUNDBEGRIFFE

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu gehören z. B.:

- Name
- E-Mail-Adresse
- Telefonnummer
- Anschrift
- Kundennummer
- IP-Adresse
- Fotos
- Bankdaten
- Mitarbeiterdaten

Was bedeutet „Verarbeitung“?

Verarbeitung meint praktisch jeden Umgang mit personenbezogenen Daten, z. B.:

- Erheben
- Speichern
- Verwenden
- Übermitteln
- Löschen

Schon wenn Du eine Kundenanfrage speicherst oder eine Bewerbung per E-Mail erhältst, verarbeitest Du personenbezogene Daten.



Wer ist verantwortlich?

Im Datenschutz gibt es zwei zentrale Rollen:

Verantwortlicher

Das ist das Unternehmen, das entscheidet, **welche Daten zu welchem Zweck** verarbeitet werden.

Auftragsverarbeiter

Das sind externe Dienstleister, die personenbezogene Daten **im Auftrag** des Unternehmens verarbeiten, z. B.:

- Hosting-Anbieter
- Cloud-Dienste
- Newsletter-Tools
- IT-Dienstleister
- Lohnbüros

Für solche Dienstleister ist in der Regel ein **Auftragsverarbeitungsvertrag (AVV)** erforderlich.



3. WANN DÜRFEN DATEN VERARBEITET WERDEN?

Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine **Rechtsgrundlage** vorliegt.

Die wichtigsten Rechtsgrundlagen sind:

Einwilligung

Zum Beispiel für:

- Newsletter
- nicht notwendige Cookies
- Werbeeinwilligungen

Wichtig: Die Einwilligung muss freiwillig, informiert und widerrufbar sein.

Vertragserfüllung

Zum Beispiel für:

- Bestellungen
- Rechnungsstellung
- Lieferabwicklung



Gesetzliche Pflicht

Zum Beispiel für:

- steuerliche Aufbewahrung
- handelsrechtliche Dokumentation

Berechtigtes Interesse

Zum Beispiel für:

- bestimmte Sicherheitsmaßnahmen
- technisch notwendige Website-Funktionen
- interne Organisationsprozesse

Hier ist immer eine Interessenabwägung erforderlich.



4. DIE 7 GRUNDSÄTZE DER DSGVO

Jede Datenverarbeitung muss sich an diesen Grundsätzen messen lassen:

- 1. Rechtmäßigkeit, Transparenz und Fairness** – Daten dürfen nur rechtmäßig und nachvollziehbar verarbeitet werden.
- 2. Zweckbindung** – Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden.
- 3. Datenminimierung** – Es dürfen nur so viele Daten erhoben werden, wie wirklich notwendig sind.
- 4. Richtigkeit** – Daten müssen korrekt und aktuell sein.
- 5. Speicherbegrenzung** – Daten dürfen nicht unbegrenzt gespeichert werden.
- 6. Integrität und Vertraulichkeit** – Daten müssen technisch und organisatorisch geschützt werden.
- 7. Rechenschaftspflicht** – Unternehmen müssen Datenschutz nicht nur einhalten, sondern dies auch **nachweisen können**.



5. FÜNF SOFORTMASSNAHMEN FÜR MEHR DATENSCHUTZ IM UNTERNEHMEN

Wenn Du schnell ins Handeln kommen willst, starte mit diesen fünf Punkten:

1. Datenschutzerklärung und Impressum prüfen –

Deine Website sollte ein vollständiges Impressum und eine aktuelle Datenschutzerklärung enthalten.

2. Cookie-Banner korrekt umsetzen – Nicht notwendige Cookies und Tracking-Dienste dürfen erst nach Einwilligung geladen werden.

3. Auftragsverarbeitung regeln – Für externe Dienstleister, die Daten in Deinem Auftrag verarbeiten, benötigst Du einen AVV.

4. Bewerber- und Mitarbeiterdaten schützen – Diese Daten sind besonders sensibel und sollten nur zweckgebunden, sicher und mit klaren Zugriffsbeschränkungen verarbeitet werden.

5. Sauberer Umgang im Büro und Homeoffice

Wichtige Basics sind:

- Clean Desk
- sichere Passwörter
- Bildschirmsperre
- verschlüsselte Geräte
- keine privaten Clouds für Unternehmensdaten



6. DIE HÄUFIGSTEN DATENSCHUTZFEHLER IN UNTERNEHMEN

Viele Datenschutzprobleme entstehen nicht aus bösem Willen, sondern aus Unwissenheit oder Nachlässigkeit.

Zu den häufigsten Fehlern gehören:

Fehlende wirksame Einwilligungen – Zum Beispiel bei Newslettern oder Tracking-Tools.

Unverschlüsselte E-Mails – Besonders problematisch bei sensiblen Daten.

Ungeregelte Zugriffsrechte – Nicht jeder Mitarbeitende darf alles sehen.

Unklare Zuständigkeiten – Wenn niemand verantwortlich ist, bleibt Datenschutz liegen.

Fehlende oder veraltete Dokumentation – Ohne aktuelle Unterlagen fehlt der Nachweis der DSGVO-Compliance.



7. DIE WICHTIGSTEN BETROFFENENRECHTE

Unternehmen müssen auf Anfragen betroffener Personen richtig reagieren können.

Zu den wichtigsten Betroffenenrechten gehören:

- **Auskunft**
- **Berichtigung**
- **Löschung**
- **Einschränkung der Verarbeitung**
- **Datenübertragbarkeit**
- **Widerspruch**
- **Widerruf von Einwilligungen**
- **Beschwerde bei der Aufsichtsbehörde**

Wichtig:

Diese Anfragen dürfen nicht ignoriert werden.
Unternehmen brauchen hierfür klare interne Prozesse.



8. WAS TUN BEI EINER DATENPANNE?

Datenpannen passieren schneller als gedacht, z. B. durch:

- Fehlversand von E-Mails
- verlorene USB-Sticks
- Hackerangriffe
- unberechtigte Zugriffe
- offengelegte Mitarbeiterdaten

So sollten Unternehmen reagieren

1. Ruhe bewahren und intern melden – Geschäftsleitung und Datenschutzbeauftragte informieren.

2. Vorfall dokumentieren – Was ist passiert? Welche Daten sind betroffen? Wer ist betroffen?

3. Sofortmaßnahmen ergreifen – Zugänge sperren, Systeme sichern, Schäden begrenzen.

4. Risiko bewerten – Besteht ein Risiko für Betroffene?

5. Meldepflicht prüfen – Wenn ein Risiko besteht, muss die Datenschutzbehörde innerhalb von 72 Stunden informiert werden.

6. Betroffene informieren – Wenn ein hohes Risiko besteht, müssen auch die betroffenen Personen benachrichtigt werden.

7. Nachbereitung – Ursachen analysieren und Maßnahmen verbessern.



9. DIE WICHTIGSTE ERKENNTNIS

Datenschutz ist kein einmaliges Projekt, sondern ein **laufender Unternehmensprozess**.

Mit klaren Regeln, regelmäßiger Pflege und etwas Sensibilisierung lassen sich viele Risiken zuverlässig vermeiden.

Schon wenige Grundmaßnahmen helfen dabei, Datenschutz praktikabel und alltagstauglich umzusetzen.

KURZ-CHECKLISTE: WO SOLLTEST DU SOFORT HINSCHAUEN?

Prüfe in Deinem Unternehmen insbesondere:

- Ist Deine Datenschutzerklärung aktuell?
- Ist Dein Cookie-Banner korrekt eingerichtet?
- Hast Du AV-Verträge mit relevanten Dienstleistern?
- Gibt es ein Verzeichnis von Verarbeitungstätigkeiten?
- Sind Betroffenenrechte intern geregelt?
- Gibt es einen Notfallplan für Datenpannen?
- Sind Mitarbeitende sensibilisiert?
- Sind Zugriffsrechte sauber geregelt?
- Gibt es klare Zuständigkeiten?
- Werden Daten nur so lange gespeichert, wie nötig?



FAZIT

Datenschutz ist Pflicht – aber auch eine echte Chance. Wer frühzeitig Strukturen schafft, spart später Zeit, Kosten und Ärger. Gleichzeitig stärkt ein guter Umgang mit personenbezogenen Daten das Vertrauen von Kunden, Mitarbeitenden und Geschäftspartnern.

Wenn Du Datenschutz nicht nur theoretisch verstehen, sondern konkret in Deinem Unternehmen umsetzen möchtest, lohnt sich der nächste Schritt: eine strukturierte Bestandsaufnahme Deiner Prozesse, Dokumente und Risiken.

Mehr Tiefe:

Wenn Du die Inhalte als Videoleitfaden inkl. Checklisten/Downloads nutzen willst, findest Du den kompletten Videoleitfaden auf unserer Website.

Dein nächster Schritt

Öffne folgenden Link und hol Dir unseren Videoleitfaden:

<https://deindatenschutzpartner.de/basiswissen-datenschutz-praxisleitfaden-fuer-unternehmen>

Hinweis:

Auch der Videoleitfaden ersetzt keine Rechtsberatung, liefert Dir aber praxistaugliche Orientierung und umsetzbare Prozesse.