SCAN FOR THE TEMPLATE

JOB DESCRIPTION TEMPLATE

Chief Privacy Officer (CPO)

The senior executive who owns the enterprise privacy program, protecting personal data and keeping the organization compliant with data protection law worldwide.

Department	Privacy / Legal / Data Governance
Reports to	General Counsel / Chief Executive Officer / Chief Compliance Officer
Location	Remote / Hybrid / On-site
Employment type	Full-time
Experience	12 to 18+ years

POSITION OVERVIEW

The Chief Privacy Officer (CPO) provides executive leadership for the organization's enterprise privacy and data protection program. This role owns the strategy, policies, controls, and governance that protect personal data and keep the organization compliant with global privacy law throughout the data lifecycle.

The CPO partners closely with legal, compliance, security, data governance, product, marketing, human resources, and business units to embed privacy by design, respond to individual rights requests, and manage privacy risk. The role often serves as, or oversees, the designated Data Protection Officer where required.

As organizations expand their use of AI and automated decision making, the Chief Privacy Officer plays a central role in governing how personal data is used to train and operate AI systems, ensuring transparency, fairness, and lawful processing alongside risk and AI governance leaders.

KEY RESPONSIBILITIES

PRIVACY PROGRAM LEADERSHIP

- Define and own the enterprise privacy strategy and program.
- Establish privacy policies, standards, and the privacy governance model.
- Set privacy risk appetite and program metrics.
- Embed privacy by design and by default across products and processes.
- Report privacy posture, risks, and incidents to executive leadership and the Board.

REGULATORY COMPLIANCE

Ensure compliance with applicable privacy and data protection laws across jurisdictions, including:

- GDPR and UK GDPR, and other regional data protection regimes
- US state privacy laws such as the CCPA and CPRA and comparable statutes
- Sector rules such as HIPAA and GLBA where relevant
- Cross-border transfer mechanisms and evolving AI and profiling rules

DATA GOVERNANCE AND MAPPING

- Maintain data inventories, records of processing, and data flow mapping.
- Define data classification, retention, and minimization standards.
- Govern lawful bases and consent management.
- Partner with data governance on quality and stewardship.

PRIVACY RISK AND ASSESSMENTS

Own the privacy impact assessment and Data Protection Impact Assessment (DPIA) process. Evaluate new products, vendors, technologies, and AI use cases for privacy risk, and drive mitigation before deployment.

INDIVIDUAL RIGHTS AND INCIDENTS

- Operate processes for access, deletion, and other individual rights requests.
- Lead privacy incident and breach response and regulatory notification.
- Manage privacy complaints and inquiries.
- Coordinate with security on data-related events.

VENDOR AND CROSS-BORDER MANAGEMENT

Assess third-party and processor privacy practices, manage data processing agreements, and govern international data transfers using approved mechanisms and safeguards.

TRAINING, CULTURE, AND ENGAGEMENT

Deliver enterprise privacy training and awareness, advise business and product teams, and engage with regulators, supervisory authorities, and industry bodies on privacy matters.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Law, Information Systems, Business, or a related discipline. Juris Doctor (JD) or Master's degree often preferred.
- 12 to 18+ years of progressive experience in privacy, data protection, legal, compliance, or information governance.
- 5+ years leading an enterprise or regional privacy program.
- Experience briefing executive leadership and Boards of Directors.
- Deep knowledge of global privacy law and data protection frameworks.
- Experience managing privacy incidents, DPIAs, and regulatory engagement.

PREFERRED CERTIFICATIONS

One or more of: CIPP (such as CIPP/US or CIPP/E), CIPM, CIPT, CDPSE, FIP, and a Juris Doctor (JD) where the role requires legal depth.

TECHNICAL KNOWLEDGE

Enterprise privacy program design, global data protection law, privacy by design, data mapping and records of processing, DPIAs and privacy impact assessments, consent and lawful-basis management, data classification and retention, individual rights operations, breach response and notification, cross-border transfers, vendor privacy management, and privacy considerations for AI and automated processing.

ESSENTIAL COMPETENCIES

Executive leadership, legal and regulatory judgment, executive and Board communication, cross-functional influence, pragmatic risk balancing, program management, and the independence to advise on and escalate privacy risk.

SUCCESS MEASURES: FIRST 12 MONTHS

- Assess and refresh the enterprise privacy program.
- Update privacy policies, notices, and standards.
- Maintain records of processing and data inventories.
- Strengthen the DPIA and privacy-by-design process.
- Operationalize individual rights and breach response.
- Govern cross-border transfers and processor agreements.
- Deliver enterprise privacy training.
- Improve privacy risk posture and Board reporting.