



# GDPR Compliance Master Checklist 2026

## (DPIA, Lawful Basis, Breach Notification, and Audit Readiness)

Data Protection & Privacy

# GDPR Compliance Services

Expert GDPR compliance services for EU data protection regulations. Comprehensive gap analysis, privacy policy development, DPO services, data subject rights management, and annual compliance audits. Achieve GDPR compliance and avoid €20M fines with our proven methodology.

**8 Principles**  
GDPR core requirements

**€20M**  
Maximum fine for non-compliance

**Common GDPR Compliance Gaps**

Gap	Percentage of organizations
Inadequate Consent Management	73% of organizations
Poor Data Subject Rights	68% of organizations
Insufficient Data Protection	62% of organizations
Lack of Privacy Notices	54% of organizations
Inadequate Documentation	47% of organizations
Missing DPO Appointment	35% of organizations

[Get Started](#) [Learn About GDPR](#)

This interactive GDPR Compliance Checklist consolidates DPIA, Lawful Basis, Breach Notification, and Audit Readiness requirements into a single working document. Use the checkboxes (□ / ✓) during audits, internal reviews, or regulatory preparation.

### A. Governance & Accountability

- DPO appointed where required and contact details published
- GDPR governance structure documented
- Privacy policy reviewed and updated in last 12 months
- Records of Processing Activities (RoPA) maintained and approved
- GDPR training delivered to all staff annually

### B. Data Inventory & Mapping

- Complete data inventory covering all systems and vendors
- Data categories and data subjects identified
- Retention periods documented per data category
- Cross-border data flows mapped
- Inventory reviewed and updated quarterly

### **C. Lawful Basis Assessment**

- Lawful basis identified for each processing activity
- Consent records stored and auditable
- Legitimate Interest Assessments completed where applicable
- Lawful basis aligned with privacy notices
- Review dates assigned for each lawful basis decision

### **D. DPIA (Data Protection Impact Assessment)**

- DPIA screening process in place
- DPIAs completed for high-risk processing
- Risks scored for likelihood and impact
- Mitigation measures documented and implemented
- DPO / Legal sign-off recorded

### **E. Data Subject Rights (DSARs)**

- DSAR intake mechanism available
- Identity verification process defined
- Response workflows documented
- DSARs completed within statutory deadlines
- DSAR log maintained

### **F. Security Measures**

- Access controls and role-based permissions enforced
- MFA enabled for privileged accounts
- Encryption applied to data at rest and in transit
- Vulnerability scans and penetration tests conducted
- Backup and recovery procedures tested

### **G. Personal Data Breaches**

- Incident response plan documented
- Breach detection and escalation procedures defined
- 72-hour notification workflow established
- Breach register maintained
- Post-incident reviews completed

### **H. Vendors & International Transfers**

- DPAs signed with all processors
- Subprocessors identified and approved
- SCCs or adequacy mechanisms in place
- Transfer risk assessments completed

- Vendor audits conducted periodically

## I. Monitoring & Audit Readiness

- Internal GDPR audits conducted annually
- Compliance KPIs defined and monitored
- Evidence repository maintained
- Regulatory guidance monitored
- Continuous improvement actions tracked

## About this document

This checklist is provided as a practical GDPR compliance support resource and reflects common regulatory expectations, industry best practices, and real-world implementation experience. It is intended to assist organizations in assessing and improving their data protection posture and should be used alongside legal advice tailored to the organization's specific circumstances.

Prepared by **SecurityWall** supporting startups and organizations in building practical, audit-ready GDPR compliance programs.



**GDPR  
ENFORCEMENT  
TRENDS IN 2026**

**GDPR Enforcement Trends in 2026**  
- Are You Ready?

As of late 2025, cumulative penalties under the EU's General Data Protection Regulation have exceeded €6.7 billion across more than 2,600 enforcement...

[Read Article →](#)