DSGVO-Checkliste für die Website

Was wirklich Pflicht ist – und was Sie sich sparen können · Stand 2026

Diese Liste ist bewusst **ehrlich** – inklusive der Punkte, die Sie sich komplett sparen können. Haken Sie ab, was bei Ihnen erledigt ist. Faustregel: Was Sie gar nicht erst einbauen (Tracker, externe Schriften, eingebettete Karten), müssen Sie auch nicht absichern.

Pflicht JEDE GESCHÄFTLICHE WEBSITE

- [ ] **Datenschutzerklärung** anlegen, klar benannt, von jeder Unterseite per Footer-Link erreichbar (max. 2 Klicks).
- [ ] **Verantwortlichen** vollständig nennen (Name/Firma, Anschrift, E-Mail); Datenschutzbeauftragten nur, falls bestellt.
- [ ] Baustein **Server-Logfiles/Hosting**: erfasste Daten (u. a. IP), Zweck, Rechtsgrundlage (Art. 6 Abs. 1 lit. f), Speicherdauer.
- [ ] Pro Funktion **Zweck + passende Rechtsgrundlage** (Art. 6); bei „berechtigtem Interesse“ das Interesse konkret benennen.
- [ ] Alle **Betroffenenrechte** auflisten + Widerrufs- und Beschwerderecht.
- [ ] **Empfänger** und jeden **Drittland-Transfer** (v. a. USA) mit Garantie ausweisen.
- [ ] **Keine Muster-Bausteine** für Dienste übernehmen, die Sie gar nicht nutzen – und genutzte nicht vergessen.
- [ ] **Impressum** nach § 5 DDG; veraltete Verweise korrigieren („TMG“ → „DDG“, „TTDSG“ → „TDDDG“).
- [ ] **HTTPS** erzwingen (gültiges Zertifikat, HTTP-zu-HTTPS-Weiterleitung); Formulare nur verschlüsselt.
- [ ] **Auftragsverarbeitungsvertrag (AVV)** mit jedem Dienstleister – nicht nur mit dem Hoster.
- [ ] Internes **Verzeichnis von Verarbeitungstätigkeiten** (Art. 30) führen – nicht veröffentlichen.
- [ ] Prozess für **Betroffenenrechte** (binnen 1 Monat) und **Datenpannen** (Meldung binnen 72 Stunden).
- [ ] Datenschutzerklärung **aktuell halten** – bei jeder neuen Funktion anpassen.

Empfohlen MACHT SIE SICHERER & OFT EINFACHER

- [ ] **Schriften, Skripte, Stylesheets lokal** einbinden statt von Google-CDN/fremden Servern.
- [ ] **Google Maps & YouTube** durch ein statisches Bild bzw. eine Zwei-Klick-Lösung ersetzen.
- [ ] **Spam-Schutz datensparsam** lösen (serverseitiger Honeypot) statt Google reCAPTCHA.
- [ ] Beim **Kontaktformular** auf eine Einwilligungs-Checkbox verzichten; nur Hinweis + Link + Pflichtfelder sparsam.
- [ ] **Personenfotos** (Team/Kunden/Mitglieder) nur mit dokumentierter, möglichst schriftlicher Einwilligung.
- [ ] Personen mit Datenzugang (auch Aushilfen, Ehrenamtliche) auf **Vertraulichkeit** verpflichten.
- [ ] Fertige Seite mit dem **Browser-Netzwerk-Tab** auf ungefragte externe Verbindungen prüfen (Ziel: null).

Kommt darauf an NUR, WENN IHRE SEITE DAS NUTZT

- [ ] **Cookie-Banner** nur, wenn nicht-notwendige Cookies/Drittdienste laden – sonst weglassen.
- [ ] Falls Banner nötig: **Opt-in**, „Alle ablehnen“ gleichwertig auf erster Ebene, granular, keine Dark Patterns.
- [ ] Eingebettete **Buchungs-, Chat- oder Bewertungs-Widgets** nur mit Einwilligung/Zwei-Klick oder als EU-/serverseitige Lösung.
- [ ] **Meta-Pixel/Social-Plugins** nur bei aktiven Werbekampagnen – mit Einwilligung; sonst weglassen.
- [ ] Bei unvermeidbaren **US-Diensten** prüfen, ob der Anbieter unter dem Data Privacy Framework zertifiziert ist; sonst Standardvertragsklauseln.
- [ ] **Datenschutzbeauftragten** prüfen (i. d. R. ab 20 Personen ständig mit automatisierter Verarbeitung).

Keine Rechtsberatung. Diese Checkliste ist eine sorgfältig recherchierte Orientierung (Stand 2026, geprüft gegen DSGVO, TDDDG und DDG) und ersetzt keine individuelle Rechtsberatung. Im Zweifel – besonders bei Abmahnungen – gehört ein Fachanwalt eingeschaltet.

Website neu oder datensparsam umbauen lassen? donauwebdesign.de/kontakt · handcodiert, ohne WordPress, ohne unnötige Tracker.