

# Wann müssen Unternehmen einen Datenschutzbeauftragten benennen

---

*An der Pflicht einen Datenschutzbeauftragten zu benennen hat sich mit der Einführung der DSGVO und des neuen BDSG in Deutschland nichts geändert. Nach wie vor gilt die Pflicht, wenn sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Dennoch wurden seitdem in zahlreichen mittelständischen Unternehmen Datenschutzbeauftragte benannt. Dies ist in manchen Fällen jedoch bei genauer Interpretation des Gesetzes nicht unbedingt erforderlich,*

---

*auch wenn es durchaus sinnvoll sein kann.*

## Kriterien zur Benennung

### Anzahl Mitarbeiter

Gemäß §38 BDSG benennen Unternehmen „eine/n Datenschutzbeauftragte/n, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“. Wann aber sind 10 Personen ständig damit beschäftigt? Sind dazu Vollzeit-Equivalente zu berechnen oder gilt die Schwelle erreicht, wenn zu einem beliebigen Zeitpunkt zu Geschäftszeiten 10 Personen mit der Verarbeitung beschäftigt sind? Eigene Kommunikation mit dem Landesamt für Datenschutzaufsicht sowie eine Mitteilung der Kassenärztlichen Vereinigung Bayern haben die derzeitige Rechtsauffassung des Landesamtes klargestellt: **Die Schwelle gilt als erreicht, wenn zumindest zehn Mitarbeiter mehr als die Hälfte ihrer Arbeitszeit mit der automatisierten Verarbeitung verbringen.**

Was bedeutet dies für mittelständische Unternehmen? Auch wenn Sie mehr als 10 Mitarbeiter haben, die gelegentlich personenbezogene Daten verarbeiten, begibt sich nicht unbedingt eine Bestellpflicht. In der Regel ist z.B. eine Arzthelferin, die vorwiegend dem Arzt assistiert, oder der KFZ-Mechaniker, der vorwiegend an Autos arbeitet, nicht für die Schwelle von 10 Personen mitzuzählen. Allerdings sind auch Teilzeitkräfte voll einzubeziehen, wenn diese die Hälfte Ihrer Arbeitszeit mit der Verarbeitung personenbezogener Daten verbringen. So ist z.B. eine 20-Stunden-Kraft zu berücksichtigen, wenn sie pro Woche zumindest 10 Stunden mit der Verarbeitung personenbezogener Daten verbringt. In der Regel werden daher Mitarbeiter der Personalabteilung, Mitarbeiter am Empfang, Vertriebsmitarbeiter oder Mitarbeiter in der IT-Administration zu berücksichtigen sein.

### Art der Verarbeitung

Neben der Anzahl der Mitarbeiter ergeben sich aus dem § 38 BDSG sowie Art. 37 DSGVO noch verschiedene andere Kriterien aus denen sich eine Pflicht zur Benennung eines Datenschutzbeauftragten ergeben kann. Diese orientieren sich im Wesentlichen an der Art der Verarbeitung bzw. dem sich aus der Verarbeitung ergebenden Risiko für Betroffene. So ist ein Datenschutzbeauftragter zu benennen wenn eines der folgenden Kriterien zutrifft:

## Wann müssen Unternehmen einen Datenschutzbeauftragten benennen

1. Eine Verarbeitung erfordert eine Datenschutz-Folgenabschätzung nach Art 35. DSGVO. Dies ist im Besonderen der Fall, wenn die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge (Art. 35 Abs. 1 DSGVO) hat.
2. Die Verarbeitung personenbezogener Daten erfolgt geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung.
3. Die Kerntätigkeit des Unternehmens macht eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich.
4. Die Kerntätigkeit besteht aus der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO oder Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.
5. Die Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln.

Für die meisten mittelständischen Unternehmen wird sich daraus keine Pflicht zur Bestellung ergeben. Auch Arztpraxen oder Pflegedienste müssen, wie aus Stellungnahmen des LDA Bayern hervorgeht, aus diesen Gründen in der Regel keinen Datenschutzbeauftragten benennen. Gehören aber z.B. Aufgaben im Bereich der Sozialversicherung, Resozialisierung sowie der Markt- oder Meinungsforschung zum (Kern-) Aufgabenbereich sollten diese Kriterien sorgfältig geprüft werden. Auch bei dem Einsatz neuer Technologien, wie z.B. Telemedizin, kann sich aus der Art der Verarbeitung die Pflicht zur Benennung eines Datenschutzbeauftragten ergeben.

## Handlungsempfehlung

Um zu bestimmen, ob Ihr Unternehmen die Mitarbeiter-Schwelle überschreitet, sollten Sie prüfen, wie viel Zeit Ihre Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten verbringen. Z.B. indem Ihre Mitarbeiter für ein paar Tage diese Zeiten notieren. Die Details und das Ergebnis der Prüfung sollten Sie für eventuelle Nachfragen sorgfältig dokumentieren und aufbewahren. Damit können Sie Ihre Pflicht nachkommen gemäß Art. 5 Abs. 2 nachzuweisen, dass weniger als zehn Personen vorwiegend mit der automatisierten Verarbeitung von Personen beschäftigt sind.

Soweit Ihr Unternehmen nicht die Schwelle von 10 Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, erreicht, müssen Sie noch prüfen, ob die Kriterien zur Art der Verarbeitung auf Sie zutreffen. Diese Prüfung sollte im Rahmen der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten erfolgen. Dabei müssen Sie ohnehin alle Verarbeitungen betrachten. Darüber hinaus wird das LDA Bayern zu gegebener Zeit eine Liste von Verarbeitungen veröffentlichen, für die eine Datenschutz-Folgenabschätzung erforderlich ist. Diese wird sich voraussichtlich an der Liste der Datenschutzkonferenz orientieren, wie sie z.B. unter [https://www.lda.bayern.de/media/dsfa\\_muss\\_liste\\_dsk\\_de.pdf](https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf) zu finden ist. Beinhaltet Ihre Geschäftstätigkeit Verarbeitungen aus dieser Liste, so müssen Sie einen Datenschutzbeauftragten benennen.

Auch wenn Sie keinen Datenschutzbeauftragten benennen müssen, entbindet Sie dies nicht von der Pflicht alle sonstigen Pflichten aus DSGVO und BDSG zu erfüllen. Im Besonderen gehört dazu:

- Erstellen eines Verzeichnisses der Verarbeitungstätigkeiten.
- Erstellen einer Datenschutzerklärung für Ihre Webseiten.
- Verpflichtung der Mitarbeiter auf den Datenschutz.

## Wann müssen Unternehmen einen Datenschutzbeauftragten benennen

- Information von Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten gemäß Art. 13 und 14.
- Prüfen ob Einwilligungserklärungen den hohen Anforderungen des Art. 7 DSGVO hinsichtlich Freiwilligkeit, Verständlichkeit, Widerrufbarkeit etc. erfüllt.
- Erstellen eines Verfahrens zur Meldung von Datenpannen binnen 72 Stunden.
- Verfahren zur Erfüllung von Betroffenenrechten auf Auskunft, Löschung etc.
- Schließen von Vereinbarungen zur Verarbeitung im Auftrag wo erforderlich

## Unterstützung durch die Süd IT

Müssen Sie einen Datenschutzbeauftragten bestellen, so unterstützen wir Sie gerne mit einem externen Datenschutzbeauftragten aus unseren Reihen. Aber auch wenn Sie diesen nicht benennen müssen oder bereits einen internen DSB benannt haben, unterstützen wir Sie gerne mit Rat und Tat bei der Umsetzung der Anforderungen von DSGVO und BDSG. Dabei können Sie auf unseren reichen Schatz an Vorlagendokumenten und Verfahren zurückgreifen, die wir in zahlreichen Projekten, vor Allem im Bereich des Mittelstandes, gesammelt haben.

## Kontakt

Dr. Stefan Krempl  
089 461 3505 12  
krempf@sued-it.de

ISO/IEC 27001 Lead-Auditor im Auftrag des TÜV Rheinland  
u. Deutsche Auditoren eG,  
Auditor IT-Sicherheitskatalog nach §11 Abs. 1a EnWG,  
Auditor gemäß §8a BSIG für kritische Infrastrukturen,  
VdS-zertifizierter Berater für Cyber-Security,  
Datenschutzbeauftragter IHK



Alico Sternbeck  
089 4613505 22  
sternbeck@sued-it.de

Auditor ISO/IEC 27001  
Datenschutzbeauftragter  
Ansprechpartner Cisco-Pix,  
Cisco Meraki, Watchguard, ISA

