10-Punkte DSGVO-Checkliste

werkstatt-ratgeber.de

Die wichtigsten Datenschutz-Pflichten für Handwerksbetriebe — verständlich und praxisnah

Seit Mai 2018 gilt die DSGVO — und sie betrifft jeden Betrieb, egal wie klein. Auch Handwerksbetriebe mit 3 Mitarbeitern müssen die Regeln einhalten. Bei Verstößen drohen **Bußgelder bis zu 20 Mio. € oder 4 % des Jahresumsatzes** (Art. 83 DSGVO). Diese Checkliste zeigt dir die 10 wichtigsten Punkte — ohne Juristendeutsch.

1 Verarbeitungsverzeichnis erstellen ☐

Schreib auf, **welche personenbezogenen Daten** du speicherst: Kundenadressen, Mitarbeiter-Stammdaten, Zeiterfassung, GPS-Daten, Fotos. Pro Kategorie notieren: Zweck, Rechtsgrundlage, Löschfrist. **Art. 30 DSGVO**

💡 Pflicht ab 250 Mitarbeitern — aber auch für kleinere Betriebe, wenn regelmäßig personenbezogene Daten verarbeitet werden (und das tut jeder Betrieb).

2 Datenschutzerklärung auf der Website ☐

Jede Website braucht eine **vollständige Datenschutzerklärung** mit: Name des Verantwortlichen, Kontaktdaten, welche Daten erhoben werden (Kontaktformular, Cookies, Analytics), Rechtsgrundlagen, Speicherdauer, Betroffenenrechte. **Art. 13 & 14 DSGVO**

💡 Cookie-Banner nicht vergessen! Tracking-Tools (Google Analytics) nur mit Einwilligung. Consent-Tool einsetzen.

3 Auftragsverarbeitungsverträge (AVV) abschließen ☐

Mit **jedem Dienstleister**, der Zugriff auf personenbezogene Daten hat, brauchst du einen AVV: Cloud-Software (Buchhaltung, Zeiterfassung), E-Mail-Provider, Steuerberater, IT-Support, Newsletter-Tool. **Art. 28 DSGVO**

💡 Die meisten Cloud-Anbieter bieten fertige AVVs zum Download an. Einfach anfordern und unterschrieben ablegen.

4 Einwilligung für Fotos einholen ☐

Baustellenfotos mit **erkennbaren Personen** (Mitarbeiter, Kunden, Passanten) brauchen eine Einwilligung — besonders bei Verwendung für Social Media, Website oder Referenzen. Schriftlich dokumentieren! **Art. 6 Abs. 1a DSGVO + § 22 KUG**

5 Mitarbeiter-Datenschutz beachten ☐

Zeiterfassung ist Pflicht, aber GPS-Tracking nur mit ausdrücklicher Einwilligung. Videoüberwachung am Arbeitsplatz nur in Ausnahmefällen. Krankmeldungen vertraulich behandeln, kein Zugriff für unbefugte Kollegen. **§ 26 BDSG**

💡 GPS-Ortung der Firmenfahrzeuge: Mitarbeiter müssen vorher schriftlich einwilligen und die Ortung außerhalb der Arbeitszeit muss deaktiviert sein.

6 Kommunikation DSGVO-konform gestalten ☐

Keine Kundendaten per WhatsApp verschicken — WhatsApp gibt Metadaten an Meta weiter. Angebote, Rechnungen und Kundendaten nur per E-Mail (idealerweise verschlüsselt) oder über ein sicheres Kundenportal.

💡 Alternative zu WhatsApp für die Team-Kommunikation: Signal, Threema Work oder ein Firmen-Messenger.

7 Löschfristen einhalten ☐

Daten nur so lange speichern wie nötig. **Aufbewahrungsfristen beachten:** Rechnungen und Buchungsbelege 10 Jahre (§ 147 AO), Handelsbriefe 6 Jahre (§ 257 HGB), Bewerbungsunterlagen max. 6 Monate nach Absage, Kundendaten nach Vertragsende + Verjährungsfristen. **Art. 17 DSGVO**

8 Datenpannen melden — 72-Stunden-Frist! ☐

Laptop verloren? E-Mail an falschen Empfänger? Hackerangriff? → **Innerhalb von 72 Stunden** an die zuständige Landesdatenschutzbehörde melden. Bei hohem Risiko auch die betroffenen Personen informieren. **Art. 33 & 34 DSGVO**

💡 Vorab klären: Wer ist die zuständige Behörde in deinem Bundesland? Kontaktdaten griffbereit halten.

9 Betroffenenrechte gewährleisten ☐

Kunden und Mitarbeiter haben das Recht auf: **Auskunft** (welche Daten?), **Berichtigung** (falsche Daten korrigieren), **Löschung** (»Recht auf Vergessenwerden«), **Datenübertragbarkeit**. Anfragen innerhalb von 1 Monat beantworten. **Art. 15–20 DSGVO**

10 Technische Schutzmaßnahmen umsetzen

Mindeststandards: Starke Passwörter (min. 12 Zeichen) + Passwort-Manager, Bildschirmsperre auf allen Geräten, regelmäßige Backups (3-2-1-Regel), Software-Updates zeitnah einspielen, Festplattenverschlüsselung auf Laptops, WLAN mit WPA3/WPA2 absichern. **Art. 32 DSGVO**

💡 Alte Festplatten und USB-Sticks nicht einfach wegwerfen — Daten vorher sicher löschen oder Datenträger physisch zerstören.