

JOB DESCRIPTION TEMPLATE

Privacy Engineer

is hiring a Privacy Engineer to build privacy into products, services, data pipelines and AI systems. You will translate privacy requirements into technical requirements, architecture and controls, then help teams validate that those controls work across the data life cycle.

Department	Engineering / Privacy / Security / Data
Reports to	Director of Privacy Engineering / Chief Privacy Officer / Security or Engineering leader
Location	Remote / Hybrid / On-site and location
Employment type	Full-time

POSITION OVERVIEW

the organization is hiring a Privacy Engineer to build privacy into products, services, data pipelines and AI systems. You will translate privacy requirements into technical requirements, architecture and controls, then help teams validate that those controls work across the data life cycle.

This role partners with Software Engineering, Data, Security, Product, Legal and Privacy. The successful candidate will combine systems thinking with practical knowledge of privacy principles and technology.

KEY RESPONSIBILITIES

KEY RESPONSIBILITIES

- Translate privacy obligations and policy into technical requirements and acceptance criteria.
- Map personal-data flows, stores, interfaces, purposes, recipients and retention.
- Design or implement minimization, access, retention, deletion and audit controls.
- Build or improve consent, preference and individual-rights capabilities.
- Apply de-identification, pseudonymization or privacy-enhancing techniques where appropriate.
- Review product, analytics, vendor and AI designs for privacy risk.
- Automate data discovery, classification, control evidence or compliance workflows.
- Develop reusable privacy design patterns, libraries and engineering guidance.
- Partner with Security on encryption, identity, incidents, logging and threat modeling.
- Test controls and track technical remediation to completion.

REQUIRED QUALIFICATIONS

- years in software, data, security, cloud, architecture or privacy engineering.
- Hands-on experience with .
- Understanding of data life cycles, APIs, databases, identity, access and distributed systems.
- Ability to translate a policy or risk statement into a technical design.
- Working knowledge of privacy by design, minimization, retention, individual rights and de-identification.
- Clear communication across technical and non-technical teams.

PREFERRED CERTIFICATIONS

Experience shipping privacy controls in production.; CIPT, CDPSE, CIPP or related credential.; Experience with privacy-enhancing technologies or privacy-preserving analytics.; Experience with machine learning, AI data governance or model pipelines.; Familiarity with [GDPR / CCPA and CPRA / applicable sector rules].

TECHNICAL KNOWLEDGE

GDPR, CCPA / CPRA, ISO/IEC 27701, NIST Privacy Framework, 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

- Teams have reusable privacy patterns rather than starting each review from zero.

- High-risk data flows are documented and receive technical controls.
- Deletion, preference and access requirements work across downstream systems.
- Privacy findings have clear engineering owners and verifiable closure.
- Product teams involve Privacy Engineering early enough to influence design.

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-engineer-job-description · A resource from **GRC Careers**