Enterprise Compliance Checklist

NeuroCluster Enterprise AI Platform

December 13, 2025

NeuroCluster Enterprise Compliance Checklist

Security, Privacy & Regulatory Compliance

Version: 1.0 **Date:** December 13, 2025 **Purpose:** Pre-deployment compliance validation checklist **Target Audience:** Compliance Officers, Security Teams, Deployment Engineers

---

How to Use This Checklist

This checklist is designed for organizations deploying NeuroCluster in regulated environments. Use it to:

- **Pre-Deployment:** Verify all requirements before go-live
- **Audit Preparation:** Document compliance posture for auditors
- **Continuous Compliance:** Quarterly compliance reviews
- **Customer Assurance:** Demonstrate compliance to enterprise customers

Legend:

- ✅ **Compliant** - Requirement fully met with evidence
- ⚠️ **Partial** - Requirement partially met, action required
- ❌ **Non-Compliant** - Requirement not met, immediate action required
- N/A **Not Applicable** - Requirement doesn't apply to deployment

---

Table of Contents

Infrastructure Security

Kubernetes Security

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | IS-1 | Pod Security Standards enforced (Restricted PSS) | □ | PSP YAML file | Prevent privileged containers | | IS-2 | Network policies configured (default deny) | □ | NetworkPolicy resources | Namespace isolation | | IS-3 | RBAC configured with least privilege | □ | Role/RoleBinding audit | No cluster-admin for apps | | IS-4 | Resource limits set for all pods | □ | Pod spec review | CPU/memory limits | | IS-5 | Read-only root filesystem where possible | □ | Pod spec review | Reduce attack surface | | IS-6 | Non-root user enforcement | □ | SecurityContext config | UID > 1000 | | IS-7 | Pod Disruption Budgets configured | □ | PDB resources | High availability | | IS-8 | Admission controllers enabled | □ | API server config | OPA/Gatekeeper |

Container Security

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | CS-1 | Container images scanned for vulnerabilities | □ | Trivy/Snyk reports | CI/CD integration | | CS-2 | Only official/trusted base images used | □ | Dockerfile review | Alpine, Distroless | | CS-3 | Container images signed | □ | Cosign signatures | Supply chain security | | CS-4 | Private container registry with RBAC | □ | Harbor configuration | Access control | | CS-5 | No secrets in container images | □ | Image audit | Use Vault/env vars | | CS-6 | Container runtime security (Falco) | □ | Falco rules | Runtime threat detection | | CS-7 | Image pull

policy: Always | □ | Pod spec review | Force latest security patches | | CS-8 | Regular base image updates (monthly) | □ | Update schedule | Security patches |

Secrets Management

| # | Requirement | Status | Evidence | Notes | |---|------------|--------|----------|-------| | SM-1 | HashiCorp Vault deployed and configured | □ | Vault status | Central secrets storage | | SM-2 | Vault auto-unseal configured | □ | Vault config | No manual unsealing | | SM-3 | Dynamic secrets for databases | □ | Vault policy | Short-lived credentials | | SM-4 | Secret rotation policy (90 days) | □ | Rotation schedule | Automated rotation | | SM-5 | No secrets in Git/ConfigMaps/env vars | □ | Codebase audit | Vault agent injection | | SM-6 | Vault audit logging enabled | □ | Vault audit config | Secret access logs | | SM-7 | Encryption at rest for Vault | □ | Vault encryption | AES-256-GCM | | SM-8 | Backup and recovery tested | □ | DR test results | Quarterly testing |

Application Security

Secure Development

| # | Requirement | Status | Evidence | Notes | |---|------------|--------|----------|-------| | SD-1 | Mandatory code review for all changes | □ | Git branch policy | 2 approvers required | | SD-2 | SAST integrated in CI/CD | □ | SonarQube config | Automated security scanning | | SD-3 | Dependency vulnerability scanning | □ | Snyk/Dependabot | Daily scans | | SD-4 | Security training for developers | □ | Training records | Annual OWASP Top 10 | | SD-5 | Secure coding guidelines documented | □ | Wiki/Confluence | Language-specific guides | | SD-6 | Threat modeling for new features | □ | Threat models | STRIDE methodology | | SD-7 | Security champions program | □ | Team roster | 1 per team | | SD-8 | Bug bounty program active | □ | HackerOne/Bugcrowd | Public disclosure |

Input Validation

| # | Requirement | Status | Evidence | Notes | |---|------------|--------|----------|-------| | IV-1 | All API inputs validated with Pydantic | □ | Code review | Type checking | | IV-2 | SQL injection prevention (parameterized queries) | □ | Code audit | No dynamic SQL | | IV-3 | XSS prevention (output encoding) | □ | Security scan | DOMPurify, CSP headers | | IV-4 | CSRF protection enabled | □ | Security scan | CSRF tokens | | IV-5 | File upload validation (type, size) | □ | Code review | Antivirus scanning | | IV-6 | Rate limiting on all endpoints | □ | Kong config | Per-user, per-IP | | IV-7 | Request size limits enforced | □ | Gateway config | 10MB max | | IV-8 | Regex DoS prevention | □ | Code review | Safe regex patterns |

API Security

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | AS-1 | JWT authentication with short expiry | □ | Auth config | 1 hour max | | AS-2 | API gateway (Kong) deployed | □ | Kong status | Central auth point | | AS-3 | TLS 1.3 enforced for all APIs | □ | Nginx/Kong config | No TLS 1.0/1.1 | | AS-4 | CORS configured securely | □ | Middleware config | Specific origins only | | AS-5 | API versioning implemented | □ | Route config | v1, v2 versioning | | AS-6 | OpenAPI spec available | □ | Swagger UI | Auto-generated docs | | AS-7 | API authentication logged | □ | Audit logs | All auth attempts | | AS-8 | API key rotation capability | □ | Key mgmt API | Customer self-service |

Data Protection & Privacy

Encryption

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | EN-1 | Encryption at rest (AES-256) | □ | Database config | PostgreSQL TDE | | EN-2 | Encryption in transit (TLS 1.3) | □ | Nginx config | All connections | | EN-3 | mTLS between services | □ | Linkerd config | Service mesh | | EN-4 | Certificate auto-renewal | □ | cert-manager config | Let's Encrypt | | EN-5 | HSTS header enabled | □ | HTTP headers | 1 year max-age | | EN-6 | Strong cipher suites only | □ | TLS config | ECDHE-RSA-AES256-GCM | | EN-7 | Key management via Vault | □ | Vault integration | Centralized KMS | | EN-8 | Backup encryption | □ | Backup config | Encrypted backups |

Data Minimization & Retention

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | DR-1 | Data retention policy documented | □ | Policy document | 30d logs, 7y audit | | DR-2 | Automatic data deletion implemented | □ | Cron jobs/scripts | Retention enforcement | | DR-3 | PII redaction in logs | □ | Logger config | Auto-redact emails, SSN | | DR-4 | Data minimization principle followed | □ | Data audit | Collect only necessary | | DR-5 | Pseudonymization for analytics | □ | Analytics config | De-identified data | | DR-6 | Data classification tags | □ | Data catalog | Public/Internal/Confidential | | DR-7 | Secure data disposal procedure | □ | SOP document | Crypto-shredding | | DR-8 | Right to erasure implemented | □ | Deletion API | GDPR Article 17 |

Data Residency

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | DR-9 | Data residency option configured | □ | Region config | EU/US/UK/on-prem | | DR-10 | No

cross-border transfers without consent | □ | Data flow map | DPA controls | | DR-11 | Standard Contractual Clauses in place | □ | DPA signed | EU-US transfers | | DR-12 | Data Processing Agreement available | □ | DPA template | Customer contracts | | DR-13 | Sub-processor list published | □ | Trust Center page | AWS, Supabase, etc. | | DR-14 | Data localization for EU customers | □ | Infrastructure audit | Frankfurt/Amsterdam | | DR-15 | UK GDPR compliance (post-Brexit) | □ | UK Addendum | Standard clauses | | DR-16 | Data transfer impact assessment | □ | DTIA document | Schrems II |

Identity & Access Management

Authentication

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | IA-1 | Multi-factor authentication enforced | □ | Auth config | Admin roles mandatory | | IA-2 | SSO integration (SAML/OIDC) | □ | Keycloak config | Azure AD, Google | | IA-3 | Password policy enforced | □ | Auth config | 12 chars, complexity | | IA-4 | Account lockout after failed attempts | □ | Auth config | 5 attempts, 15min lock | | IA-5 | Session timeout configured | □ | Auth config | 12 hours idle | | IA-6 | Secure session management | □ | Cookie audit | HttpOnly, Secure, SameSite | | IA-7 | Password reset via email only | □ | Auth flow | No SMS reset | | IA-8 | Concurrent session limits | □ | Auth config | Max 5 per user |

Authorization

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | AZ-1 | RBAC implemented | □ | Role definitions | 5 standard roles | | AZ-2 | Principle of least privilege | □ | Access review | Minimal permissions | | AZ-3 | Default deny policy | □ | Policy config | Explicit grants | | AZ-4 | Separation of duties | □ | Role matrix | Admin ≠ Auditor | | AZ-5 | Quarterly access reviews | □ | Review schedule | Document results | | AZ-6 | Automated de-provisioning | □ | SCIM config | On termination | | AZ-7 | Group-based access control | □ | Group mapping | SSO group sync | | AZ-8 | Privileged access monitoring | □ | Audit logs | Admin actions logged |

Document-Level Access Control

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | AC-1 | ACL sync from source systems | □ | Connector config | M365, Google | | AC-2 | Permission-aware RAG retrieval | □ | RAG config | User-scoped results | | AC-3 | User and group permissions supported | □ | ACL service | Both enforced | | AC-4 | Permission cache with TTL | □ | Redis config | 1 hour TTL | | AC-5 | Permission audit trail | □ | ACL logs | All access logged | | AC-6 | Inheritance from source system | □ | ACL sync | Preserves source

ACL | | AC-7 | Real-time permission sync | □ | Webhook config | Delta API | | AC-8 | Permission denial logged | □ | Audit logs | Unauthorized attempts |

Logging & Monitoring

Audit Logging

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | AL-1 | Comprehensive audit logging enabled | □ | backend_logs table | All events logged | | AL-2 | Authentication events logged | □ | Auth logs | Success/failure | | AL-3 | Authorization decisions logged | □ | AuthZ logs | Allow/deny logged | | AL-4 | Data access logged | □ | Access logs | CRUD operations | | AL-5 | Admin actions logged | □ | Admin logs | User mgmt, config changes | | AL-6 | Log integrity protected | □ | Immutable logs | Append-only | | AL-7 | Log retention: 7 years | □ | Retention policy | Archive to S3 Glacier | | AL-8 | Logs exported to SIEM | □ | SIEM integration | Splunk/ELK |

Security Monitoring

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | SM-1 | Intrusion detection system (Falco) | □ | Falco rules | Runtime detection | | SM-2 | Vulnerability scanning (weekly) | □ | Scan reports | Nessus/Qualys | | SM-3 | File integrity monitoring | □ | FIM config | AIDE/Tripwire | | SM-4 | Anomaly detection enabled | □ | ML models | Behavioral analysis | | SM-5 | Security alerts to SOC | □ | Alert config | Slack/PagerDuty | | SM-6 | Security dashboard | □ | Grafana dashboards | Real-time visibility | | SM-7 | Threat intelligence integration | □ | TI feeds | MISP/STIX | | SM-8 | Security event correlation | □ | SIEM rules | Pattern detection |

Application Monitoring

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | AM-1 | Application performance monitoring | □ | APM config | New Relic/Datadog | | AM-2 | Error tracking (Sentry) | □ | Sentry config | Exception monitoring | | AM-3 | LLM tracing (Langfuse) | □ | Langfuse config | Token/cost tracking | | AM-4 | Metrics collection (Prometheus) | □ | Prometheus config | System metrics | | AM-5 | Distributed tracing (Jaeger) | □ | Tracing config | Request tracing | | AM-6 | Uptime monitoring | □ | Pingdom/UptimeRobot | External monitoring | | AM-7 | Synthetic monitoring | □ | Test scripts | End-to-end tests | | AM-8 | SLA dashboards | □ | Grafana dashboards | 99.9% uptime target |

Incident Response

Incident Response Plan

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | IR-1 | Incident response plan documented | □ | IRP document | Phases, roles, contacts | | IR-2 | Incident classification defined | □ | IRP appendix | P1-P4 severity | | IR-3 | On-call rotation established | □ | PagerDuty schedule | 24/7 coverage | | IR-4 | Incident response playbooks | □ | Runbooks | Common scenarios | | IR-5 | Security incident drill (annual) | □ | Drill report | Tabletop exercise | | IR-6 | Incident communication plan | □ | Comm template | Internal/external | | IR-7 | Post-incident review process | □ | PIR template | Lessons learned | | IR-8 | Root cause analysis required | □ | RCA template | 5 Whys, fishbone |

Data Breach Response

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | BR-1 | Data breach response plan | □ | Breach plan | GDPR 72-hour rule | | BR-2 | DPO contact defined | □ | Contact list | dpo@neurocluster.ai | | BR-3 | Breach notification templates | □ | Email templates | Pre-approved legal | | BR-4 | Regulatory notification process | □ | Escalation path | DPA, ICO, etc. | | BR-5 | Breach register maintained | □ | Breach log | All incidents logged | | BR-6 | Customer notification SLA | □ | Comm plan | Within 72 hours | | BR-7 | Breach forensics capability | □ | Forensics tools | Preserve evidence | | BR-8 | Cyber insurance in place | □ | Insurance policy | $10M coverage |

Business Continuity

Backup & Recovery

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | BC-1 | Daily automated backups | □ | Backup schedule | Database, configs | | BC-2 | Backup encryption enabled | □ | Backup config | AES-256 | | BC-3 | Offsite backup storage | □ | S3 Glacier config | Geographic separation | | BC-4 | Backup restoration tested (quarterly) | □ | Test reports | RTO/RPO validated | | BC-5 | Point-in-time recovery (24 hours) | □ | Backup config | PITR capability | | BC-6 | Backup retention: 30 days | □ | Retention policy | Compliance requirement | | BC-7 | Disaster recovery plan documented | □ | DR plan | Procedures, contacts | | BC-8 | DR site/region configured | □ | Infrastructure | Multi-region |

High Availability

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | HA-1 | Multi-replica deployment | □ | K8s config | Min 2 replicas | | HA-2 | Load balancing configured | □ | Ingress config | Round-robin | | HA-3 | Health checks enabled | □ | Liveness/readiness | Auto-restart | | HA-4 | Database replication | □ | PostgreSQL config | Master-replica | | HA-5 | Redis clustering | □ | Redis config | High availability | | HA-6 | Geographic redundancy | □ | Multi-region | Active-passive | | HA-7 | Failover testing (annual) | □ | Failover test | Documented results | | HA-8 | SLA target: 99.9% uptime | □ | Uptime reports | Monthly tracking |

Compliance Frameworks

SOC 2 Type II

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | SOC-1 | Security policies documented | □ | Policy docs | ISMS policies | | SOC-2 | Risk assessment completed | □ | Risk register | Annual update | | SOC-3 | Vendor risk management | □ | Vendor assessments | Sub-processors | | SOC-4 | Background checks for employees | □ | HR records | Pre-employment | | SOC-5 | Security awareness training | □ | Training records | Annual | | SOC-6 | Change management process | □ | Change tickets | Approval workflow | | SOC-7 | Incident management process | □ | Incident tickets | Tracking system | | SOC-8 | Business continuity plan | □ | BCP document | Tested annually | | SOC-9 | Logical access controls | □ | Access reviews | Quarterly | | SOC-10 | Monitoring and logging | □ | SIEM logs | Centralized |

ISO 27001

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | ISO-1 | ISMS policy approved | □ | ISMS policy | Management signature | | ISO-2 | Asset inventory maintained | □ | CMDB | All IT assets | | ISO-3 | Risk treatment plan | □ | Risk register | Mitigation plans | | ISO-4 | Statement of Applicability | □ | SoA document | 93 controls | | ISO-5 | Information security objectives | □ | Objectives doc | Measurable goals | | ISO-6 | Internal audit program | □ | Audit schedule | Quarterly | | ISO-7 | Management review meetings | □ | Meeting minutes | Quarterly | | ISO-8 | Corrective action process | □ | CAR register | Track to closure | | ISO-9 | Continual improvement process | □ | Improvement log | PDCA cycle | | ISO-10 | Competence and awareness | □ | Training matrix | Role-based |

GDPR

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | GDPR-1 | DPA available for customers | □ | DPA template | Downloadable | | GDPR-2 | Privacy policy published | □ | Privacy page | Plain language | | GDPR-3 | Cookie consent management | □ | Cookie banner | Granular consent | | GDPR-4 | Data subject rights implemented | □ | User portal | Self-service | | GDPR-5 | Data processing records (ROPA) | □ | ROPA document | Article 30 | | GDPR-6 | Data protection impact assessment | □ | DPIA | High-risk processing | | GDPR-7 | Data breach notification procedure | □ | Breach plan | 72-hour SLA | | GDPR-8 | DPO appointed | □ | DPO contact | Dr. Elena Vermeer | | GDPR-9 | Privacy by design implemented | □ | Architecture docs | Article 25 | | GDPR-10 | International data transfer safeguards | □ | SCCs | EU-US transfers |

EU AI Act

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | AI-1 | AI system classification | □ | Classification doc | Limited risk GPAI | | AI-2 | Transparency obligations met | □ | AI disclosure | User notification | | AI-3 | Technical documentation | □ | Model cards | Architecture, data | | AI-4 | Risk assessment conducted | □ | Risk assessment | High-risk use cases | | AI-5 | Human oversight mechanisms | □ | Oversight controls | Human-in-loop | | AI-6 | Quality management system | □ | QMS docs | ISO 9001-aligned | | AI-7 | Training data documentation | □ | Data cards | Public summary | | AI-8 | Safeguards against illegal content | □ | Content filters | Harmful content | | AI-9 | Energy efficiency reporting | □ | Energy metrics | Carbon footprint | | AI-10 | Conformity assessment | □ | Assessment report | Third-party audit |

Third-Party Risk

Vendor Management

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | VM-1 | Vendor risk assessment process | □ | Assessment template | Security questionnaire | | VM-2 | All vendors assessed | □ | Vendor register | AWS, Supabase, etc. | | VM-3 | DPA with all sub-processors | □ | Signed DPAs | On file | | VM-4 | SOC 2 reports from vendors | □ | SOC reports | Annual review | | VM-5 | Vendor monitoring (annual) | □ | Review schedule | Ongoing assessment | | VM-6 | Vendor offboarding procedure | □ | Offboarding SOP | Data deletion | | VM-7 | Fourth-party risk considered | □ | 4th party list | Vendor's vendors | | VM-8 | Critical vendor backup plan | □ | Vendor BCP | Alternative suppliers |

Documentation & Training

Documentation

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | DOC-1 | Security policies documented | □ | Policy library | ISMS policies | | DOC-2 | Standard operating procedures | □ | SOP library | Operational runbooks | | DOC-3 | Architecture diagrams | □ | Diagrams | Network, data flow | | DOC-4 | Disaster recovery runbooks | □ | DR runbooks | Step-by-step | | DOC-5 | User guides and training materials | □ | Documentation site | Self-service | | DOC-6 | API documentation | □ | OpenAPI specs | Swagger UI | | DOC-7 | Change log maintained | □ | CHANGELOG.md | Version history | | DOC-8 | Security whitepaper published | □ | Whitepaper PDF | Public/customer |

Training

| # | Requirement | Status | Evidence | Notes | |---|---|---|---|---| | TR-1 | Security awareness training | □ | Training records | Annual, all staff | | TR-2 | Role-specific training | □ | Training matrix | Engineers, support | | TR-3 | Phishing simulation exercises | □ | Simulation results | Monthly | | TR-4 | Secure coding training | □ | Training records | Developers | | TR-5 | Incident response training | □ | Drill records | Annual tabletop | | TR-6 | Privacy training (GDPR) | □ | Training records | Data handlers | | TR-7 | Training completion tracking | □ | LMS reports | 100% completion | | TR-8 | Training effectiveness measurement | □ | Assessment scores | >80% pass rate |

Compliance Summary

Pre-Deployment Checklist

Before deploying NeuroCluster to production, ensure:

- [ ] All **Infrastructure Security** items marked ✅
- [ ] All **Application Security** items marked ✅
- [ ] All **Data Protection** items marked ✅
- [ ] All **IAM** items marked ✅
- [ ] All **Logging** items marked ✅
- [ ] **Incident Response** plan tested
- [ ] **Business Continuity** plan tested

- [ ] Relevant **Compliance Framework** items completed
- [ ] **Vendor assessments** current
- [ ] **Documentation** complete and published
- [ ] **Training** records up-to-date

Quarterly Review Checklist

Every quarter, review and update:

- [ ] Access reviews completed
- [ ] Vendor assessments current
- [ ] Backup restoration tested
- [ ] Vulnerability scans reviewed
- [ ] Incident log reviewed
- [ ] Policy updates (if applicable)
- [ ] Training completion verified
- [ ] Risk register updated

Annual Review Checklist

Every year, complete:

- [ ] Third-party penetration test
- [ ] Disaster recovery drill
- [ ] Security awareness training
- [ ] Policy and procedure review
- [ ] Compliance framework audit
- [ ] Vendor contract renewals
- [ ] Insurance policy review
- [ ] Business continuity plan test

Compliance Attestation

Deployment Certification

I certify that the NeuroCluster deployment described below meets all applicable compliance requirements listed in this checklist.

Deployment Details:

- **Environment:** □ Production □ Staging □ Development
- **Deployment Type:** □ SaaS □ VPC □ On-Premise □ Air-Gapped
- **Data Residency:** □ EU □ US □ UK □ Other: _____
- **Compliance Frameworks:** □ SOC 2 □ ISO 27001 □ GDPR □ HIPAA □ Other: _____

Compliance Officer:

- Name: _____
- Title: _____
- Signature: _____
- Date: _____

Security Officer:

- Name: _____
- Title: _____
- Signature: _____
- Date: _____

Appendix: Evidence Requirements

Documentation to Maintain

- [ ] Security Policy Suite (10+ policies)
- [ ] Risk Register (updated quarterly)
- [ ] Vendor Assessment Reports
- [ ] Penetration Test Reports (annual)
- [ ] Incident Response Logs
- [ ] Change Management Tickets
- [ ] Access Review Reports (quarterly)
- [ ] Training Completion Records
- [ ] Backup Test Results (quarterly)
- [ ] DR Drill Reports (annual)

Audit Artifacts

For compliance audits, prepare:

- [ ] System architecture diagrams
- [ ] Data flow diagrams
- [ ] Network diagrams
- [ ] Access control matrix
- [ ] Encryption inventory
- [ ] Asset inventory (CMDB)
- [ ] Patch management logs
- [ ] Vulnerability scan reports
- [ ] SIEM alert reports
- [ ] Incident postmortems

Support & Resources

Compliance Support:

- Email: compliance@neurocluster.ai
- Documentation: https://docs.neurocluster.com/compliance
- Trust Center: https://neurocluster.ai/trust

Security Support:

- Email: security@neurocluster.ai
- Phone: +31 20 123 4569 (24/7 SOC)

Professional Services:

- Compliance consulting available
- Audit preparation assistance
- Custom compliance reporting
- Contact: sales@neurocluster.ai

Checklist Version: 1.0 **Last Updated:** December 13, 2025 **Next Review:** March 13, 2026

Prepared By: NeuroCluster Compliance Team **Approved By:** Dr. Elena Vermeer, Data Protection Officer

---

This checklist is provided as a guide and does not constitute legal advice. Organizations should consult with legal counsel and compliance experts to ensure full compliance with applicable laws and regulations.
