

# Datenschutz-Check

TÜV Informationstechnik GmbH

Langemarckstr. 20

45141 Essen

☎ (0201) 8999-643

www.tuvit.de



**HINWEIS:** Diese Checkliste gibt Ihnen einen ersten Überblick, ob der Datenschutz in Ihrem Unternehmen den gesetzlichen Bestimmungen entspricht und wo ggf. noch Handlungsbedarf besteht. Aufgrund der Komplexität des Themas und der vielfältigen speziellen Anforderungen an Unternehmen einzelner Branchen und möglicherweise bestehenden Sondervorschriften, wie z.B. Tarifverträge oder betriebliche Vereinbarungen, erhebt dieser Kurz-Check keinen Anspruch auf Vollständigkeit.

Bitte beachten Sie, das sich mögliche Risiken bei der Nichtbestellung eines Datenschutzbeauftragten nicht nur auf die Sanktionsmöglichkeiten des Bundesdatenschutzgesetz (BDSG) beziehen. Vielmehr sollten Sie die weitergehenden Risiken z. B. aus dem Zivilrecht (bei Verletzung von Vertragspflichten), dem Strafrecht (bei Verletzung des Fernmeldegeheimnisses oder Verletzung beruflicher Schweigepflicht) oder dem Arbeitsrecht (bei Beweisverwertungsverbote auf Grund unzulässiger Datenerhebung) bei Ihren Überlegungen zum Datenschutz und zur Datensicherheit einbeziehen.

## 1. Informationsbeschaffung

**Werden die für Ihre Geschäftstätigkeit benötigten Daten rechtmäßig beschafft?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich
Grün	Gelb	Rot	Rot

Zu beachten:

- Wo werden Daten erhoben (z. B. bei Mitarbeitern, Kunden, Lieferanten)?
- Wie werden Daten erhoben (z. B. mit Fragebogen, im Internet, durch Interview, bei Dritten)?
- Werden Datenschutzformalien eingehalten (z. B. Datenschutz-Hinweise auf Fragebögen, im Internet)?
- Sind die Zwecke der Erhebung hinreichend bestimmt und transparent (z. B. Vertragserfüllung, Werbung)?

## 2. Informationsverarbeitung

**Werden die für Ihre Geschäftstätigkeit benötigten Daten rechtmäßig verarbeitet und genutzt?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich
Grün	Gelb	Rot	Rot

Zu beachten:

- Welche Daten werden verarbeitet und genutzt (z. B. über Mitarbeiter, Kunden, Lieferanten, Interessenten, Teilnehmer an Preisausschreiben, Internet-Kontakte)?
- Wer verarbeitet und nutzt die Daten (z. B. Personalabteilung, Marketing, Vertrieb, Internet- Betreuung, externe Dienstleister / Outsourcing)?
- Erfolgt die Verarbeitung und Nutzung der Daten ausschließlich im Rahmen der bei der Erhebung festgelegten und legalisierten Zweckbestimmung (z. B. zur Erfüllung des Arbeitsvertrages, einer Bestellung, gesetzlicher Bestimmungen)?
- Werden Datenschutzformalien eingehalten (z. B. Hinweise auf Werbewiderspruch bei Anschreiben)?

## 3. Informationsweitergabe

**Werden die für Ihre Geschäftstätigkeit benötigten Daten rechtmäßig weitergegeben?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich
Grün	Gelb	Rot	Rot

Auch die Weitergabe personenbezogener Daten sowohl innerhalb des Unternehmens, als auch im Konzern oder an andere Stellen bedarf der besonderen Legitimierung.

Zu beachten:

- Welche Daten werden weitergegeben (z. B. über Mitarbeiter, Kunden, Lieferanten, Interessenten, Teilnehmer an Preisausschreiben, Internet-Kontakte)?
- An wen werden Daten weitergegeben (z. B. andere Fachabteilungen, verbundene Unternehmen, externe Dienstleister, Banken, Versicherungen, Empfänger in Nicht-EU-Ländern)?
- Erfolgt die Übermittlung der Daten ausschließlich im Rahmen der bei der Erhebung festgelegten Zweckbestimmung (z. B. zur Erfüllung des Arbeitsvertrages, einer Bestellung, gesetzlicher Bestimmungen)?
- Werden Datenschutzformalien eingehalten (z. B. Hinweise auf die Zweckbindung beim Empfänger)?

#### 4. Informationsverarbeitung in besonderen Verfahren

**Sind die Voraussetzungen für besondere Arten des Datenumgangs in Ihrem Unternehmen erfüllt?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Folgende Verfahren müssen besonders legitimiert werden:

- Datenübermittlungen in Nicht-EU-Länder, z. B. an verbundene Unternehmen, Konzernrechenzentren im Ausland
- Der Umgang mit besonders sensiblen Daten, z. B. beim betriebsärztlichen Dienst, Forschungsdaten
- Videoüberwachung, z. B. zur Überwachung öffentlich zugänglicher Geschäftsräume, zum Gebäudeschutz
- Der Umgang mit privaten Telefongesprächen der Mitarbeiter über die betriebliche Telefonanlage
- Angebote und Kontakt-Möglichkeiten über das Internet
- Gemeinsame Kunden- und Lieferantendatenbanken mit verbundenen Unternehmen
- Die Verwendung von Chipkarten z. B. zur Zeiterfassung
- Die automatisierte Bewertung von Personen z. B. im Bewerbungsverfahren und in CRM-Systemen

#### 5. Nutzung und Angebot von Dienstleistungen

**Sind Dienstleistungen für und durch Ihr Unternehmen datenschutzgerecht gestaltet?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Die Nutzung und das Angebot von Dienstleistungen müssen besonders gestaltet werden:

- Outsourcing z. B. durch gemeinsame RZ-Nutzung, zentrale Personalstellen, Auslagerung der EDV, Call-Center.
- Datenträgervernichtung durch Spezial-Firmen (z. B. Akten, Mikrofilm, Magnetbänder)
- Die Betreuung durch externe Unternehmen z. B. zur Hard- und Software-Wartung, Help-Desk, Fernwartung.
- Der Einsatz von Mitarbeitern von Fremdfirmen in Ihrem Unternehmen, z. B. externe Berater, Programmierer, Reinigungskräfte, Wachdienste.

#### 6. Datenschutzbeauftragter

**Hat Ihr Unternehmen einen externen oder internen Datenschutzbeauftragten (schriftlich) bestellt?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Zu beachten:

- Der Datenschutzbeauftragte muss Fachkunde und Zuverlässigkeit nachweisen.
- Ihm muss es möglich sein, den Datenschutz im Unternehmen umzusetzen. Er berät vor allem in den Bereichen Datenbeschaffung, Datenverarbeitung, Datenweitergabe und Dienstleistungsnutzung.
- Erfüllt der Datenschutzbeauftragte diese Anforderungen nicht oder entspricht seine Bestellung nicht den formalen Erfordernissen, so gilt er als nicht bestellt. Dies kann die Verhängung eines Bußgeldes zur Folge haben!
- Ist laut Bundesdatenschutzgesetz die Bestellung eines Datenschutzbeauftragten nicht erforderlich, so muss die Geschäftsleitung den Datenschutz sicherstellen.
- Auch wenn ausnahmsweise keine Rechtspflicht zur Bestellung eines Datenschutzbeauftragten besteht, kann praktizierter Datenschutz ein Wettbewerbsvorteil für Ihr Unternehmen sein.

#### 7. Mitarbeiter

**Werden Ihre Mitarbeiter auf das Datengeheimnis verpflichtet und hinreichend über ihre Datenschutzpflichten aufgeklärt?**

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Zu beachten:

- Sind die Mitarbeiter über die Datenschutzorganisation aufgeklärt?
- Sind die Mitarbeiter über ihre Datenschutz- und Datensicherheit Pflichten informiert?
- Erhalten die Mitarbeiter bei der Einstellung Informationsmaterial zu Datenschutz und Datensicherheit?
- Werden die Mitarbeiter beim Umgang mit besonders sensiblen Daten auf ihre speziellen Pflichten hingewiesen (z. B. betriebsärztlicher Dienst, Telefonadministration, Email und Internetadministration)?

## 8. Betroffene

Werden die die Rechte der Betroffenen berücksichtigt?

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Zu beachten:

Ist z. B. sichergestellt, dass

- die Betroffenen unterrichtet werden?
- Eventuelle Auskunftersuchen bearbeitet werden?
- Berichtigungen oder Löschungen von Daten technisch realisiert werden können?
- ein Verzeichnisse für Jedermann zur Einsicht bereitgehalten wird?

## 9. Datensicherheit

Sind Ihre Verfahren technisch-organisatorisch so abgesichert, dass sie den Anforderungen des Datenschutzes gerecht werden?

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Datenschutz und technisch-organisatorische Maßnahmen zur Datensicherung (8 Gebote des Datenschutzes) gehören zusammen.

Zu beachten:

- Gibt es ein IT-Sicherheitskonzept für Ihr Unternehmen?
- Sind Ihre Systeme passwortgeschützt?
- Können ihre Mitarbeiter nur auf die Daten zugreifen, die sie für ihre Aufgabenerfüllung benötigen (Berechtigungskonzepte)?
- Gibt es ein Backup-Konzept?
- Ist der Virenschutz organisiert?
- Sind Ihre Mitarbeiter mit notwendigen Datensicherheitsmaßnahmen vertraut gemacht worden?
- Erfolgt die Nutzung von Online-Diensten über eine Firewall?

## 10. Datenschutzorganisation

Ist der Datenschutz in Ihrem Unternehmen ausreichend organisiert?

JA	Klärung notwendig	NEIN	Klärung nicht möglich

Zu beachten:

- Sind die Verantwortlichkeiten für Datenschutz und Datensicherheit geregelt?
- Ist sichergestellt, dass der Datenschutzbeauftragte bei der Einführung neuer und der Änderung bestehender Verfahren informiert und einbezogen wird?
- Ist sichergestellt, dass die gesetzlich geforderten Verzeichnisse erstellt und bereitgehalten werden?
- Ist die Verpflichtung der Mitarbeiter auf das Datengeheimnis und deren Schulung organisiert?
- Wird die Einhaltung der Regelungen zu Datenschutz und Datensicherheit regelmäßig kontrolliert?

### Anleitung:

Die folgende Checkliste soll Ihnen helfen, Ihre unternehmensspezifischen Risiken zu identifizieren, um in einem nächsten Schritt Massnahmen zur Verbesserung einzuleiten.

<b>GRÜN</b>	Kreuzen Sie dieses Feld nur an, wenn Sie diesbezüglich keine Zweifel haben.
<b>GELB</b>	Falls Nachforschungen notwendig sind oder Klärungsbedarf besteht, kreuzen Sie das gelbe Feld an.
<b>ROT</b>	Falls die Frage in einem oder mehreren Punkten nicht erfüllt ist, kreuzen Sie das rote Feld an.

Ihr Unternehmen hat seine Datenschutzrisiken minimiert und ist hinreichend sicher organisiert, wenn bei allen Fragen das **grüne Feld** angekreuzt werden konnte.

Bei **gelben Feldern** sollten Sie Sachverhaltsaufklärung betreiben und klären, ob dann die Frage auf grün oder rot gesetzt werden kann.

Bei den **rot angekreuzten Feldern** ist Handlungsbedarf gegeben. Hier sollten Sie je nach potentielltem Risiko evtl. auch auf Experten zurückgreifen.

## Ein gutes Wort zum Schluss...

Wir hoffen, dass Ihnen der vorliegende Datenschutz-Check Sie bei Ihrer Bewertung unterstützen konnte und Ihnen eine Hilfestellung bietet, um vorab klären zu können, ob Ihr Unternehmen bereits Maßnahmen für ein nachhaltiges Datenschutzniveau unterhält.

In vielen Unternehmen wird Datenschutz und Datensicherheit schlichtweg vernachlässigt. Als Gründe hierfür werden vom Management häufig die gleichen Meinungen zum Datenschutz geäußert:

- Datenschutz hat keinen Nutzen, er verursacht ja doch nur Kosten!
- Datenschutz gehört nicht zu den primären Geschäftsinteressen unseres Unternehmens!
- Es ist doch noch nie etwas passiert, was einen Datenschutz rechtfertigt!

Ursachen dieser Argumentation sind häufig, dass die Themen Datenschutz und Datensicherheit von vielen Unternehmensleitungen nicht systematisch genug betrachtet und einer eingehenden Risikoanalyse unterzogen wurde. Es ist ja auch viel leichter, dieses lästige und durchaus schwierige Thema mit Pauschalargumenten abzutun, als selbst die Initiative zu ergreifen.

Betrachtet man die üblichen Argumente etwas genauer, so ergibt sich hier durchaus eine andere Fokussierung.

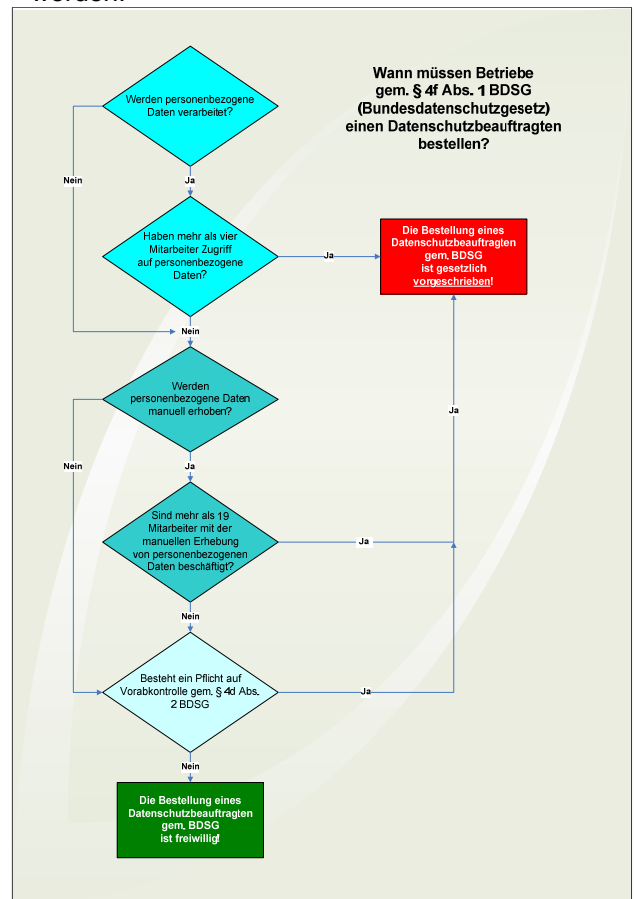
- Image- und Vertrauensverlust bei den Kunden und in der Öffentlichkeit.
- Mögliche Gerichtsverfahren und damit verbundene Kosten.
- Letztendlich eine allgemeine Unzufriedenheit bei Ihren Kunden.

Die wirklichen Gründe, warum Themen wie Datenschutz und Datensicherheit nicht pragmatisch angegangen werden, liegen häufig in der Unsicherheit nachfolgender Lösungsansätze:

- Worum müssen wir uns kümmern, um ein nachhaltiges Datenschutzniveau in unserem Unternehmen erzielen zu können?
- Wo liegen die Risiken?
- Welche Unterstützung und Hilfen stehen uns dabei zur Verfügung?
- Wie kann ein schneller Überblick geschaffen werden, ob und an welchen Stellen im Unternehmen technische und/oder organisatorische Maßnahmen eingeführt werden müssen?
- Können wir dabei auf externe Fachspezialisten bauen, die uns kostenneutral unterstützen?

Die TÜV Informationstechnik GmbH, als Mitglied der anerkannten Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) hat sich zum erklärten Ziel gesetzt, Institutionen, mittelständische Unternehmen und Gesellschaften davor zu schützen, dass ihre Mitarbeiter durch den Umgang mit personenbezogene Daten gegen bestehendes Recht und damit gegen das Bundesdatenschutzgesetz (BDSG) verstoßen.

Wir analysieren und bewerten datenschutzrelevante Prozesse und erarbeiten Empfehlungen zur Behebung möglicher Schwachstellen. Gerne erstellen wir für Sie ein individuelles Datenschutzkonzept mit den für Ihr Unternehmen relevanten Datenschutzbestimmungen und die zur Erfüllung umzusetzenden notwendigen Verfahren. Sprechen Sie mit uns, denn Datenschutz und Datensicherheit ist nicht nur Vertrauenssache, sie muss auch zur Chefsache werden!



Sie möchten sofort mit einem unserer Experten zum Thema Datenschutz Kontakt aufnehmen?

Wählen Sie (0201) 8999-643

und unsere kompetenten Berater stehen Ihnen mit Rat und Tat gerne zur Seite!

**Rufen Sie uns einfach an!**