DSGVO-Checkliste für Online-Shops: So bleibt dein Shop rechtssicher

Die DSGVO-Compliance deines Online-Shops ist essenziell, um Datenschutzrisiken zu minimieren, Abmahnungen zu vermeiden und das Vertrauen deiner Kundschaft zu stärken. Diese Checkliste deckt alle relevanten Bereiche ab, die du regelmäßig überprüfen solltest – praxisnah und aktuell.

1. Datenschutzorganisation & Verantwortlichkeiten

- ☐ Wurde ein *Datenschutzbeauftragte*r benannt? (In der Regel Pflicht ab 20 Personen, die regelmäßig mit personenbezogenen Daten arbeiten – aber auch bei bestimmten Verarbeitungstätigkeiten bereits darunter erforderlich, z. B. gem. § 38 Abs. 1 BDSG.)
- ☐ Gibt es ein schriftliches Datenschutzkonzept für deinen Shop?
- ☐ Werden regelmäßige Datenschutz-Audits durchgeführt (mind. einmal jährlich)?

2. Verzeichnis von Verarbeitungstätigkeiten

- ☐ Sind alle Verarbeitungstätigkeiten gem. Art. 30 DSGVO dokumentiert? (z. B. Kundendaten, Zahlungsabwicklung, Newsletter)
- ☐ Wurden Speicherfristen definiert und Löschfristen technisch umgesetzt?

3. Datenschutzfreundliche Gestaltung (Privacy by Design & Default)

- ☐ Werden Datenschutzmaßnahmen bereits in der Entwicklungsphase berücksichtigt?
- ☐ Sind nur datenschutzfreundliche Voreinstellungen aktiviert (Privacy by Default)?
- ☐ Wird auf Datenminimierung geachtet – insbesondere auf den Verzicht auf sensible Informationen, wenn nicht erforderlich?

4. Datenschutzerklärung & Impressum

- ☐ Ist die Datenschutzerklärung aktuell, verständlich und einfach zugänglich?
- ☐ Werden alle Pflichtinhalte abgedeckt (Zwecke, Rechtsgrundlagen, Empfänger, Drittlandtransfers, Betroffenenrechte)?

Hinweis: Das Impressum ist rechtlich verpflichtend nach TMG/DDG, nicht nach DSGVO. Trotzdem sollte es korrekt und leicht auffindbar sein.

5. Cookie-Banner & Einwilligungsmanagement

- ☐ Werden nicht essenzielle Cookies erst nach aktiver Einwilligung gesetzt?
- ☐ Ist die Einwilligung freiwillig, informiert und dokumentiert (z. B. per Consent Management Tool)?
- ☐ Können Einwilligungen jederzeit einfach widerrufen werden (z. B. über Cookie-Link im Footer)?

6. Webanalyse & Tracking-Tools

- ☐ Werden Tracking-Skripte erst nach gültigem Consent geladen?
- ☐ Ist bei Google Analytics die IP-Anonymisierung aktiviert?
- ☐ Besteht ein AV-Vertrag mit Tracking-Anbietern?
- ☐ Wurden datenschutzfreundliche Alternativen geprüft (z. B. Matomo, Piwik PRO)?

7. Sicherheit der Kundendaten

- ☐ Wird TLS/SSL für die gesamte Website verwendet?
- ☐ Ist 2FA für administrative Zugänge aktiviert?
- ☐ Gibt es ein aktuelles, geprüftes Backup-Konzept?
- ☐ Ist der Zugriff auf Daten rollenbasiert beschränkt?
- ☐ Werden Löschkonzepte technisch umgesetzt?

8. Betroffenenrechte gewährleisten

- ☐ Können Nutzer ihre Rechte auf Auskunft, Löschung, Berichtigung und Datenübertragbarkeit einfach wahrnehmen?
- ☐ Werden Anfragen innerhalb von 30 Tagen beantwortet?
- ☐ Bestehen dokumentierte Prozesse (z. B. Ticketsystem) zur Bearbeitung dieser Anfragen?

9. Zusammenarbeit mit Dienstleistern & Drittanbietern

- ☐ Bestehen AV-Verträge mit allen Dienstleistern, die in deinem Auftrag personenbezogene Daten verarbeiten (z. B. Hosting, Newsletter)?
- ☐ Wurde geprüft, ob es sich ggf. nicht um eine Auftragsverarbeitung, sondern um eigene oder gemeinsame Verantwortlichkeit handelt (z. B. Zahlungsdienste, CRM)?
- ☐ Sind alle Drittanbieter-Tools DSGVO-konform konfiguriert und dokumentiert?
- ☐ Findet ein Datentransfer in Drittländer statt? Wenn ja:
    - ☐ Ist der Anbieter nach dem EU-US Data Privacy Framework zertifiziert?

- ☐ Falls nicht: Wurden Standardvertragsklauseln (SCCs) abgeschlossen und zusätzliche Schutzmaßnahmen getroffen?
- ☐ Optional: Gibt es eine datenschutzfreundlichere Alternative mit Hosting in der EU?

10. Technische Datenschutzmaßnahmen (TOMs)

- ☐ Werden personenbezogene Daten durch technische Maßnahmen wie Verschlüsselung und Zugriffskontrollen geschützt?
- ☐ Ist eine rollenbasierte Rechtevergabe im System hinterlegt?
- ☐ Werden Daten pseudonymisiert oder anonymisiert, wo möglich?
- ☐ Wurden alle Prozesse und Systeme im Verzeichnis der Verarbeitungstätigkeiten korrekt erfasst?