UNTERNEHMERGEIST

Anfordeungen des Datenschutzrechts in Deutschland

Leitfaden + Checkliste

Einführung in das Datenschutzrecht

Datenschutz ist ein zentraler Bestandteil des modernen Geschäftslebens und betrifft nahezu jedes Unternehmen, das mit personenbezogenen Daten arbeitet. Die Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 in der gesamten EU gilt, stellt sicher, dass personenbezogene Daten geschützt und nur unter bestimmten Bedingungen verarbeitet werden dürfen. Ergänzend zur DSGVO gibt es in Deutschland weitere Regelungen wie das Bundesdatenschutzgesetz (BDSG) und das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG), das insbesondere den Einsatz von Cookies und Online-Tracking regelt.

Die DSGVO verfolgt das Ziel, die Rechte von Individuen zu stärken und sicherzustellen, dass Unternehmen verantwortungsvoll mit personenbezogenen Daten umgehen. Die Einhaltung dieser Vorschriften ist nicht nur eine gesetzliche Pflicht, sondern schützt auch vor hohen Bußgeldern, die bei Datenschutzverstößen verhängt werden können.
Unternehmen müssen sicherstellen, dass ihre Datenverarbeitungen transparent, sicher und im Einklang mit den gesetzlichen Vorgaben erfolgen.

Geltungsbereich der DSGVO – Wer ist betroffen?

Die DSGVO betrifft alle Unternehmen, Organisationen und Behörden, die in der EU ansässig sind oder personenbezogene Daten von EU-Bürgern verarbeiten. Auch Unternehmen außerhalb der EU müssen die DSGVO einhalten, wenn sie Waren oder Dienstleistungen für EU-Bürger anbieten oder deren Verhalten überwachen, beispielsweise durch Tracking-Tools auf Webseiten oder Apps.

Die Verordnung gilt nicht nur für große Unternehmen, sondern auch für kleine und mittlere Betriebe sowie Selbstständige, sofern sie personenbezogene Daten verarbeiten. Eine Ausnahme besteht lediglich für rein private oder familiäre Tätigkeiten, bei denen keine kommerzielle oder berufliche Verarbeitung personenbezogener Daten stattfindet.

Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Dazu gehören klassische Identifikationsmerkmale wie Name, Adresse, Telefonnummer oder Geburtsdatum, aber auch digitale Informationen wie IP-Adressen, Standortdaten oder Gerätekennungen.

Besonders sensibel sind sogenannte besondere Kategorien personenbezogener Daten, darunter:

- Gesundheitsdaten
- Politische Meinungen
- Ethnische Herkunft
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Biometrische und genetische Daten

Die Verarbeitung dieser besonderen Daten ist nur unter besonders strengen Auflagen erlaubt, um Diskriminierung und Missbrauch zu verhindern.

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

Die DSGVO erlaubt die Verarbeitung personenbezogener Daten nur, wenn eine rechtmäßige Grundlage dafür besteht. Diese kann sein:

- **Einwilligung:** Die betroffene Person hat ausdrücklich zugestimmt.
- **Vertragserfüllung:** Die Datenverarbeitung ist notwendig, um einen Vertrag zu erfüllen.

- **Gesetzliche Verpflichtung**: Die Verarbeitung ist durch eine gesetzliche Vorschrift erforderlich.
- **Berechtigtes Interesse:** Es besteht ein berechtigtes Interesse des Unternehmens, das die Rechte der betroffenen Person nicht überwiegt.

Besonders sensible Daten dürfen nur in Ausnahmefällen verarbeitet werden, etwa wenn eine ausdrückliche Einwilligung vorliegt oder ein überwiegendes öffentliches Interesse besteht.

Rechte der betroffenen Personen

Die DSGVO stärkt die Rechte von Personen, deren Daten verarbeitet werden. Unternehmen müssen sicherstellen, dass betroffene Personen ihre Rechte wahrnehmen können, darunter:

- **Auskunftsrecht:** Nutzer können erfragen, welche Daten über sie gespeichert sind.
- **Recht auf Berichtigung:** Falsche oder unvollständige Daten müssen korrigiert werden.
- **Recht auf Löschung:** Betroffene können verlangen, dass ihre Daten gelöscht werden („Recht auf Vergessenwerden“).
- **Recht auf Datenübertragbarkeit:** Nutzer können verlangen, dass ihre Daten in einem gängigen Format an sie oder einen anderen Anbieter übermittelt werden.

- **Recht auf Widerspruch:** Personen können der Verarbeitung ihrer Daten widersprechen, insbesondere bei Direktwerbung.

Unternehmen sind verpflichtet, diese Anfragen innerhalb eines Monats zu beantworten.

Transparenzpflichten für Unternehmen

Unternehmen müssen betroffene Personen umfassend über die Verarbeitung ihrer Daten informieren. Dazu gehört insbesondere:

✓ Der Name und die Kontaktdaten des Unternehmens
✓ Der Zweck der Datenverarbeitung
✓ Die rechtliche Grundlage der Verarbeitung
✓ Die Speicherdauer der Daten
✓ Die Rechte der betroffenen Person

Diese Informationen müssen in verständlicher und leicht zugänglicher Form bereitgestellt werden, beispielsweise in einer Datenschutzerklärung auf der Webseite.

Datenschutz & Webseiten – Was müssen Betreiber beachten?

Wer eine Webseite betreibt, muss sicherstellen, dass die Daten der Nutzer sicher verarbeitet werden. Dazu gehören:
✔ Eine klare und vollständige **Datenschutzerklärung**
✔ Eine **Cookie-Einwilligung** für nicht notwendige Tracking-Technologien
✔ Verschlüsselte Datenübertragung durch **SSL-Zertifikate**
✔ Einfache Opt-out-Möglichkeiten für Tracking und Werbung
Das TTDSG verschärft die Regeln für Cookies und Online-Werbung und erfordert, dass Nutzer aktiv zustimmen, bevor Tracking-Tools eingesetzt werden dürfen.

Verzeichnis von Verarbeitungstätigkeiten

Alle Unternehmen müssen ein **Verarbeitungsverzeichnis** führen, in dem sie dokumentieren:

✔ Welche personenbezogenen Daten verarbeitet werden

✓ Zu welchem Zweck die Daten verwendet werden
✓ Wer Zugang zu den Daten hat
✓ Wie lange die Daten gespeichert werden
✓ Welche Sicherheitsmaßnahmen angewendet werden
Das Verzeichnis dient als Nachweis gegenüber Datenschutzbehörden und muss auf Anfrage vorgelegt werden.

Auftragsverarbeitung – Zusammenarbeit mit Dienstleistern

Wenn Unternehmen externe Dienstleister beauftragen, die personenbezogene Daten verarbeiten (z. B. Cloud-Anbieter, Buchhaltungssoftware), müssen sie mit diesen einen **Auftragsverarbeitungsvertrag (AVV)** abschließen. Dieser Vertrag regelt unter anderem:
✓ Die Art der Datenverarbeitung
✓ Die Sicherheitsmaßnahmen des Dienstleisters
✓ Die Rechte und Pflichten der beteiligten Parteien
Ohne diesen Vertrag ist die Nutzung externer Dienstleister **nicht DSGVO-konform.**

Datenschutzverletzungen & Meldepflichten

Falls es zu einem Datenleck oder Hackerangriff kommt, müssen Unternehmen innerhalb von

72 Stunden die Datenschutzbehörde informieren und, falls nötig, auch die betroffenen Personen benachrichtigen.

Beispiele für meldepflichtige Vorfälle:
🚨 Hackerangriff auf Kundendaten
🚨 Versehentliches Versenden von sensiblen Daten an falsche Empfänger
🚨 Verlust eines unverschlüsselten Laptops mit personenbezogenen Daten
Unternehmen sollten einen Notfallplan für Datenschutzverletzungen haben, um schnell und effektiv reagieren zu können.

Datenschutzbeauftragter – Wann ist einer erforderlich?

Nicht jedes Unternehmen benötigt einen Datenschutzbeauftragten (DSB), aber in bestimmten Fällen schreibt die DSGVO die Ernennung vor.
Ein Datenschutzbeauftragter ist **verpflichtend**, wenn:

✔ **Mindestens 20 Mitarbeiter regelmäßig mit personenbezogenen Daten arbeiten**
✔ **Besonders sensible Daten** (z. B. Gesundheitsdaten) in großem Umfang verarbeitet werden
✔ **Eine umfangreiche Überwachung** von Personen erfolgt (z. B. durch Videoüberwachung oder Tracking-Technologien)

Ein Datenschutzbeauftragter kann entweder **intern** ernannt oder **extern** beauftragt werden. Seine Aufgaben umfassen:

- Überwachung der Einhaltung der Datenschutzvorschriften
- Beratung der Geschäftsleitung zu Datenschutzfragen
- Schulung der Mitarbeiter im Datenschutz
- Kommunikation mit den Datenschutzbehörden

Fehlt ein Datenschutzbeauftragter, obwohl eine Pflicht besteht, drohen empfindliche Bußgelder.

Internationale Datenübertragungen & Drittstaatenregelungen

Die DSGVO schützt personenbezogene Daten nicht nur innerhalb der EU, sondern stellt auch strenge Anforderungen an die Übermittlung von Daten in **Drittländer** (Länder außerhalb der EU und des EWR). Eine Datenübermittlung ist nur zulässig, wenn:

✓ Das Zielland über ein angemessenes Datenschutzniveau verfügt (laut EU-Kommission, z. B. Schweiz, UK, Neuseeland)
✓ Standardvertragsklauseln (SCC) mit dem Empfänger abgeschlossen wurden
✓ Zusätzliche Sicherheitsmaßnahmen ergriffen werden, falls ein Land kein angemessenes Datenschutzniveau hat (z. B. USA)

Unternehmen, die internationale Cloud-Dienste oder Dienstleister außerhalb der EU nutzen, müssen sicherstellen, dass die DSGVO-Vorgaben eingehalten werden.

Datenschutz in der Personalabteilung – Umgang mit Mitarbeiterdaten

Mitarbeiterdaten unterliegen ebenfalls dem Datenschutz und dürfen nur unter bestimmten Bedingungen verarbeitet werden.

✓ Erlaubt sind die Erhebung und Verarbeitung von Daten, wenn sie zur **Vertragserfüllung** erforderlich sind (z. B. Gehaltsabrechnung, Urlaubsanträge).
✓ Gesundheitsdaten, Religionszugehörigkeit oder politische Überzeugungen dürfen nur mit Einwilligung oder in Ausnahmefällen verarbeitet werden.
✓ Bewerberdaten müssen nach einer **Absage innerhalb von 6 Monaten** gelöscht werden, sofern keine Einwilligung zur längeren Speicherung vorliegt.
✓ Unternehmen müssen **klare Richtlinien** für den Zugriff auf Mitarbeiterdaten festlegen.

Marketing & Datenschutz – Regeln für Werbung und E-Mail-Marketing

Direktwerbung ist nur erlaubt, wenn die DSGVO eingehalten wird. Besonders wichtig ist die **Einwilligungspflicht bei Newslettern und Werbe-E-Mails.**

✓ E-Mail-Werbung ist nur **mit einer klaren, freiwilligen und dokumentierten Einwilligung** erlaubt.

✓ Bei Bestandskunden kann Werbung **ohne Einwilligung** erlaubt sein, wenn sie für ähnliche Produkte erfolgt und ein Widerspruch möglich ist.

✓ Postalische Werbung benötigt keine Einwilligung, muss aber ein Widerspruchsrecht enthalten.

✓ Telefonwerbung ist nur mit **vorheriger Einwilligung** erlaubt.

Das Double-Opt-in-Verfahren stellt sicher, dass Newsletter-Anmeldungen **rechtssicher dokumentiert** werden.

Kundendaten & CRM-Systeme – DSGVO-konforme Verwaltung

Unternehmen nutzen häufig **Customer-Relationship-Management-Systeme (CRM)**, um Kundendaten zu verwalten. Damit die Nutzung DSGVO-konform bleibt, müssen Unternehmen:

✓ **Nur notwendige Kundendaten erfassen** und keine überflüssigen Informationen speichern.

✔ Ein Verarbeitungsverzeichnis führen, um zu dokumentieren, welche Kundendaten wie verarbeitet werden.
✔ Sicherstellen, dass **Zugriffsrechte eingeschränkt** sind und nur autorisierte Personen Kundendaten einsehen können.
✔ Daten regelmäßig **aktualisieren und löschen**, wenn sie nicht mehr benötigt werden.
Ein gut gepflegtes CRM-System hilft nicht nur beim Datenschutz, sondern verbessert auch das Kundenmanagement.

IT-Sicherheit & Datenschutzmaßnahmen für Unternehmen

Die DSGVO verlangt von Unternehmen, geeignete technische und organisatorische Maßnahmen (TOMs) zu ergreifen, um personenbezogene Daten zu schützen.
🔐 **Starke Passwörter & Zwei-Faktor-Authentifizierung (2FA)**
🔐 **Verschlüsselte Kommunikation & Speicherung von Daten**
🔐 **Zugriffsrechte minimieren & aufgabenbezogen vergeben**
🔐 **Regelmäßige Backups & Updates von IT-Systemen**
🔐 **Schulung der Mitarbeiter im sicheren Umgang mit Daten**

Ein hohes Sicherheitsniveau hilft nicht nur beim Datenschutz, sondern schützt auch vor Cyberangriffen und Datendiebstahl.

Mobile Geräte & Datenschutz – Richtlinien für BYOD (Bring Your Own Device)

Viele Unternehmen erlauben es Mitarbeitern, private Geräte für die Arbeit zu nutzen. Dieses sogenannte BYOD (Bring Your Own Device) kann jedoch Datenschutzrisiken mit sich bringen.

✔ Unternehmen sollten klare **Richtlinien für die Nutzung privater Geräte** im Arbeitskontext festlegen.

✔ Es sollten Sicherheitsmaßnahmen wie Mobile Device Management (MDM) eingesetzt werden, um dienstliche Daten zu schützen.

✔ Sensible Unternehmensdaten sollten **nicht auf ungesicherten Geräten gespeichert** werden.

✔ Falls ein Mitarbeiter das Unternehmen verlässt, muss sichergestellt werden, dass **keine geschäftlichen Daten auf dem privaten Gerät verbleiben.**

Cloud-Dienste & Datenschutz – Nutzung externer Server sicher gestalten

Immer mehr Unternehmen speichern Daten in der Cloud. Dabei müssen sie sicherstellen, dass die genutzten Dienste DSGVO-konform sind.

✓ Vertrag zur Auftragsverarbeitung (AVV) mit Cloud-Anbietern abschließen.
✓ Sicherstellen, dass der Cloud-Anbieter **Server innerhalb der EU** nutzt oder geeignete Schutzmaßnahmen ergriffen werden.
✓ Daten sollten **verschlüsselt gespeichert** und übertragen werden.
✓ Unternehmen müssen dokumentieren, welche **Daten in der Cloud gespeichert werden** und wer darauf zugreifen kann.
Nicht jeder Cloud-Anbieter erfüllt die DSGVO-Anforderungen – daher ist eine **sorgfältige Auswahl** erforderlich.

Social Media & Datenschutz – Risiken & Best Practices

Unternehmen nutzen Social Media für Marketing und Kundenkommunikation, müssen aber auch hier die DSGVO beachten.
✓ K**eine personenbezogenen Daten ohne Zustimmung veröffentlichen** (z. B. Kundennamen, Mitarbeiterfotos).
✓ Falls Social Media Plattformen Daten verarbeiten (z. B. Facebook-Pixel), ist eine **Einwilligung erforderlich**.
✓ Unternehmen sollten eine **Social-Media-Richtlinie** haben, um die Nutzung durch Mitarbeiter zu regeln.
✓ Datenschutzfreundliche Alternativen wie **dezentrale Plattformen** in Betracht ziehen.

Fazit: Datenschutz als Chance nutzen

Datenschutz ist mehr als nur eine gesetzliche Pflicht – er kann auch ein **Wettbewerbsvorteil** sein. Unternehmen, die Datenschutz transparent und verantwortungsvoll umsetzen, stärken das Vertrauen von Kunden und Geschäftspartnern.
Eine frühzeitige und strategische Einhaltung der Datenschutzvorschriften hilft, **Bußgelder zu vermeiden**, Risiken zu minimieren und Geschäftsprozesse sicherer zu gestalten. Wer Datenschutz ernst nimmt, schützt nicht nur sensible Informationen, sondern auch das eigene Unternehmen vor Cyberangriffen und Reputationsschäden.

Wir wünschen dir viel Erfolg bei deiner Gründung

Disclaimer
Unsere Muster und Dokumente dienen ausschließlich als unverbindliche Information und stellen keine Rechtsberatung dar. Für die Vollständigkeit, Richtigkeit und Aktualität übernehmen wir keine Gewähr. Im Zweifelsfall empfehlen wir, eine juristische Fachberatung in Anspruch zu nehmen.
Trotz sorgfältiger Erstellung kann aufgrund der Komplexität und ständigen Weiterentwicklung des Rechts jegliche Haftung ausgeschlossen werden, soweit dies gesetzlich zulässig ist.
Zur besseren Lesbarkeit wird das generische Maskulinum verwendet. Alle Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.
Stand: 2022

Datenschutzanforderung
Checkliste

Allgemeine Anforderungen & Transparenz

- [ ] Datenschutzerklärung erstellen und bereitstellen
- [ ] Rechtsgrundlage für jede Datenverarbeitung prüfen
- [ ] Verzeichnis der Verarbeitungstätigkeiten führen

Datenschutz auf Webseiten & Online-Diensten

- [ ] Cookie-Banner mit Opt-in einrichten
- [ ] Google Analytics & Tracking nur mit Einwilligung nutzen
- [ ] SSL-Verschlüsselung für Webseiten aktivieren

Verarbeitung & Speicherung von Daten

- [ ] Nur notwendige Daten erfassen (Datenminimierung)
- [ ] Speicherfristen definieren und Daten regelmäßig löschen
- [ ] Zugriffsrechte für Mitarbeiter einschränken

Auftragsverarbeitung & externe Dienstleister

- [ ] Liste aller externen Dienstleister erstellen
- [ ] Auftragsverarbeitungsverträge (AVV) abschließen
- [ ] Internationale Datenübertragungen absichern

Datenschutz in der Personalabteilung

- [ ] Bewerberdaten nach 6 Monaten löschen
- [ ] Datenschutzschulungen für Mitarbeiter durchführen
- [ ] Arbeitsverträge mit Datenschutzklausel ergänzen

Sicherheitsmaßnahmen & IT-Schutz

- [ ] Starke Passwörter & Zwei-Faktor-Authentifizierung nutzen
- [ ] Software-Updates & Sicherheits-Patches regelmäßig einspielen
- [ ] Notfallplan für Datenschutzverletzungen erstellen