

JOB DESCRIPTION TEMPLATE

Data Protection Officer

is appointing a Data Protection Officer to perform the advisory, monitoring and liaison tasks established by applicable data-protection law. The DPO will report directly to the highest management level, receive timely access to matters involving personal data and perform DPO duties independently.

Reports to	Highest management level: Board / CEO / equivalent
Employment type	Full-time

POSITION OVERVIEW

the organization is appointing a Data Protection Officer to perform the advisory, monitoring and liaison tasks established by applicable data-protection law. The DPO will report directly to the highest management level, receive timely access to matters involving personal data and perform DPO duties independently.

The organization remains accountable for compliance and for decisions about the purposes and means of processing. The DPO advises, monitors and escalates; the DPO does not assume management's legal responsibility.

KEY RESPONSIBILITIES

KEY RESPONSIBILITIES

- Inform and advise the organization and its employees about data-protection obligations.
- Monitor compliance with applicable law, policies, assigned responsibilities, training and audits.
- Advise on data protection impact assessments and monitor their performance.
- Cooperate with supervisory authorities and act as their contact point.
- Serve as an accessible contact point for individuals on data-protection matters.
- Report significant concerns to the highest management level.
- Monitor privacy risk, incidents, complaints, remediation and program effectiveness.
- Maintain awareness of processing operations, information systems and regulatory change.

REQUIRED QUALIFICATIONS

- Expert knowledge of data-protection law and practice appropriate to the organization's processing, sector and risk.
- Substantial experience advising on or monitoring privacy programs.
- Ability to exercise independent judgment and communicate concerns to senior leadership.
- Experience with DPIAs, audits, incidents, complaints and regulatory engagement.
- Working understanding of information systems, security, data governance and the organization's operations.
- Professional discretion, integrity and credibility.

PREFERRED CERTIFICATIONS

CIPP/E and/or CIPM, while recognizing that the GDPR does not mandate a particular certification.; Prior DPO, Deputy DPO, senior privacy counsel, audit or privacy-leadership experience.; Experience in [industry] and across [relevant jurisdictions].; Relevant language skills.

TECHNICAL KNOWLEDGE

GDPR, UK GDPR, CCPA / CPRA, 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

- Confirm the appointment's scope, resources, reporting and conflict safeguards.
- Establish direct access to the highest management level and a regular reporting cadence.
- Assess program effectiveness and prioritize material gaps.
- Review the DPIA, incident, complaint, training and monitoring arrangements.

- Build effective working relationships with management and supervisory authorities while preserving independence.

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/data-protection-officer-job-description · A resource from **GRC Careers**