

JOB DESCRIPTION TEMPLATE

Chief Privacy Officer

is hiring a Chief Privacy Officer to set and lead our enterprise privacy strategy. The CPO will establish how the organization governs personal data across products, operations, workforce systems, vendors, analytics and artificial intelligence.

Reports to	CEO / General Counsel / Chief Risk Officer / other executive
Location	Remote / Hybrid / On-site and location
Employment type	Full-time

POSITION OVERVIEW

the organization is hiring a Chief Privacy Officer to set and lead our enterprise privacy strategy. The CPO will establish how the organization governs personal data across products, operations, workforce systems, vendors, analytics and artificial intelligence.

As the senior privacy executive, the CPO will advise leadership and the board, lead the privacy organization and align Legal, Security, Data, Product, Engineering, HR, Marketing, Procurement, Audit and AI Governance around clear accountability. The position requires deep privacy judgment and the ability to build an effective, appropriately resourced program.

KEY RESPONSIBILITIES

KEY RESPONSIBILITIES

- Set enterprise privacy strategy, governance, risk appetite and priorities.
- Maintain the privacy framework, policies, controls and operating model.
- Lead regulatory readiness across .
- Oversee product privacy, assessments, rights, data inventories, vendors and incident coordination.
- Sponsor privacy engineering and privacy-enhancing capabilities.
- Govern privacy risk in analytics, automated decisions and AI systems.
- Define decision rights, escalation and risk-acceptance processes.
- Report material privacy risk and program performance to executives and the board.
- Engage regulators, customers and external stakeholders on significant matters.
- Lead the privacy team, budget, technology portfolio and outside advisers.
- Coordinate with the DPO while respecting the DPO's legally required independence, if applicable.

REQUIRED QUALIFICATIONS

- years of progressive experience across privacy, legal, compliance, risk, security, data governance or related fields.
- Significant experience leading an enterprise or global privacy program.
- Demonstrated executive and board communication on material risk.
- Experience building teams, allocating resources and leading through regulatory change or incidents.
- Strong working knowledge of privacy laws relevant to .
- Technical and business fluency sufficient to advise on products, data and AI.
- Record of influencing senior stakeholders and resolving difficult cross-functional decisions.

PREFERRED CERTIFICATIONS

CIPP and CIPM; CIPT, CDPSE, AIGP or FIP where relevant.; JD and active bar membership if the role will also perform legal duties.; Experience in [industry], [jurisdictions] and organizations of comparable scale.; Prior regulator engagement, major incident leadership or transformation experience.; Experience integrating privacy with security, data and AI governance.

TECHNICAL KNOWLEDGE

GDPR, CCPA / CPRA, HIPAA, EU AI Act, 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

- Leadership agrees on privacy risk, priorities, accountability and investment.
- The program has a credible roadmap and measures outcomes rather than activity alone.
- High-risk product, data and AI decisions receive timely executive attention.
- Material issues are transparent, owned and progressing toward resolution.
- The privacy organization has the talent, technology and authority to operate effectively.
- Board reporting is concise, decision-oriented and connected to enterprise risk.

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