



Rechtslage: Datenschutz & Cookie-Consent

Keine Abmahnungen riskieren! Eine absolute Sensibilität für DSGVO/GDPR Regeln. Von korrekten Formularen bis hin zu rechtskonformen Cookie-Bannern ohne Tracking-Verluste. Diese Liste ersetzt keine anwaltliche Prüfung (eRecht24 / IT-Recht Kanzlei), aber filtert die größten Fehler aus.

1. Das Cookie & Tracking Setup (Consent)

- ☐ **Banner "Before Load":** Blockiert dein Consent-Tool (wie Borlabs Cookie oder Real Cookie Banner) sämtliche externe Skripte (Meta Pixel, Google Analytics) strikt, BIS der Nutzer aktiv auf "Akzeptieren" gedrückt hat?
- ☐ **Transparente Speicherung:** Kann der Nutzer im Cookie-Banner exakt einsehen, welche Daten (Statistik, Marketing, Essenziell) wohin gefunkt werden?
- ☐ **Leichter Opt-Out:** In deiner Datenschutzerklärung muss per Gesetz zwingend ein Link sein, um das Cookie-Banner wieder aufzurufen und die Einwilligung sofort zu revidieren.

2. Formulare & Nutzerdaten

- ☐ **Pflichtfelder minimiert:** Datensparsamkeit. Nimm nie eine Telefonnummer als "Pflichtfeld *", wenn für das Ziel eine E-Mail vollkommen ausreicht. Was man nicht anfragt, muss nicht gelöscht werden.
- ☐ **Privacy-Verweis (Checkbox optional):** Früher Standard, heute nur wichtig, falls Werbezwecke (Newsletter) folgen: Steht direkt unter dem Formular ein Text "Mit dem Absenden, stimmst du der Datenschutzerklärung zu" mit echtem Link?
- ☐ **SSL-Übersendung:** Da du in Kontaktformularen teils empfindliche Daten sammelst, ist SSL/HTTPS als Transfer-Voraussetzung extrem wichtig (sollte ohnehin Standard sein).

3. Externe Verbindungen & Fonts

- ☐ **Google Fonts LOKAL einbinden!** Lade Fonts niemals direkt von `fonts.googleapis.com` herunter, da dies die IP-Adresse des Users illegal nach Amerika (Google) sendet. (Einer der absoluten Top-Abmahngründe!). Die Fonts müssen auf den eigenen Server geladen werden.
- ☐ **Video-Einbettungen:** Lade YouTube-Videos nicht bloß via iFrame hoch. Nutze die Option "Erweiterter Datenschutzmodus" (`youtube-nocookie.com`) oder ein Vorschaubild, bei dem man zum Aktivieren erst klicken muss (Borlabs kann das blocken).
- ☐ **Google Maps:** Zeigt Maps erst an, wenn man sein Einverständnis gibt (die Google API trackt massiv).

4. Technischer Datenschutz

- ☐ **Server-Standort:** Steht das Hosting oder der CDN in Europa und ist vertraglich sicher (z.B. EU-U.S. Data Privacy Framework)?
- ☐ **AVV (Auftragsdatenverarbeitungsvertrag):** Mit wem du zusammenarbeitest (Mailchimp, Hoster, Agentur, Google), benötigst du (teils digital abgeschlossen) einen AV-Vertrag.

Tipp der Profis: Ein gutes Consent-Banner vernichtet keine Performance, es stärkt das Vertrauen in die DSGVO! Nutze Tools, die auf deiner Website auch bei verweigertem Tracking weiterhin datenschutzkonforme "Essenzielle" Besucherzählungen (ohne Cookies) zulassen – Tools wie Fathom oder Matomo eignen sich da hervorragend.