



JOB DESCRIPTION TEMPLATE

Data Protection Officer (DPO)

The organization's independent authority on data protection, monitoring GDPR compliance, advising on processing, and serving as contact for regulators and data subjects.

Department	Privacy / Legal / Compliance
Reports to	Board / General Counsel / Chief Privacy Officer
Location	Remote / Hybrid / On-site
Employment type	Full-time
Experience	8 to 12+ years

POSITION OVERVIEW

The Data Protection Officer (DPO) provides independent oversight of the organization's data protection compliance. As defined under GDPR Articles 37 to 39, the DPO monitors compliance, advises the organization, and serves as the contact point for supervisory authorities and data subjects.

The DPO partners with legal, privacy, security, IT, and business units to embed data protection by design, advise on data protection impact assessments, and support the exercise of data subject rights, while maintaining the independence the role requires.

As privacy regulation expands globally, the DPO serves as the organization's trusted authority on data protection compliance and the responsible handling of personal data.

KEY RESPONSIBILITIES

COMPLIANCE MONITORING

- Monitor compliance with the GDPR and applicable data protection laws.
- Advise the organization on its data protection obligations.
- Assess processing activities and records of processing.
- Report on the state of data protection to leadership and the Board.
- Maintain independence in performing the DPO role.

ADVISORY AND DPIAS

Provide advice on data protection impact assessments and high-risk processing, including:

- When a DPIA is required and how to conduct it
- Assessment of risks to data subjects
- Mitigations and safeguards for high-risk processing
- Consultation with supervisory authorities where needed

DATA SUBJECT RIGHTS

- Support handling of access, erasure, and other rights requests.
- Advise on lawful bases and consent management.
- Oversee response processes and timelines.
- Track and report on rights request volumes and outcomes.

DATA PROTECTION BY DESIGN

Advise on embedding data protection by design and by default into systems, products, and processes, including data minimization, purpose limitation, retention, and security safeguards.

SUPERVISORY AUTHORITY LIAISON

Serve as the contact point for supervisory authorities, cooperate on investigations and consultations, and act as the contact for data subjects on matters related to processing of their personal data.

RECORDS AND ACCOUNTABILITY

- Support records of processing activities (ROPA).
- Advise on data processing agreements and transfers.
- Assess vendors and processors for data protection compliance.
- Maintain documentation demonstrating accountability.

AWARENESS AND TRAINING

Raise awareness of data protection across the organization through training, guidance, and staff education, and monitor the effectiveness of data protection controls.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Law, Information Systems, Privacy, or a related discipline. Advanced degree a plus.
- 8 to 12+ years of experience in data protection, privacy, legal, or compliance.
- Expert knowledge of the GDPR and applicable data protection law.
- Experience advising on DPIAs and high-risk processing.
- Ability to operate independently and report to the highest level of management.
- Experience liaising with regulators or supervisory authorities preferred.

PREFERRED CERTIFICATIONS

One or more of: CIPP/E, CIPM, CIPT, or ISO 27701 Lead Implementer or Lead Auditor.

TECHNICAL KNOWLEDGE

GDPR and data protection law, data protection impact assessments, data subject rights, lawful bases and consent, records of processing activities, international data transfers, data processing agreements, privacy by design, ISO 27701, and vendor and processor assessment.

ESSENTIAL COMPETENCIES

Independence and objectivity, sound judgment, regulatory interpretation, stakeholder advisory, discretion and confidentiality, clear communication, and the ability to influence without authority.

SUCCESS MEASURES: FIRST 12 MONTHS

- Assess the maturity of the data protection program.
- Establish or refresh DPIA and high-risk processing procedures.
- Strengthen data subject rights handling and timelines.
- Support and validate records of processing activities.
- Advise on data protection by design in key initiatives.
- Establish the supervisory authority liaison process.
- Deliver data protection awareness and training.
- Build data protection reporting to leadership and the Board.

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**