

(2026 Edition)

GDPR Compliance Checklist for Websites

1. Transparency & Privacy Notice (Articles 12–14)

- ☐ Publish a clear and accessible privacy policy
- ☐ Identify data controller contact details
- ☐ Specify lawful basis for each processing activity (Article 6)
- ☐ Disclose third-party recipients and subprocessors
- ☐ Explain international data transfers (Chapter V)
- ☐ State data retention periods

2. Lawful Basis Documentation (Article 6)

- ☐ Document lawful basis for all processing activities
- ☐ Conduct Legitimate Interest Assessments (if applicable)
- ☐ Avoid bundled or forced consent
- ☐ Maintain internal compliance records (Article 30)

3. Cookie & Tracking Compliance (ePrivacy + Article 7 GDPR)

- ☐ Implement prior script blocking for non-essential cookies
- ☐ Provide equal 'Accept' and 'Reject' options
- ☐ Log consent with timestamp and version
- ☐ Allow easy withdrawal of consent
- ☐ Avoid pre-ticked boxes or dark patterns

4. Data Subject Rights (Articles 15–22)

- ☐ Provide accessible request submission method
- ☐ Verify identity before fulfilling requests
- ☐ Respond within one month
- ☐ Implement erasure and data portability processes
- ☐ Document request handling

5. Vendor & Processor Management (Article 28)

- ☐ Execute Data Processing Agreements (DPAs)
- ☐ Conduct vendor due diligence
- ☐ Monitor subprocessors
- ☐ Maintain processor list

(2026 Edition)

GDPR Compliance Checklist for Websites

6. International Transfers (Chapter V)

- ☐ Identify cross-border data transfers
- ☐ Implement Standard Contractual Clauses (SCCs) where required
- ☐ Conduct Transfer Impact Assessments
- ☐ Update privacy notice accordingly

7. Security Measures (Article 32)

- ☐ Implement HTTPS encryption
- ☐ Restrict admin access
- ☐ Conduct regular vulnerability scans
- ☐ Maintain incident response plan
- ☐ Prepare 72-hour breach notification procedure (Articles 33–34)

8. Accountability & Governance (Article 5(2))

- ☐ Maintain Records of Processing Activities (Article 30)
- ☐ Conduct periodic GDPR audits
- ☐ Train employees on data protection
- ☐ Review policies annually