GDPR Checklist for Online Shops: How to Keep Your Shop Legally Compliant

The GDPR compliance of your online shop is essential to minimize data protection risks, avoid warnings and strengthen your customer's trust. This checklist covers all relevant areas that you should review regularly – practical and up-to-date.

1. Data Protection Organization & Responsibilities

- □ Has a Data Protection Officer been appointed? (In general mandatory for 20 persons regularly working with personal data – but also required for certain processing activities below that threshold, e.g. according to § 38 para. 1 BDSG.)
- □ Is there a written data protection concept for your shop?
- □ Are regular data protection audits carried out (at least once a year)?

2. Record of Processing Activities

- □ Are all processing activities documented according to Art. 30 GDPR (e.g. customer data, payment processing, newsletter)?
- □ Have retention periods been defined and deletion periods technically implemented?

3. Privacy-friendly Design (Privacy by Design & Default)

- □ Are data protection measures considered already during the development phase?
- □ Are only privacy-friendly default settings activated (Privacy by Default)?
- □ Is data minimization observed – especially avoiding sensitive information when not required?

4. Privacy Policy & Legal Notice

- □ Is the privacy policy up to date, understandable and easily accessible?
- □ Are all mandatory contents covered (purposes, legal bases, recipients, third country transfers, data subject rights)?

Note: The legal notice is legally required under TMG/DDG, not under GDPR. Nevertheless, it should be correct and easy to find.

5. Cookie Banner & Consent Management

- □ Are non-essential cookies only set after active consent?
- □ Is consent voluntary, informed and documented (e.g. via consent management tool)?
- □ Can consents be easily revoked at any time (e.g. via cookie link in the footer)?

6. Web Analytics & Tracking Tools

- □ Are tracking scripts only loaded after valid consent?
- □ Is IP anonymization activated for Google Analytics?
- □ Is there a data processing agreement with tracking providers?
- □ Have privacy-friendly alternatives been reviewed (e.g. Matomo, Piwik PRO)?

7. Customer Data Security

- □ Is TLS/SSL used for the entire website?
- □ Is 2FA activated for administrative accesses?
- □ Is there a current, tested backup concept?
- □ Is access to data restricted by role-based permissions?
- □ Are deletion processes technically implemented?

8. Safeguarding Data Subject Rights

- □ Can users easily exercise their rights of access, erasure, correction, and data portability?
- □ Are requests answered within 30 days?
- □ Are there documented processes (e.g. ticket system) to handle these requests?

9. Cooperation with Service Providers & Third Parties

- □ Are data processing agreements (DPAs) in place with all service providers processing personal data on your behalf (e.g. hosting, newsletters)?
- □ Has it been checked whether processing is actually commissioned processing or joint / independent responsibility (e.g. payment services, CRM)?
- □ Are all third-party tools configured and documented in a GDPR-compliant manner?
- □ Does data transfer to third countries take place? If so:
  - □ Is the provider certified under the EU-US Data Privacy Framework?
  - □ If not: Have Standard Contractual Clauses (SCCs) been concluded and additional protective measures taken?
  - □ Optional: Is there a more privacy-friendly alternative with EU-based hosting?

10. Technical Data Protection Measures (TOMs)

- □ Is personal data protected through technical measures such as encryption and access controls?
- □ Is role-based permission assignment implemented in the system?
- □ Is data pseudonymized or anonymized where possible?
- □ Have all processes and systems been correctly recorded in the record of processing activities?