



JOB DESCRIPTION TEMPLATE

AI Privacy & Compliance Analyst

The analyst who reviews how AI systems use personal data and tests them against privacy law and compliance obligations across the lifecycle.

Department	Privacy / Compliance / AI Governance
Reports to	Chief Privacy Officer / Privacy & Compliance Director
Location	Remote / Hybrid / On-site
Employment type	Full-time
Experience	3 to 6+ years

POSITION OVERVIEW

The AI Privacy and Compliance Analyst evaluates how the organization's AI systems use personal data and whether they meet privacy and compliance requirements. This role reviews AI use cases for data protection risk and supports compliance across the AI lifecycle.

Working with privacy, legal, governance, security, and data science teams, the analyst conducts privacy reviews and impact assessments, tests compliance with applicable requirements, and helps embed privacy-by-design into AI development.

As AI systems consume more personal data, the AI Privacy and Compliance Analyst helps the organization innovate while protecting individuals and meeting its obligations.

KEY RESPONSIBILITIES

AI PRIVACY REVIEW

- Review AI use cases for personal data use and privacy risk.
- Support data protection impact assessments for higher-risk AI.
- Evaluate lawful basis, purpose, and data minimization.
- Advise on transparency, notice, and individual rights.

COMPLIANCE TESTING

Test AI systems and processes against privacy and compliance requirements, including:

- Consent, notice, and individual rights handling
- Data retention, minimization, and deletion
- Cross-border transfer and vendor obligations
- Documentation and record-keeping requirements

REGULATORY MAPPING

Map obligations from data protection law, the EU AI Act, and the NIST AI Risk Management Framework to internal privacy and AI controls, and track changes over time.

PRIVACY-BY-DESIGN SUPPORT

- Advise teams on privacy-preserving AI design choices.
- Support data-minimization and de-identification approaches.
- Help embed privacy controls into AI pipelines.
- Review third-party AI tools for privacy compliance.

DOCUMENTATION AND EVIDENCE

- Maintain privacy assessments, records, and control evidence.
- Support audit and regulatory readiness for AI systems.
- Track remediation of identified privacy findings.

MONITORING AND AWARENESS

Monitor AI systems for privacy issues and build awareness so teams handle personal data responsibly in AI projects.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Information Systems, Law, Data Science, Business, or a related discipline.

- 3 to 6+ years of experience in privacy, data protection, compliance, or a related field, including exposure to AI or data-intensive systems.
- Working knowledge of privacy principles, data protection law, and compliance methods.
- Familiarity with AI and machine learning concepts and their privacy implications.
- Strong analytical, documentation, and communication skills.

PREFERRED CERTIFICATIONS

One or more of: CIPP, CIPT, AIGP, CDPSE.

TECHNICAL KNOWLEDGE

AI privacy reviews, data protection impact assessments, privacy compliance testing, data minimization and de-identification, lawful basis and rights handling, regulatory mapping, third-party privacy review, and AI governance fundamentals.

ESSENTIAL COMPETENCIES

Analytical rigor, attention to detail, clear communication of privacy requirements, collaboration with technical teams, and practical problem solving.

This is a free, editable template. Replace bracketed fields with your specifics before posting.

Post this role, or find more templates, at ai-governance-jobs.com/templates/ai-privacy-and-compliance-analyst · A resource from **GRC Careers**