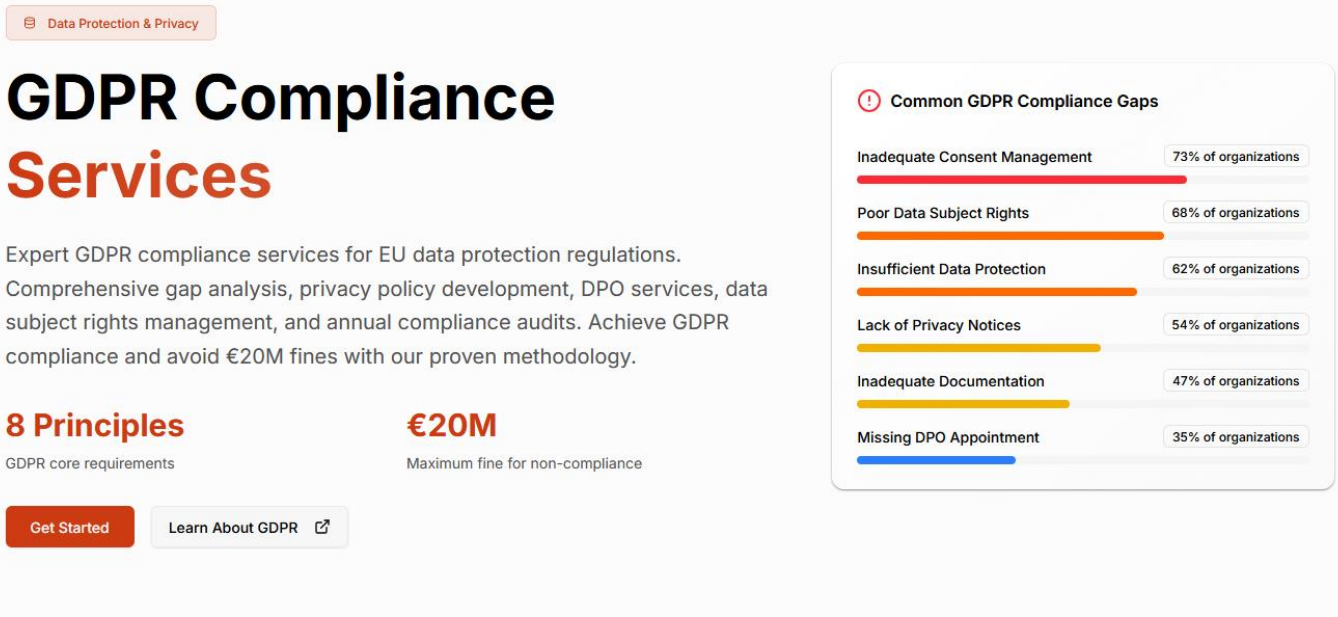
# GDPR Compliance Master Checklist 2026

## (Role-specific GDPR sub-checklists to support accountability, clear ownership, and effective cross-functional compliance)



# GDPR Role-Based Sub-Checklists – 2026

This document provides role-specific GDPR sub-checklists to support accountability, clear ownership, and effective cross-functional compliance. Each section is designed to be used independently or alongside the GDPR Compliance Master Checklist.

## 1. Legal & Compliance Team Checklist

- ☐ Determine GDPR applicability and territorial scope
- ☐ Identify controller / processor / joint controller roles
- ☐ Maintain Records of Processing Activities (RoPA)
- ☐ Define lawful basis for all processing activities
- ☐ Conduct and approve Legitimate Interest Assessments (LIAs)
- ☐ Review and approve DPIAs for high-risk processing
- ☐ Draft and update privacy notices and policies
- ☐ Oversee data subject rights handling and escalations
- ☐ Approve breach notifications to supervisory authorities
- ☐ Monitor regulatory guidance and enforcement actions

## 2. Information Security / IT Checklist

- ☐ Implement access controls and least-privilege principles
- ☐ Enforce MFA for privileged and remote access
- ☐ Apply encryption to personal data at rest and in transit
- ☐ Maintain logging, monitoring, and alerting systems
- ☐ Conduct vulnerability scans and penetration tests
- ☐ Maintain incident response and breach detection capabilities
- ☐ Support forensic investigations and evidence preservation
- ☐ Test backup, recovery, and business continuity plans
- ☐ Secure endpoints, cloud services, and APIs

## 3. Product / Engineering Checklist

- ☐ Apply privacy-by-design and privacy-by-default principles
- ☐ Minimize personal data collection in product features
- ☐ Ensure consent mechanisms are properly implemented
- ☐ Flag new features requiring DPIAs
- ☐ Document data flows and integrations
- ☐ Avoid hardcoding personal data in logs or test environments
- ☐ Support data subject rights within product functionality
- ☐ Review third-party SDKs and analytics tools
- ☐ Coordinate with Legal on AI, profiling, or monitoring features

## 4. Human Resources (HR) Checklist

- ☐ Maintain employee data inventories
- ☐ Define lawful basis for employee data processing
- ☐ Publish employee privacy notices
- ☐ Restrict access to HR systems and personnel files
- ☐ Define retention schedules for employee records
- ☐ Manage DSARs from employees and candidates
- ☐ Secure recruitment and background-check vendors
- ☐ Train staff on data protection obligations
- ☐ Handle employee data breaches appropriately

**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.