DATA PROTECTION OFFICER

Position Description

Data Protection Officer

Organizational Relationship[1]: Reports to [Chief Financial Officer / Chief Operating Officer / General Counsel / Head of Public Policy / Chief Compliance Officer]

Location[2]: [●]

Compensation: [●]

General Summary:

[Company] is looking to recruit an experienced Data Protection Officer (DPO) to meet its obligations under the European Union (EU) General Data Protection Regulation (GDPR). Reporting to the [Chief Financial Officer / Chief Operating Officer / General Counsel / Head of Public Policy / Chief Compliance Officer], the statutory DPO will monitor compliance and data practices internally to ensure the business and its functions comply with the applicable requirements under the GDPR. The DPO will be responsible for staff training, data protection impact assessments, and internal audits. The DPO will also serve as the primary contact for supervisory authorities and individuals whose data is processed by the organisation.

Essential Duties and Responsibilities:

In this role, you will work closely with the [Legal, Compliance, Public Policy, and Information Security] functions to develop and monitor policies and standards applicable to the business and in compliance with the GDPR. Duties will include:

- Implementing measures and a privacy governance framework to manage data use in compliance with the GDPR, including developing templates for data collection, assisting with data mapping, and vendor management reviews.
- Working with key internal stakeholders in the review of projects and related data to ensure compliance with local data privacy laws, and where necessary, complete and advise on privacy impact assessments.
- Serving as the primary point of contact and liaison for the [Lead Supervisory Authority] and other EEA Data Protection Authorities on all data protection related matters under the GDPR.
- Serving as the primary point of contact for queries in the business.
- Reviewing vendor contracts (including Model Clauses) and consents needed to implement projects in partnership with the firm's Procurement and Information Security functions, and ensuring filing requirements with local regulators are achieved.
- Participating in the [Data Privacy / Information Governance] Committee.
- Managing and conducting ongoing reviews of [Company's] privacy governance framework [including Binding Corporate Rules (BCR)[3]]
- Monitoring changes to local privacy laws and making recommendations to the [Data Privacy / Information Governance] Committee when appropriate.
- Setting standards and reviewing policies and procedures globally that meet the requirements under the GDPR and any localization requirements in countries of operation.
- Developing and delivering privacy training to various business functions.
- Developing strategies and initiatives to ensure engagement with key internal and external stakeholders.
- Coordinating and conducting data privacy audits.
- Collaborating with the Information Security function(s) to raise employee awareness of data privacy and security issues, and providing training on the subject matter.
- Collaborating with the Information Security function(s) to maintain records of all data assets and exports, and maintaining a data security incident management plan to ensure timely remediation of incidents including impact assessments, security breach response, complaints, claims or notifications, and responding to subject access requests (SARs).

[1] Note: Under the GDPR, the DPO must operate independently, report to the highest management level of the organization (e.g., board level), and not be penalised for performing their duties.
[2] Note: While the DPO does not need to be physically located in an EU Member State, the DPO must be available to the supervisory authorities.
[3] Note: Applicable only if the Company has approved BCRs

DATA PROTECTION OFFICER continued

Position Description

- Ensuring that the [Company's] IT systems and procedures comply with all relevant data privacy and protection law, regulation and policy (including in relation to the retention and destruction of data).
- Working with designated privacy law attorneys across the [Company's] offices and, where necessary, outside counsel to help advise on local data privacy law issues.
- Promoting effective work practices, working as a team member, and showing respect for co-workers.

Position Specifications

Education	▪ [Law degree from an accredited law school required.] ▪ Hold at least one Data Protection and/or Privacy certification such as, CIPP, CIPT, ISEB, etc., (preferred).
Work Experience	▪ [●] years PQE experience required. ▪ Experience in [Country] and/or EU data privacy laws. ▪ [●] years' experience within a compliance, legal, audit and/or risk function, with recent experience in privacy compliance. ▪ Experience in developing policy and compliance training. ▪ [Experience working in a regulated industry.][4]
Knowledge, Skills, and Abilities	▪ Strong knowledge of EU data privacy and data protection regulation, and a good understanding of other major privacy frameworks and evolving legislation worldwide. ▪ Sufficient knowledge of information technology and data management systems required. ▪ Well-developed and professional interpersonal skills; ability to interact effectively with people at all organisational levels of the firm. ▪ [Experience of working in a large, global organisation][5] ▪ Ability to work unsupervised, exercise leadership, and influence change. ▪ Excellent writing and presentation skills. ▪ Strong change and project management skills, including the ability to manage time well, prioritise effectively, and handle multiple deadlines. ▪ Ability to undertake large, long-term projects, develop alternative methods to complete them, and implement solutions. ▪ Ability to use independent judgment and discretion when making majority of decisions. ▪ Detail-oriented approach needed to recommend and implement strategic improvements on a range of data privacy and data protection issues. ▪ Ability to handle confidential and sensitive information with the appropriate discretion. ▪ Knowledge of PC applications, including MS Office.
Additional Requirements	▪ Some international travel [will] / [may] be required.[6] ▪ The statements contained in this position description are not necessarily all-inclusive; additional duties may be assigned and requirements may vary from time to time.

[4] *If the Company operates in a regulated industry, such as telecoms, healthcare, or financial services.*
[5] *If applicable to the Company*
[6] *If Company has an international footprint*