GDPR Compliance Checklist

50-Point Audit Framework for Data Protection

anonym.legal

Updated: February 2026

Executive Summary: GDPR in 2026

With **€4.7 billion in GDPR fines** issued to date—83% to US companies—systematic compliance isn't optional. This checklist covers every major GDPR requirement organized into actionable sections.

Key Statistics:
• €1.2 billion: Single largest GDPR fine (Meta, 2023)
• 72 hours: Maximum breach notification window
• 99 articles: Total GDPR provisions you must address
• 48 languages: Supported by anonym.legal for global compliance

Section 1: Legal Basis for Processing (6 items)

- ■ Documented lawful basis for each processing activity (Art. 6)
- ■ Special category data has explicit legal basis (Art. 9)
- ■ Processing purposes clearly defined and limited
- ■ Data minimization principle applied
- ■ Storage limitation periods defined
- ■ Regular lawful basis reviews scheduled

Section 2: Data Subject Rights (8 items)

- ■ Right of access process documented (Art. 15)
- ■ Right to rectification process (Art. 16)
- ■ Right to erasure ('right to be forgotten') (Art. 17)
- ■ Right to restriction of processing (Art. 18)
- ■ Right to data portability (Art. 20)
- ■ Right to object process (Art. 21)
- ■ Response within 30-day deadline ensured
- ■ Identity verification for requests

Section 3: Consent Management (5 items)

- ■ Consent is freely given, specific, informed, and unambiguous
- ■ Consent withdrawal is as easy as giving consent
- ■ Consent records maintained with timestamps
- ■ Separate consent for different processing purposes
- ■ Children's consent verified (under 16/13 depending on jurisdiction)

Section 4: Data Mapping & Records (6 items)

- ■ Records of Processing Activities (ROPA) maintained (Art. 30)
- ■ All data categories documented
- ■ Data flows mapped (internal and external)
- ■ Third-party processors identified
- ■ Data retention periods defined per category
- ■ Regular ROPA updates scheduled

Section 5: Privacy Notices & Transparency (4 items)

- ■ Privacy notice is clear, concise, and accessible
- ■ All required information included (Art. 13/14)
- ■ Notice provided at point of data collection
- ■ Notices updated when processing changes

Section 6: Data Protection Impact Assessments (4 items)

- ■ DPIA process established for high-risk processing (Art. 35)
- ■ Criteria for 'high risk' defined
- ■ DPO consulted on all DPIAs
- ■ Mitigation measures documented and implemented

Section 7: Cross-Border Transfers (5 items)

- ■ Transfer mechanisms identified (SCCs, adequacy, BCRs)
- ■ Transfer Impact Assessments completed post-Schrems II
- ■ Supplementary measures implemented where needed
- ■ No transfers to inadequate countries without safeguards
- ■ Regular transfer mechanism reviews

Section 8: Breach Notification (4 items)

Critical: You have only 72 hours to notify your supervisory authority of a breach.

- ■ Breach detection procedures in place
- ■ 72-hour notification process documented (Art. 33)
- ■ High-risk breach communication to individuals (Art. 34)
- ■ Breach register maintained

Section 9: Data Protection Officer (3 items)

- ■ DPO appointed if required (Art. 37)
- ■ DPO has adequate resources and independence
- ■ DPO contact published and notified to supervisory authority

Section 10: Vendor & Processor Management (5 items)

- ■ Data Processing Agreements (DPAs) with all processors
- ■ Processor due diligence conducted
- ■ Sub-processor approval process
- ■ Processor security measures verified
- ■ Regular processor audits scheduled

Section 11: Technical & Organizational Measures

Implement appropriate technical and organizational measures (Art. 32):

Encryption & Pseudonymization

- ■ Data encrypted at rest and in transit
- ■ Pseudonymization applied where appropriate
- ■ Encryption key management documented

Access Control

- ■ Role-based access control implemented
- ■ Principle of least privilege applied
- ■ Access regularly reviewed and revoked

Security Testing

- ■ Regular vulnerability assessments
- ■ Penetration testing scheduled
- ■ Security incident response tested

How anonym.legal Helps

anonym.legal provides technical measures to support your GDPR compliance:

- **260+ Entity Types**: Detect PII across all GDPR-relevant categories
- **48 Languages**: Process documents in any EU language
- **Reversible Encryption**: AES-256-GCM encryption with key management
- **Zero-Knowledge Auth**: We never see your encryption keys
- **German Data Residency**: 100% EU infrastructure, no US Cloud Act exposure
- **Chrome Extension**: Protect AI workflows from data leakage
- **MCP Server**: Integrate with Claude, Cursor, and other AI tools

Start your free trial at **https://anonym.legal**

Quick Reference: One-Page Summary

Requirement	Key Action	Deadline
Lawful Basis	Document legal basis for all processing	Ongoing
Data Subject Rights	Respond to requests	30 days
Breach Notification	Notify supervisory authority	72 hours
DPIA	Assess high-risk processing	Before processing
ROPA	Maintain processing records	Ongoing
DPO	Appoint if required	Before processing
Privacy Notice	Inform at collection	At collection
Transfers	Implement safeguards	Before transfer
Security	Technical measures	Ongoing
Processors	Execute DPAs	Before engagement