GDPR Cybersecurity Checklist for 2026

Use this checklist to assess your organization's GDPR cybersecurity posture across data protection, technical controls, testing, and response readiness.

Data Protection Foundations

- [ ] Completed data mapping to identify all personal data processing activities
- [ ] Documented lawful basis for each processing activity
- [ ] Appointed Data Protection Officer (if required)
- [ ] Established data retention policies and deletion procedures

Technical Security Measures

- [ ] Implemented encryption for data at rest and in transit
- [ ] Deployed access controls based on least-privilege principles
- [ ] Configured network security controls (firewalls, segmentation)
- [ ] Enabled logging and monitoring for systems processing personal data
- [ ] Secured endpoints with anti-malware and patch management

Testing and Assessment

- [ ] Conducted annual penetration testing of systems processing personal data
- [ ] Performed vulnerability assessments with validated remediation
- [ ] Completed Data Protection Impact Assessments for high-risk processing
- [ ] Documented test results and remediation actions for audit evidence

Incident Response and Recovery

- [ ] Developed breach notification procedures (72-hour timeline)
- [ ] Tested incident response plan through tabletop exercises
- [ ] Implemented backup and recovery procedures for personal data
- [ ] Established communication templates for data subjects and authorities

Third-Party Management

- [ ] Executed Data Processing Agreements with all processors
- [ ] Conducted security due diligence on third-party vendors
- [ ] Verified sub-processor compliance with GDPR requirements

Training and Awareness

- [ ] Provided GDPR awareness training to all employees
- [ ] Conducted phishing simulations and security awareness exercises
- [ ] Trained staff on data subject rights and request handling