DSGVO-Leitfaden für Handwerksbetriebe

Was muss mein Betrieb tun? Schritt für Schritt erklärt — Stand 2026

Gilt die DSGVO für meinen Handwerksbetrieb? Ja — ohne Ausnahme. Jeder Betrieb, der Kundendaten, Mitarbeiterdaten oder eine Website hat, muss die DSGVO einhalten. Egal ob Einmann-Betrieb oder 50 Mitarbeiter. Bei Verstößen drohen Bußgelder bis zu 20 Mio. Euro oder 4 % des Jahresumsatzes (Art. 83 DSGVO).

Schritt für Schritt: Was Sie jetzt tun müssen

1 Verarbeitungsverzeichnis anlegen

Listen Sie auf, welche Daten Sie warum und wie lange speichern (Art. 30 DSGVO). Mindestens: Kundenverwaltung, Mitarbeiterdaten, Zeiterfassung, Lohnbuchhaltung, Website.

2 Datenschutzerklärung Website

Jede Website braucht eine Datenschutzerklärung (Art. 13 DSGVO). Diese muss über alle Datenverarbeitungen informieren: Hosting, Kontaktformular, Analytics, Cookies.

3 Auftragsverarbeitungsverträge (AVV)

Mit jedem Dienstleister, der Ihre Daten verarbeitet, brauchen Sie einen AVV (Art. 28 DSGVO): Hosting-Anbieter, Cloud-Software, Steuerberater, IT-Dienstleister.

4 Mitarbeiter belehren

Alle Mitarbeiter müssen auf den vertraulichen Umgang mit Daten hingewiesen werden. Schriftliche Belehrung + Unterschrift → in die Personalakte.

5 Technisch-organisatorische Maßnahmen (TOM)

Dokumentieren Sie, wie Sie Daten schützen: Passwörter, Bildschirmsperre, Backup, Virenschutz, abschließbare Räume, Aktenvernichter.

6 Einwilligungen einholen

Für Baustellenfotos mit Personen, GPS-Tracking, Newsletter, WhatsApp-Kommunikation. Schriftlich, freiwillig, widerrufbar.

7 Löschkonzept erstellen

Wann werden welche Daten gelöscht? Steuerunterlagen: 10 Jahre. Geschäftsbriefe: 6 Jahre. Bewerbungen (Absagen): 6 Monate. Kontaktanfragen: 6 Monate.

8 Notfallplan Datenpanne

Datenpannen müssen innerhalb 72 Stunden der Aufsichtsbehörde gemeldet werden (Art. 33 DSGVO). Legen Sie fest: Wer ist zuständig? Wie wird gemeldet?

Checkliste: Ist Ihr Betrieb DSGVO-fit?

- ☐ Verarbeitungsverzeichnis erstellt und aktuell
- ☐ Datenschutzerklärung auf der Website (mit Impressum verlinkt)
- ☐ Cookie-Banner mit Einwilligungsmöglichkeit
- ☐ AVV mit allen Dienstleistern abgeschlossen (Hosting, Cloud, Steuerberater)
- ☐ Mitarbeiter schriftlich auf Datenschutz verpflichtet
- ☐ Passwörter sicher (keine Zettel am Monitor!)
- ☐ Bildschirmsperre auf allen Geräten aktiv
- ☐ Regelmäßiges Backup der Daten
- ☐ Virenschutz und Firewall aktuell
- ☐ Einwilligungen für Fotos / GPS / WhatsApp vorhanden
- ☐ Löschfristen definiert und eingehalten
- ☐ Datenschutzbeauftragter benannt (Pflicht ab 20 Personen in Datenverarbeitung)

Die 10 häufigsten DSGVO-Fragen von Handwerkern

1. Brauche ich als kleiner Betrieb einen Datenschutzbeauftragten?

Ein Datenschutzbeauftragter ist nach § 38 BDSG erst Pflicht, wenn mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Für die meisten Handwerksbetriebe gilt das nicht. Das bedeutet aber nicht, dass Sie sich nicht um Datenschutz kümmern müssen — die DSGVO gilt trotzdem vollständig.

2. Darf ich Kundendaten in meinem Handy speichern?

Ja, aber nur auf einem dienstlichen Gerät mit Zugangssperre (PIN/Biometrie). Auf privaten Handys sollten keine Kundendaten gespeichert werden. Besonders problematisch: WhatsApp synchronisiert Ihr gesamtes Adressbuch zu Meta/Facebook.

3. Darf ich Baustellenfotos für meine Website nutzen?

Fotos von Arbeiten: ja. Fotos, auf denen Personen erkennbar sind: nur mit schriftlicher Einwilligung. Achten Sie auch auf Hausnummern, Namensschilder und Kfz-Kennzeichen — diese müssen unkenntlich gemacht werden.

4. Muss ich ein Verarbeitungsverzeichnis führen?

Ja. Zwar gibt es eine Ausnahme für Betriebe unter 250 Mitarbeitern (Art. 30 Abs. 5 DSGVO), aber diese gilt nur, wenn die Verarbeitung „gelegentlich" erfolgt. Da jeder Handwerksbetrieb regelmäßig Kunden- und Mitarbeiterdaten verarbeitet, greift die Ausnahme nicht.

5. Was mache ich bei einer Datenpanne?

Beispiel: Laptop mit Kundendaten gestohlen, E-Mail mit Kundenliste an falschen Empfänger. Dann gilt: Sofort dokumentieren, Risiko bewerten. Wenn ein Risiko für die Betroffenen besteht → Meldung an die Datenschutz-Aufsichtsbehörde Ihres Bundeslandes innerhalb von 72 Stunden. Bei hohem Risiko auch die Betroffenen informieren.

6. Darf ich GPS-Tracking für meine Mitarbeiter nutzen?

Nur mit ausdrücklicher, freiwilliger Einwilligung der Mitarbeiter und nur zu eng begrenzten Zwecken (Zeiterfassung, Einsatzplanung). Eine heimliche oder lückenlose Überwachung ist unzulässig. Betriebsrat (falls vorhanden) hat Mitbestimmungsrecht.

7. Brauche ich einen AVV mit meinem Steuerberater?

Das kommt darauf an: Wenn Ihr Steuerberater eigenverantwortlich die Buchhaltung führt (eigene Berufspflichten), ist er kein Auftragsverarbeiter, sondern eigenständig Verantwortlicher. Ein AVV ist dann nicht nötig. Wenn er jedoch nur weisungsgebunden Daten verarbeitet (z. B. reine Dateneingabe), brauchen Sie einen AVV. Im Zweifel: Steuerberater fragen.

8. Wie lange muss ich Kundendaten aufbewahren?

Rechnungen und Buchungsbelege: 10 Jahre (§ 147 AO). Geschäftsbriefe (auch E-Mails): 6 Jahre (§ 257 HGB). Gewährleistung Bauwerk: 5 Jahre (§ 634a BGB). Danach: löschen, sofern kein anderer Grund für die Speicherung besteht.

9. Darf ich WhatsApp geschäftlich nutzen?

Nur mit ausdrücklicher Einwilligung des Gesprächspartners und unter strengen Auflagen (separates Diensthandy, keine Kundendaten im privaten Adressbuch). Die Nutzung ist datenschutzrechtlich riskant, da WhatsApp Kontaktdaten an Meta übermittelt. Besser: Signal, Threema Work oder E-Mail.

10. Was kostet ein DSGVO-Verstoß?

Theoretisch bis zu 20 Mio. Euro oder 4 % des Jahresumsatzes. In der Praxis verhängen Aufsichtsbehörden bei kleinen Betrieben meist Bußgelder zwischen 500 € und 10.000 €. Häufigste Verstöße: fehlende Datenschutzerklärung auf der Website, fehlende Cookie-Einwilligung, fehlende AVVs.

Wichtig: Dieser Leitfaden bietet eine allgemeine Orientierung und ersetzt keine individuelle Rechtsberatung. Bei Unsicherheiten wenden Sie sich an einen Datenschutzbeauftragten oder einen auf Datenschutz spezialisierten Rechtsanwalt. Ihre zuständige Handwerkskammer bietet häufig kostenlose DSGVO-Beratungen an.