

JOB DESCRIPTION TEMPLATE

Privacy Analyst

is hiring a Privacy Analyst to help operate and improve our privacy program. The analyst will support privacy assessments, data inventories, individual-rights requests, vendor reviews, incident response and compliance reporting across .

Department	Privacy / Legal / Compliance / Risk
Reports to	Privacy Program Manager / Director of Privacy / Chief Privacy Officer
Location	Remote / Hybrid / On-site and location
Employment type	Full-time / Part-time / Contract

POSITION OVERVIEW

the organization is hiring a Privacy Analyst to help operate and improve our privacy program. The analyst will support privacy assessments, data inventories, individual-rights requests, vendor reviews, incident response and compliance reporting across the organization.

Working with Legal, Security, Product, Data, Procurement and business teams, you will gather facts, identify privacy risks, document decisions and help track issues through resolution. This role is well suited to someone who combines careful analysis with practical follow-through.

KEY RESPONSIBILITIES

KEY RESPONSIBILITIES

- Conduct or support privacy impact assessments and data protection impact assessments.
- Maintain data inventories, records of processing and data-flow documentation.
- Coordinate access, deletion, correction, opt-out and other individual-rights requests.
- Support privacy reviews of vendors, contracts, products and new data uses.
- Track privacy issues, incidents, remediation actions and control evidence.
- Research regulatory requirements and prepare concise internal guidance.
- Maintain procedures, templates, training materials and program records.
- Prepare metrics and reports on workload, deadlines, risk and remediation.
- Partner with Legal, Security, Data, Product, Marketing, HR and Procurement.

REQUIRED QUALIFICATIONS

- years of relevant experience in privacy, compliance, audit, legal operations, data governance, security, risk or a related function. For a genuinely junior role, accept internships, substantial project work or equivalent experience.
- Working knowledge of privacy principles and at least one relevant legal framework.
- Ability to gather facts, analyze requirements and produce clear documentation.
- Strong organization, judgment and communication skills.
- Ability to manage several deadlines and escalate material concerns.

PREFERRED CERTIFICATIONS

Experience with privacy assessments, rights requests, data mapping or vendor review.; Familiarity with [GDPR / CCPA and CPRA / HIPAA / sector rules].; CIPP, CIPM or progress toward a relevant credential.; Experience with [privacy-management, ticketing, data-discovery or reporting tools].; Exposure to product development, cloud services, analytics or AI governance.

TECHNICAL KNOWLEDGE

GDPR, CCPA / CPRA, HIPAA, ISO/IEC 27701, privacy impact assessments, data mapping, records of processing.

ESSENTIAL COMPETENCIES

Analysis, documentation, judgment, cross-functional collaboration, and clear communication of privacy risk.

SUCCESS IN THE FIRST YEAR

- Core privacy workflows are completed accurately and on time.

- Data and processing records become more complete and useful.
- Assessments identify material risk early enough to influence decisions.
- Issues and remediation have clear owners, deadlines and evidence.
- Business partners receive practical, consistent guidance.

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/privacy-analyst-job-description · A resource from **GRC Careers**