Job Description

Position: Data Protection Officer (DPO) Zimbabwe
Reports To: [Managing Director/Board]
Department: [N/A]
Location: [Insert Location]
Job Type: [Full-Time/Part-Time/Contractual]

Purpose

To ensure compliance with the Cyber and Data Protection Act [Chapter 12:07] and SI 155 of 2024, safeguard organizational data integrity and confidentiality, oversee data processing activities, uphold rights of data subjects, and oversee implementation of cybersecurity measures to protect personal identifiable information and sensitive information.

Key Responsibilities

Compliance and Oversight

- Ensure personal data processing complies with principles of fairness, lawfulness, and transparency.
- Monitor data collection, storage, and transfer practices to ensure adherence to the Act.
- Develop, review, and oversee implementation of internal policies for data protection, privacy notices, and cybersecurity compliance.
- Oversee and ensure compliance with transborder data transfer regulations.

Data Protection Governance

- Act as the primary liaison with the Data Protection Authority for audits, notifications, and compliance reporting.
- Maintain the organization's data processing register and submit updates to the Authority as required.
- Develop and enforce a Code of Conduct for data controllers in line with the Authority's guidelines.

- Ensure privacy notices follow the guidelines of the Act and fulfill the mandate of informing the data subjects of their rights and processing of information.

Risk Management and Incident Response

- Oversee Implementation of appropriate technical and organizational measures to protect against data breaches and unauthorized access.
- Notify the Authority within 24 hours of a data breach and affected individuals within 72 hours for high-risk breaches and mitigate risks promptly.
- Maintain comprehensive records of all data breaches and provide timely reports to the Authority.
- Conduct periodic data protection impact assessments and privacy audits to identify and address vulnerabilities.

Training and Advocacy

- Educate staff about data protection responsibilities and cybersecurity best practices.
- Provide guidance on the rights of data subjects, including access, correction, and objection to processing.
- Promote a culture of data protection and security within the organization.

Legal and Regulatory Support

- Provide expert advice on data processing, privacy rights, and sensitive information management.
- Collaborate with legal teams to handle compliance disputes, audits, or investigations by the Authority.
- Ensure compliance with cybersecurity measures for protecting critical information infrastructures.

Technical Oversight

- Ensure secure processing of personal identifiable information, genetic, biometric, and health data in compliance with the Act.
- Oversee the deployment of encryption, access controls, and other data protection measures.

Children's Data Protection

- Oversee processing of children's personal information, ensuring parental or guardian consent is obtained and verified.
- Conduct regular assessments to identify and mitigate privacy risks to children.
- Implement data protection by design and default for children's data and prevent automated decision-making that could affect their rights.

Qualifications

- Bachelor's degree in Information Technology, Cybersecurity, Law, Data Science or a related field.
- Certification in Data Protection from POTRAZ.
- Thorough knowledge of data protection laws and practices, including the Cyber and Data Protection Act [Chapter 12:07].
- Strong understanding of IT systems, and cybersecurity protocols.

Skills and Competencies

- Change Management.
- Ability to communicate effectively with executives and the Board.
- Analytical skills to assess data protection risks.
- Ability to develop and enforce compliance frameworks.
- Excellent communication and training abilities.
- Familiarity with legal and regulatory environments.
- Strong ethical standards and attention to detail.

Disclaimer:

This job description is intended to provide a general overview of the responsibilities and requirements of the position. It is not an exhaustive list of all duties, responsibilities, or qualifications associated with the job. The organization

reserves the right to amend or add to the job description at any time to meet organizational needs and those of the regulator.

All responsibilities and qualifications outlined herein are in alignment with the Cyber and Data Protection Act [Chapter 12:07] and the Cyber and Data Protection Regulations (S.I. 155 of 2024). Compliance with these legal frameworks is mandatory and subject to change as per the guidance of the Data Protection Authority (POTRAZ).

You are advised that additional requirements or adjustments to responsibilities may be necessary to address evolving data protection laws, regulations, or organizational priorities.

PrivacyCure will not be held accountable for any damages or non-compliance matters that may arise from the use of this Job Description. For expert assistance please contact us.