PROPOSED · SUBMITTED FOR ODPC CONSIDERATION

OFFICE OF THE DATA PROTECTION COMMISSIONER · REPUBLIC OF KENYA

Draft Guidelines on the Designation, Tasks, Position, and Professional Development of Data Protection Officers

Issued pursuant to Section 8 of the Data Protection Act, 2019, to operationalise the Data Protection Officer function under Section 24

PREPARED BY
Muchangi Patrick & Co. Advocates

REFERENCE FRAMEWORKS
Mauritius (2026) & Nigeria (2025)

VERSION
1.0 · July 2026

DPA §24
2019

A NOTE ON THIS DOCUMENT

Kenya's Data Protection Act, 2019 provides for the designation of Data Protection Officers under Section 24, but is silent on their qualification, certification, verification and continuous professional development. Mauritius and Nigeria have each recently addressed that gap through detailed regulation. The guidelines below draw on the strengths of both frameworks, adapted to the Kenyan context, and are put forward for consideration and consultation by the Office of the Data Protection Commissioner. They are not currently in force. For the full comparative analysis behind this proposal, see our Insights article.

CONTENTS

1. Part I — Definitions & Interpretation
2. Part II — Designation of DPOs
3. Part III — Tasks & Duties of the DPO
4. Part IV — Position & Independence
5. Part V — Verification Framework
6. Part VI — Continuous Professional Development
7. Part VII — Compliance & Enforcement
8. Part VIII — Transitional Provisions
9. Part IX — Miscellaneous Provisions

> ***WHEREAS*** *Section 24 of the Data Protection Act, 2019 (the "Act") provides for the designation of Data Protection Officers (DPOs) to advise on and ensure compliance with*

data protection requirements;

WHEREAS *the Act provides that DPOs shall advise data controllers and data processors, ensure compliance, facilitate capacity building, provide advice on data protection impact assessments, and cooperate with the Data Commissioner;*

WHEREAS *there is a need to clarify the qualifications, tasks, and protections to be afforded to DPOs to ensure effective implementation of the Act;*

WHEREAS *there is a need to establish a framework for the verification of DPO qualifications and ongoing professional development to ensure that DPOs maintain the competence required to fulfil their functions;*

NOW, THEREFORE, the Office of the Data Protection Commissioner, pursuant to Section 8 of the Act, is invited to issue these Guidelines to operationalise the DPO function.

PART I

Definitions & Interpretation

1.1 Definitions

In these Guidelines, unless the context otherwise requires:

"Accredited Training Institution"
means a training institution registered and approved by the Data Commissioner for its expertise in data protection laws and practices.

"Active Verification Status"
means the status of a DPO who has met the verification and professional development requirements under these Guidelines.

"CPD"
means Continuous Professional Development as defined by the Data Commissioner.

"Data Controller" / "Data Processor"
have the meanings assigned under Section 2 of the Act.

"DPO"
means a Data Protection Officer designated under Section 24 of the Act.

"Lead DPO"
means a DPO designated as the primary point of contact with the Office in cases where multiple DPOs are designated.

"Office"
means the Office of the Data Protection Commissioner.

"PEER Form"
means the Professional Education and Engagement Review Form prescribed by the Data Commissioner.

PART II

Designation of Data Protection Officers

2.1 Mandatory Designation

Every data controller and data processor shall designate a DPO from among their staff members. Where a group of entities share a DPO, the designation must be made by each controller or processor, and the shared arrangement clearly documented.

2.2 Criteria for Designation

A DPO shall be designated on the basis of professional qualifications and shall demonstrate:

a. Expert knowledge of data protection laws and practices applicable in Kenya, including the Act and any regulations or guidelines issued thereunder;

b. Proven ability to fulfil the tasks specified in these Guidelines and under the Act;

c. In-depth understanding of the operational requirements of the organisation and the specific regulatory environment of its business sector;

d. Relevant experience in data protection, compliance, law, information technology, or a related field.

2.3 Certification Requirements

Every DPO shall hold evidence of certification issued either by:

a. The Office, following successful completion of training conducted by the Office, or by a training institution accredited by the Office; or

b. A recognised international privacy certification body, provided such certification is approved by the Office.

2.4 Multiple DPOs

a. A data controller or data processor may designate more than one DPO, having regard to organisational structure, size and scale; the complexity of processing operations; and the sensitivity of personal data processed.

b. Where multiple DPOs are designated, the controller or processor shall designate a Lead DPO, serving as the primary point of contact with the Office and with data subjects.

2.5 Publication of DPO Details

A data controller or data processor shall publish the DPO's contact details on the organisation's website, communicate them to the Office, and notify the Office and data subjects of any change in designation.

PART III

Tasks & Duties of the Data Protection Officer

3.1 Core Functions

A DPO shall perform the following core functions under Section 24 of the Act:

a. Advise the data controller or data processor and their employees on data processing requirements under the Act or any other written law;

b. Ensure, on behalf of the controller or processor, that the Act is complied with;

c. Facilitate capacity building of staff involved in data processing operations;

d. Provide advice on data protection impact assessments; and

e. Co-operate with the Office and any other authority on matters relating to data protection.

3.2 Additional Functions

In addition, a DPO shall:

a. Monitor and evaluate the efficiency of data systems in the organisation;

b. Keep written records of processing activities;

c. Serve as the primary point of contact for data subjects exercising their rights under the Act;

d. Manage data subject access requests and privacy complaints;

e. Conduct data protection impact assessments for new processing activities;

f. Maintain records of processing activities and data flow maps;

g. Ensure data protection policies and procedures are reviewed and updated regularly;

h. Report data breaches to the Office in accordance with the Act.

3.3 Involvement in Processing Activities

The DPO shall be involved, in a timely manner, in all issues related to the protection of personal data, including the development of policies, implementation of technical and organisational measures, DPIAs, and the handling of data subject requests and complaints.

PART IV

Position & Independence of the Data Protection Officer

4.1 Reporting Line

A DPO shall report to the highest management level of the organisation. Where multiple DPOs are designated, the Lead DPO shall have direct access to the highest management level.

4.2 Resources & Support

A data controller or data processor shall provide the DPO with necessary resources — time, budget, access to information and appropriate training — and allow participation in relevant meetings and decisions relating to data protection.

4.3 Conflict of Interest

Duties assigned to the DPO must be compatible with their regulatory tasks and must not create a conflict of interest that would compromise independence.

4.4 Protection from Penalisation

A data controller or data processor shall not dismiss, suspend, or otherwise penalise a DPO for lawfully performing their duties under the Act and these Guidelines.

4.5 Independent Performance

A DPO shall be permitted to carry out their functions independently, without unlawful interference from the controller, processor, or any other person.

PART V

Verification Framework

5.1 DPO Verification

Every DPO shall be verified by the Office to confirm compliance with the qualification, certification, and professional development requirements under these Guidelines.

5.2 Application for Verification

An application shall be submitted in the prescribed form and shall include evidence of certification; a curriculum vitae; a statement of duties and responsibilities; a declaration of no conflict of interest; and any other information the Office may require.

5.3 Verification Validity

A DPO verification shall be valid for one year from issuance, subject to annual renewal.

5.4 Annual Verification

Renewal requires evidence of compliance with the CPD requirements under Part VI.

5.5 Temporary Inactive Status

A DPO who fails to meet prescribed requirements may be placed on temporary inactive status pending remediation, and may be required to cease performing certain functions during that period.

5.6 Digital Platform

The Office shall establish a digital platform for the submission and monitoring of DPO verification and CPD records.

PART VI

Continuous Professional Development

6.1 Annual CPD Requirement

a. A verified DPO shall obtain a minimum of twenty (20) CPD points annually to maintain active verification status.

b. At least ten (10) of the required points must be earned through structured training and certification activities.

6.2 Qualifying CPD Activities

6.2.1 Formal Training and Certification (minimum 10 points): Office-accredited training programmes; recognised workshops and webinars; approved e-learning courses; the Office's Virtual Privacy Academy courses; acquisition or renewal of recognised international privacy certifications.

6.2.2 Knowledge Contribution (maximum 10 points annually): publication of peer-reviewed articles; publication of industry articles and policy briefs.

6.2.3 Professional Engagement (maximum 8 points annually): speaking engagements, panels and facilitation of accredited training; participation in recognised privacy conferences;

membership in professional bodies; participation in Office technical working groups; mentorship of emerging privacy professionals; contributions to regulatory consultations.

6.3 Evidence of CPD Activities

A DPO shall retain verifiable evidence — certificates of attendance, confirmation emails, copies or links to publications, formal letters of participation, and Professional Education and Engagement Review (PEER) Forms.

6.4 CPD Points Allocation & Assessment

The Office shall prescribe a CPD points framework, review compliance annually at revalidation, and may request CPD records for review at any time.

PART VII

Compliance & Enforcement

7.1 Compliance Review

Compliance with these Guidelines shall be reviewed annually during DPO verification revalidation.

7.2 Non-Compliance (Controller/Processor)

A data controller or processor who fails to designate a DPO or ensure compliance may be subject to enforcement action under the Act, including a compliance notice, an enforcement notice, administrative fines, and any other available remedy.

7.3 Non-Compliance (DPO)

A DPO who fails to meet prescribed CPD requirements may be placed on temporary inactive status pending remediation; failure to remediate within a specified period may result in suspension of verification status.

PART VIII

Transitional Provisions

8.1 Transition Period

Existing DPOs designated under Section 24 shall have twelve (12) months from issuance of these Guidelines to comply with the qualification, certification, and verification requirements.

8.2 Legacy Recognition

A DPO who does not meet the certification requirements under Section 2.3 but possesses significant experience may be recognised case-by-case, provided they demonstrate expert knowledge of Kenyan data protection law, have held the role for at least three (3) years, submit a development plan to achieve certification within twelve (12) months, and meet all other requirements.

8.3 Training Accreditation

The Office shall, within six (6) months of issuance, establish a process for accrediting training institutions and approving certification programmes.

8.4 Digital Platform

The Office shall, within twelve (12) months of issuance, develop and launch the digital platform for submission and monitoring of DPO verification and CPD records.

PART IX

Miscellaneous Provisions

9.1 Interpretation

These Guidelines shall be interpreted in accordance with the Data Protection Act, 2019 and any other relevant laws.

9.2 Amendment

The Office may amend these Guidelines from time to time as necessary to give effect to the Act or to align with emerging best practices.

9.3 Review

The Office shall review these Guidelines within three (3) years of issuance.

SUBMITTED FOR CONSIDERATION BY

The Office of the Data Protection Commissioner, Republic of Kenya

PREPARED BY

Muchangi Patrick & Co. Advocates, Nairobi

VERSION 1.0 · JULY 2026

ABOUT THIS PROPOSAL

Muchangi Patrick & Co. Advocates prepared this draft framework as part of our ongoing regulatory and policy work on data protection in Kenya. We welcome engagement from the ODPC, industry bodies, and fellow practitioners on refining it ahead of any formal consultation process.

Discuss This Proposal | Read the Full Analysis | Back to Resource Centre