Update 2025

1. Dokumentation | 2. Informationspflicht | 3. Betroffenenrechte | 4. Website

Checkliste für Datenschutz-Geplagte:

# Die 4 wichtigsten DSGVO-Pflichten … und welche du davon nicht erfüllst.

**Wissen, welche DSGVO-Pflichten wirklich zählen.**
**Lücken erkennen. Risiko einschätzen. Strafen vermeiden.**

# Herzlich willkommen!

**Schön, dass du dir diese Checkliste für Datenschutz-Geplagte heruntergeladen hast.**

**Ich habe diese für dich erstellt, damit sie dir eine prägnante Übersicht zur Selbstüberprüfung sein kann.**

**Überprüfe selbst, ob bei euch in Sachen DSGVO alles im grünen Bereich ist.**

## Wie das Abmahnrisiko möglichst klein halten?

Die nachfolgenden 4 Bereiche sind entscheidend für Unternehmen, wenn es darum geht das Risiko in Sachen DSGVO zu minimieren. Du solltest sie am Schirm haben, um auf der sicheren Seite zu sein.

Wo solltest du ansetzen? Finde es über meine Checkliste mit einer Übersicht der zentralen DSGVO-Pflichten heraus.

Los geht‘s!

Ich wünsche dir viel Freude und Erfolg beim Anwenden!

*Dein Daniel Lukmann*

## Daniel Lukmann

Gründer des DSGVO Schutzteam | Zertifizierter Datenschutzbeauftragter

Über 3.500 Unternehmen haben mit ihm ihre Datenschutz-Sorgen bereits hinter sich gelassen. Diese Checkliste soll helfen unbewusste DSGVO-Risiken aufzudecken.

# 1. Dokumentationspflicht

Ein zentraler Teil der DSGVO ist die Dokumentationspflicht. Es ist, wie ein Tagebuch. Du notierst, welche Daten ihr sammelt, was ihr damit tut/ wie ihr sie schützt.

Klopft die Behörde an, hat man 2 Wochen um alles zu liefern – und wir sprechen hier schnell von mehreren 100 Seiten.

## Ihre Checkliste zur Dokumentationspflicht:

Ja ☐ Nein ☐

**Gibt es ein aktuelles Verzeichnis der Verarbeitungstätigkeiten (nicht älter als 3 Monate)?**

*Was ist ein „Verzeichnis der Verarbeitungstätigkeiten (VVT)“?*

Es handelt sich hier quasi um die **Datenschutz-Landkarte** eines Unternehmens. Hier wird aufgelistet, welche personenbezogenen Daten verarbeitet werden, wofür, wie lange und wer Zugriff hat.
Es ist Pflicht nach Artikel 30 DSGVO – und hilft dabei, Datenschutz transparent zu dokumentieren.

*Was steht drin?*

Jede Verarbeitungstätigkeit (z. B. Bewerbermanagement, Kundenverwaltung, Rechnungsstellung) muss mit diesen Infos dokumentiert werden:

| | |
|---|---|
| **Name der Verarbeitung** | ➔ z.B. Bewerberverwaltung |
| **Zweck der Verarbeitung** | ➔ Warum werden die Daten verarbeitet? |
| **Betroffene Personen** | ➔ Wer ist betroffen? (z.B. Kunden) |
| **Kategorien personenbezogener Daten** | ➔ Welche Daten? (z.B. Name, Adresse) |
| **Rechtsgrundlage** | ➔ Auf welcher Grundlage? (z.B. Einwilligung, Vertrag) |
| **Empfänger der Daten** | ➔ Wer bekommt die Daten? (z.B. Steuerberater, Cloud-Dienstleister) |
| **Speicherdauer** | ➔ Wie lange werden Daten aufbewahrt? |

Ja ☐ Nein ☐

**Sind eure TOMs (Technische und organisatorische Maßnahmen) dokumentiert?**

*Was sind TOMs?*

Hier handelt es sich um Maßnahmen, die euer Unternehmen trifft, um personenbezogene Daten sicher zu verarbeiten. Die DSGVO fordert, dass ihr genau nachweisen könnt, wie ihr Daten schützt.

TOMs bestehen aus technischen und organisatorischen Maßnahmen:

1. **Technische Maßnahmen** (Schutz durch Technik)
   Diese betreffen die IT-Sicherheit und Infrastruktur. Beispiele:

| | |
|---|---|
| **Verschlüsselung** | ➔ bei z.B. E-Mails und Datenbanken |
| **Passwortschutz** | ➔ starke Passwörter und 2FA-Schutz |
| **Firewall & Antivirus** | ➔ Schutz vor Cyberangriffen |
| **Zugriffsrechte** | ➔ Nur autorisierte dürfen Daten sehen. |

2. **Organisatorische Maßnahmen** (Schutz durch Regeln & Prozesse)
   Diese betreffen die IT-Sicherheit und Infrastruktur. Beispiele:

| | |
|---|---|
| **Schulungen** | ➔ Mitarbeiter regelmäßig zur DSGVO schulen. |
| **Vertraulichkeit** | ➔ Verträge mit Mitarbeitern & Dienstleistern |
| **Löschkonzept** | ➔ Daten werden nach Ablauf der Frist gelöscht |
| **Meldeprozesse** | ➔ Klare Abläufe für Datenschutzverletzungen |

Ja ☐ Nein ☐

**Wurden für riskante Datenverarbeitungen Datenschutz-Folgeabschätzungen (DSFA) durchgeführt und dokumentiert?**

*Kriterien für eine risikoreiche Verarbeitung:*

| | |
|---|---|
| **Verarbeitung großer Datenmengen** | ➔ z.B. > 1.000 Kundendaten |
| **Besonders schützenswerte Daten** | ➔ Gesundheitsdaten, biometrische oder finanzielle Daten |
| **Automatisierte Entscheidungsfindung/ Profiling** | ➔ Algorithmen entscheiden über Kredite oder Versicherungen |
| **Überwachung von Personen** | ➔ Videoüberwachung/Tracking auf der Website |
| **Datenweitergabe an Drittländer** | ➔ Verarbeitung außerhalb der EU ohne ausreichende Schutzmaßnahmen |

*Was beinhaltet eine DSFA?*

| | |
|---|---|
| **Beschreibung der Verarbeitung** | ➔ Welche Daten werden verarbeitet und warum? |
| **Bewertung der Notwendigkeit** | ➔ Ist die Verarbeitung wirklich erforderlich? |
| **Risikoanalyse** | ➔ Welche Datenschutzrisiken gibt es? |
| **Schutzmaßnahmen** | ➔ Welche Maßnahmen minimieren die Risiken? |

💡 Hast du keine “risikoreiche Verarbeitung“, antworte hier mit „Ja“.

Ja ☐ Nein ☐

**Wurden Verträge mit allen Auftragsverarbeitern geschlossen?**

*Typische Beispiele für Auftragsverarbeiter:*

**IT & Cloud-Dienste**

➔ Cloud-Speicher-Anbieter (z.B. Google Drive, Microsoft OneDrive, Dropbox, iCloud)
➔ E-Mail-Dienstleister (z.B. Microsoft Outlook, Google Workspace)
➔ Hosting-Anbieter (z.B. AWS, IONOS, Hetzner)
➔ Backup-Dienstleister (z.B. Acronis, Veeam)

**Software & Online-Tools**

➔ CRM-Systeme (z.B. Salesforce, HubSpot, Pipedrive)
➔ Newsletter-Tools (z.B. z.B. Mailchimp, Brevo. CleverReach)
➔ Projektmanagement-Tools (z.B. Trello, Asana, Monday.com)
➔ Buchhaltungssoftware (z.B. DATEV, Lexware, sevDesk)

**Externe Dienstleister**

➔ Lohnbuchhaltung (z.B. Steuerberater, ext. Lohnbuchhaltungsfirmen)
➔ Callcenter/ Kundenservice-Dienstleister (z.B. ext. Hotline-Dienste)
➔ Externe IT-Support-Dienstleister (z.B. Wartung von IT-Systemen)
➔ Druck- & Versanddienstleister (z.B. personalisierte Mailings)

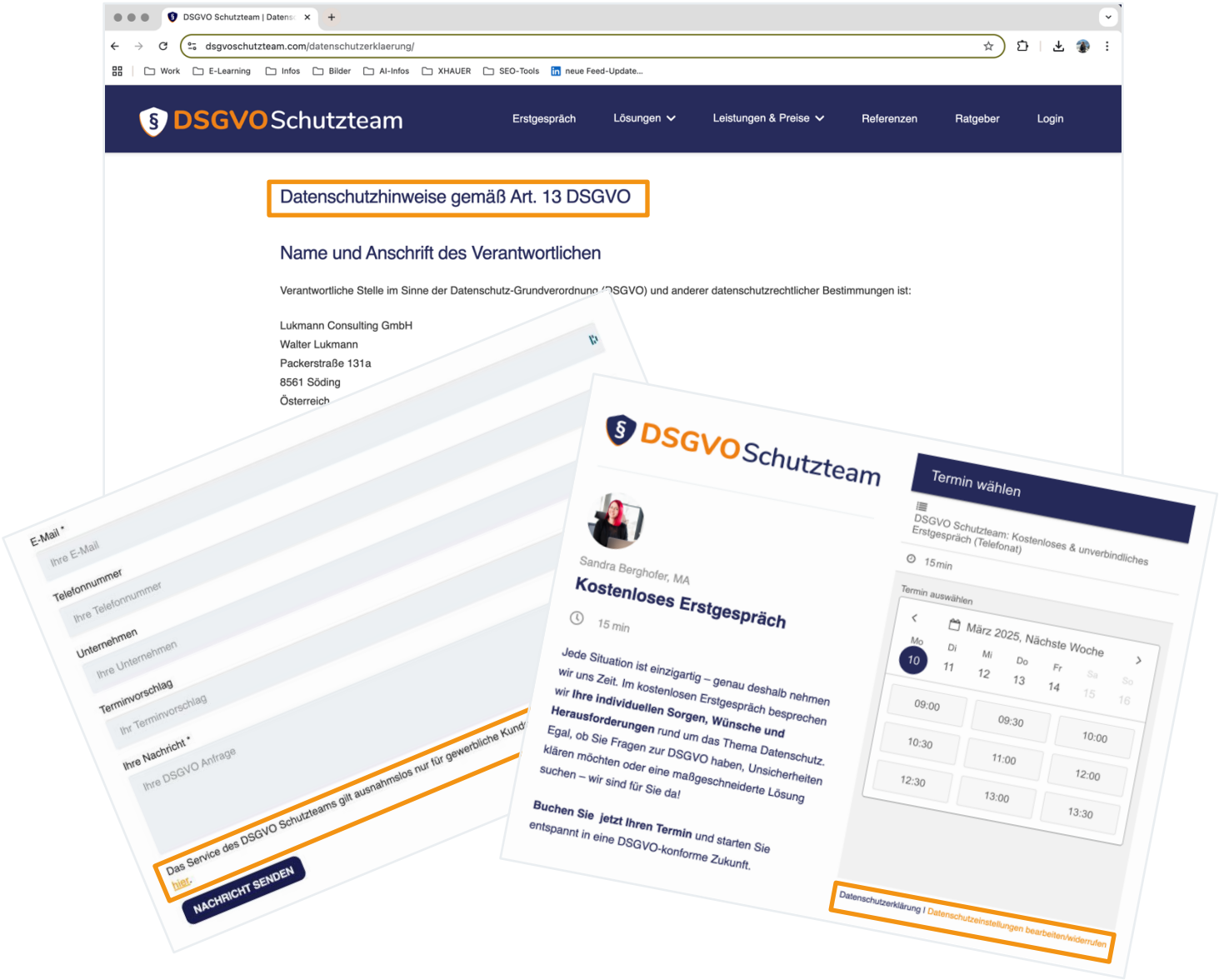
**Analyse & Marketing-Dienste**

➔ Webanalyse-Dienste (z.B. Google Analytics, Matomo)
➔ Social-Media-Management-Tools (z.B. z.B. Hootsuite, Buffer)
➔ Werbeplattformen mit personenbezogener Datenverarbeitung (z.B. Facebook Ads, Google Ads)

# 2. Informationspflicht & Datenschutz-Schulungen

Unternehmen sind nach Artikel 13 & 14 DSGVO verpflichtet, betroffene Personen transparent über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Das nennt man Informationspflicht.

## Deine Checkliste zu Informationspflicht & Datenschutz-Schulungen:



Ja ☐ Nein ☐

**Könnt ihr Datenschutzhinweise an eure Mitarbeiter, Bewerber und Kunden/Patienten aushändigen?**

*Wann muss informiert werden?*

1. Wenn Daten direkt bei der Person erhoben werden (z. B. Kontaktformular, Bewerbung, Online-Kauf).

2. Wenn Daten aus anderen Quellen stammen (z. B. gekaufte Adresslisten, öffentlich zugängliche Daten).

*Pflichtangaben für Datenschutzerklärungen, Verträge oder Websites:*

| | |
|---|---|
| **Verantwortlicher** | ➔ Name und Kontaktdaten des Unternehmens. |
| **Zweck der Verarbeitung** | ➔ Warum werden die Daten genutzt? |
| **Rechtsgrundlage** | ➔ z.B. Einwilligung, Vertragserfüllung |
| **Empfänger der Daten** | ➔ Wer bekommt die Daten (z.B. Dienstleister)? |
| **Drittland-Übermittlung** | ➔ Falls Daten außerhalb der EU gespeichert werden. |
| **Speicherdauer** | ➔ Wie lange bleiben Daten gespeichert? |
| **Betroffenenrechte** | ➔ Auskunft, Berichtigung, Löschung, Widerspruch |
| **Beschwerderecht** | ➔ Möglichkeit zur Beschwerde bei einer Datenschutzbehörde. |
| **Pflicht zur Bereitstellung** | ➔ Falls Daten für Vertrag notwendig sind. |
| **Automatisierte Entscheidungen** | ➔ Falls z.B. Algorithmus ohne menschliches Zutun entscheidet. |

Ja ☐ Nein ☐

**Schult ihr eure Mitarbeiter jährlich zum Thema Datenschutz?**

*Themen für ein Datenschutz-Sensibilisierungstraining:*

| | |
|---|---|
| **Datenschutz-Grundlagen** | ➔ Warum Datenschutz wichtig ist (DSGVO & BDSG). |
| **Personenbezogene Daten** | ➔ Was zählt dazu? Welche Schutzmaßnahmen sind nötig? |
| **Rechte von Betroffenen** | ➔ Auskunft, Berichtigung, Löschung, Widerspruch |
| **Datensicherheit im Alltag** | ➔ Passwörter, Phishing, E-Mails |
| **Vertraulichkeit & Zugriffsrechte** | ➔ Wer darf welche Daten einsehen/verarbeiten? |
| **Datenverarbeitung in Unternehmen** | ➔ Verzeichnisse, AVV |
| **Umgang mit DSGVO-Verletzungen** | ➔ Erkennung, Meldung, Folgen |
| **Social Engineering & Cybergefahren** | ➔ Täuschungsversuche & Schutzmaßnahmen |
| **Lösch- & Aufbewahrungsfristen** | ➔ Wann und wie müssen Daten gelöscht werden? |
| **Praxisbeispiele & Fallstudien** | ➔ Alltagssituationen und Best Practices |

💡 **Tipp:** Tests + interaktive Elemente fördern nachhaltig das Bewusstsein.

# 3. Betroffenenrechte & Datenschutzvorfälle

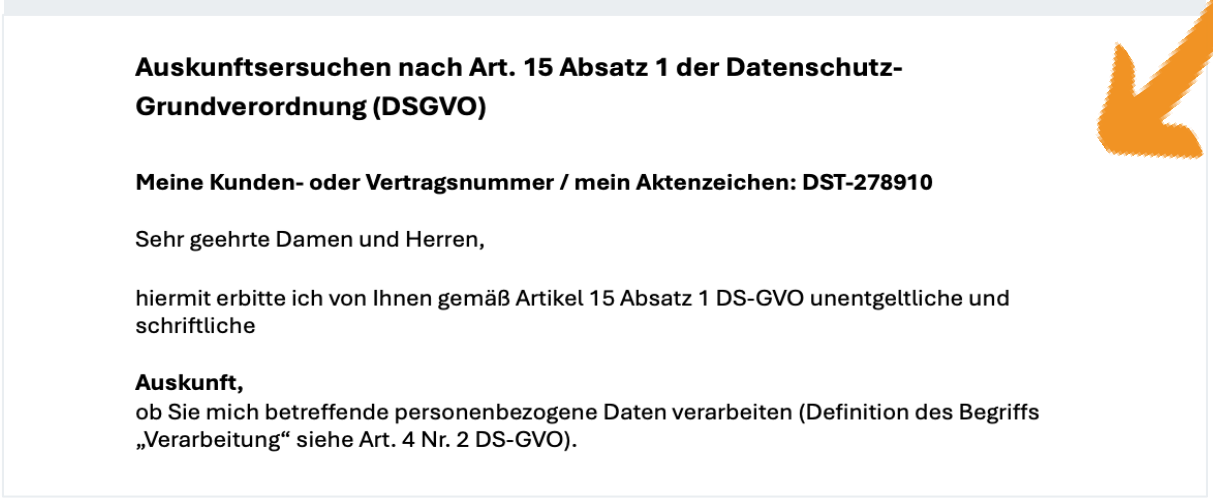
Betroffenenrecht– was ist das? Personen haben das Recht zu erfahren, was mit ihren Daten passiert. Sie können Auskunft verlangen oder ihre Daten löschen lassen. Das ist kein Spaß – unterschätzt den Aufwand nicht! Eine einzige Anfrage kann je nach Komplexität schnell Stunden oder sogar Tage kosten.

Und bei Datenschutzvorfällen? Hier zählt jede Sekunde

## Deine Checkliste zu Betroffenenrechten & Datenschutzvorfällen:

Ja ☐ Nein ☐ **Gibt es Prozesse zur Bearbeitung von Anfragen Betroffener (z.B. Auskunft, Löschung)?**

Du musst sicherstellen, dass ihr Anfragen von Betroffenen (auch Auskunfts-, Lösch- oder Berechtigungsanfrage genannt), innerhalb der gesetzlichen Fristen beantworten könnt. Diese sind meist zu kurz, um erst bei Eingang der Anfrage zu reagieren. – der Prozess und die nötigen Dokumente sollten bereits im Voraus vorhanden sein.



**Auskunftsersuchen nach Art. 15 Absatz 1 der Datenschutz-Grundverordnung (DSGVO)**

**Meine Kunden- oder Vertragsnummer / mein Aktenzeichen: DST-278910**

Sehr geehrte Damen und Herren,

hiermit erbitte ich von Ihnen gemäß Artikel 15 Absatz 1 DS-GVO unentgeltliche und schriftliche

**Auskunft,**
ob Sie mich betreffende personenbezogene Daten verarbeiten (Definition des Begriffs „Verarbeitung“ siehe Art. 4 Nr. 2 DS-GVO).

Ja ☐ Nein ☐

**Gibt es einen festen Ablauf für den Umgang mit Datenschutzvorfällen/Datenpannen?**

*Beispiele für Datenpannen gemäß DSGVO:*

| | |
|---|---|
| **Verlust von Geräten** | ➔ Laptop oder USB-Stick mit sensiblen Daten wird gestohlen/verloren. |
| **Fehlversand von E-Mails** | ➔ Personenbezogene Daten werden an falschen Empfänger geschickt. |
| **Offene CC bei E-Mails** | ➔ E-Mail-Adressen mehrere Empfänger für alle sichtbar satt in BCC. |
| **Hackerangriff** | ➔ Unbefugte verschaffen sich Zugriff auf Kundendaten/Systeme |
| **Phishing-Angriff** | ➔ Mitarbeiter geben versehentlich Login-Daten preis. |
| **Unverschlüsselte Datenübertragung** | ➔ Laden nur mit Zustimmung (z.B. YouTube, Google Maps) |
| **Datenleck durch Fehlkonfiguration** | ➔ Eine Cloud-Datenbank ist öffentlich zugänglich. |
| **Falsch entsorgte Dokumente** | ➔ Personenbezogene Daten landen ungeschreddert im Papiermüll. |
| **Zugriff durch Unbefugte** | ➔ Ein Ex-Mitarbeiter hat noch Zugriff auf interne Systeme. |
| **Verlust von Backup-Daten** | ➔ Keine Wiederherstellung möglich, z.B. durch Ransomware |

💡 **Wichtig:** Datenpannen müssen nach Art. 33 DSGVO in bestimmten Fällen innerhalb von 72h der Behörde gemeldet werden!

# 4. Website

Sie ist euer Aushängeschild nach außen und die größte **DSGVO-Schwachstelle**. Sei hier besonders sorgfältig! Stelle unbedingt sicher, dass hier IMMER alles vollständig und korrekt ist.



## Deine Checkliste zur Website:

Ja ☐ Nein ☐ **Erfüllt eure Website alle gesetzlichen Datenschutz-Anforderungen?**

*Diese Anforderungen müsst ihr erfüllen:*

| | |
|---|---|
| **SSL-Verschlüsselung** | ➔ HTTPS ist Pflicht! |
| **Cookie Banner** | ➔ DSGVO-konform, echte Einwilligung (kein voreingestelltes Ja-Häkchen!) |
| **Datenschutzerklärung** | ➔ Vollständig, leicht zu finden, aktuell |
| **Kontaktformulare** | ➔ Datenschutzhinweis + Einwilligung vor Absenden |
| **Analyse & Tracking** | ➔ Nur mit Einwilligung (z.B. Google Analytics) |
| **Drittanbieter-Plugins** | ➔ Laden nur mit Zustimmung (z.B. YouTube, Google Maps) |
| **Newsletter-Anmeldung** | ➔ Double-Opt-in + Hinweis auf Widerruf |
| **Auftragsverarbeiter (AVV)** | ➔ Falls externe Dienstleister personenbezogene Daten verarbeiten. |
| **Widerruf & Löschung** | ➔ Betroffenenrechte klar kommunizieren. |
| **Impressum & Kontakt** | ➔ Vollständige Angaben des Unternehmens |

💡 **Tipp:** Regelmäßige Überprüfung sichert DSGVO-Konformität!

# Was ist der nächste Schritt zu mehr Sicherheit?

Zähle je Checkliste die Anzahl der Haken bei „Ja“ („Ich weiß es nicht“ = Haken bei “Nein“), die du machen konntest. Dein Ergebnis kannst du unten in die jeweiligen Felder eintragen. (z.B. für „1. Dokumentationspflicht“ 3 von 4)

| | |
|---|---|
| 1. Dokumentationspflicht | ____ von 4 |
| 2. Informationspflicht & Datenschutz-Schulungen | ____ von 2 |
| 3. Betroffenenrechte & Datenschutzvorfälle | ____ von 2 |
| 4. Website | ____ von 1 |
| GESAMT | ____ von 9 |

In welchem der 4 Bereiche hast keine der Punkte bestätigen können? Analysiere deine Ergebnisse auf der folgenden Seite.

# Endspurt: Deine Bewertung

| Punktzahl | Bewertung |
| --- | --- |
| 0 - 5 Punkte | **DSGVO Outlaws** – Ihr habt die DSGVO bisher zu locker genommen. Jetzt seit ihr auf der Überholspur zum Bußgeld. Die Behörde schmeißt schonmal das Blaulicht an. Bevor es zum teuren Fiasko kommt, holt euch Unterstützung. |
| 6 – 7 Punkte | **DSGVO-Taktiker** – Ihr seit die Pragmatiker unter den Datenschützern – das Nötigste habt ihr im Griff, damit es nicht krackt. Der Meisterstatus ist greifbar, aber es bleibt riskant. |
| 8 – 9 Punkte | **DSGVO Meister** – Ihr seit so sicher, dass sogar Behörden den Hut ziehen. Bleibt dran! |

Du willst deine DSGVO-Pflichten schnell + einfach erledigen oder ihr habt nicht die Kapazität, Lücken selbst zu schließen?

Dann freue ich mich auf das Gespräch mit dir!

**Fragen oder Feedback?**

Vereinbare gerne einen Termin zum persönlichen Gespräch.

*Dein Daniel Lukmann*

**Vereinbare deinen Termin zum Gespräch über diesen Link:**

👉 **dsgvoschutzteam.com/termin**

DSGVO Schutzteam