**the national identification and registration authority (nira)**

**job description**

|  |  |
| --- | --- |
| **JOB TITLE:** | Data Protection Officer |
| **DIVISION:** |  |
| **DEPARTMENT:** | Data Protection |
| **LOCATION:** |  |
| **REPORTS TO:** | DIRECTLY: The Chief Data Protection Officer |
| **MANAGES:** | DIRECTLY: N/A  INDIRECTLY: N/A |

This document will be used as a management tool. It will specifically enable the classification of positions and the evaluation of the performance of the post incumbent.

This document is validated as an accurate and true description of the job as signified below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Manager/Supervisor Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Head of Department/Division Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date received in Human Resource Department Date Created/revised

**1. POSITION SUMMARY**

The Data Protection Officer (DPO) supports the Chief Data Protection Officer in ensuring compliance with the Data Protection Act and the National Identification and Registration Act. The DPO monitors data handling practices, supports data protection audits, manages data subject requests, and promotes a culture of privacy by design and default. The role involves detailed analysis, regular monitoring, staff support, and liaison with both internal stakeholders and regulatory bodies under the direction of the CDPO.

**2. KEY OUTPUTS**

* Reports on compliance in processing data, Data Protection Impact Assessments (DPIAs), and risk assessments.
* Records of data subject requests and breach management logs.
* Compliance checklists, gap analysis reports, and policy updates.
* Training and awareness materials, along with the delivery record.
* Internal audit support documents and logs of corrective actions.

**3. KEY RESPONSIBILITY AREAS**

**Compliance and Risk Monitoring**

* Monitor the organisation’s adherence to the Data Protection Act and related regulations.
* Conduct and support privacy risk assessments, Data Protection Impact Assessments (DPIAs), and compliance checks.
* Monitor developments in international privacy laws and revise internal guidance accordingly.
* Maintain and update the Record of Processing Activities (ROPA).

**Data Subject Rights and Breach Management**

* Receive, log, and manage data subject access requests (DSARs) while complying with statutory deadlines.
* Assist with breach investigations and escalate issues to the CDPO with recommendations for response and remediation.
* Support the design and enhancement of data rights request workflows and templates.

**Policy and Process Support**

* Assist in drafting, updating, and reviewing policies and procedures related to data protection.
* Help integrate privacy by design into new projects and data initiatives.
* Support the CDPO in implementing safeguards and controls for cross-border data transfers.

**Training and Awareness**

* Coordinate and provide training on data privacy to NIRA staff.
* Develop materials for awareness and privacy-related communications intended for internal distribution.
* Monitor staff participation and the effectiveness of training activities.

**Reporting and Documentation**

* Prepare compliance updates, audit summaries, and DPIA outcomes for the CDPO.
* Maintain thorough documentation on all data protection activities for internal reviews and external audits.
* Assist in drafting the Authority’s data protection reports for external regulatory bodies.

**Stakeholder Engagement**

* Serve as the first point of contact for staff regarding data protection issues, escalating when necessary.
* Support internal teams to ensure data privacy requirements are met in all processes and projects.

**Other Duties**

* Carry out additional related duties as directed by the CDPO, in accordance with the position's nature and objectives.

**4. PERFORMANCE STANDARDS**

* All DSARs and breach responses are handled within statutory timeframes.
* Compliance reports are submitted in accordance with internal schedules.
* Data protection training is delivered according to annual plans.
* DPIAs, risk assessments, and internal audits are conducted to required standards.
* Policies and procedures have been updated based on legal changes or audit findings.

**5. AUTHORITY**

* Recommend updates to internal policies and procedures to the CDPO.
* Escalate compliance breaches and potential risks to the CDPO.
* Engage MDA staff to investigate or clarify data use practices.

**6. INTERNAL AND EXTERNAL CONTACTS**

Internal Contacts

* All Divisions

External Contacts

* The Office of the Information Commissioner
* Law Enforcement Agencies as delegated
* Data Subjects and their representatives

**7. REQUIRED COMPETENCIES**

Core

* Strong communication and interpersonal skills
* Attention to detail and methodical work ethic
* High ethical standards and confidentiality
* Ability to work independently under guidance

Technical

* Sound knowledge of the Data Protection Act and the NIRA
* Familiarity with international data protection laws (e.g., GDPR)
* Understanding of privacy impact assessments, DSARs, and data governance
* Working knowledge of IT systems and information security principles

**8. REQUIRED EDUCATION AND EXPERIENCE**

* Bachelor’s Degree in Law, Information Management, Computer Science, Public Administration, or a related discipline.
* 2 – 4 years of experience in data protection, compliance, audit or privacy-related roles
* Formal certification in data protection or privacy (e.g. CIPP/E, CIPM) is desirable.

**9. SPECIAL CONDITIONS ASSOCIATED WITH THE JOB**

* Work will take place in an office and training environment equipped with standard office and training equipment, specialised software, and teaching and learning tools. The environment requires regular interactions with staff.
* May be required to travel for audits, training, or stakeholder engagement
* Will interact with sensitive personal data and must observe strict confidentiality
* May require occasional extended hours for audit deadlines or breach response

**REMUNERATION**

Salary range: $ 5,198,035.00 p.a. - $ 6,990,779.00 p.a. - **Band 8**