



SUMMARY: GUIDANCE NOTES FOR
DATA PROTECTION OFFICERS

DATA & PRIVACY LAW

Kenya

Mayfair Suites, 4th Floor,
Parklands Gardens, Westlands,
Parklands Road,
Nairobi, KE.

e: hello@onganyaombo.com

t: +254 208 400 629

w: www.obang.law

Guidance Notes for Data Protection Officers

INTRODUCTION

The Guidance Notes published by the Office of the Data Protection Commissioner (ODPC) is meant to provide practical guidance on designating and positioning Data Protection Officers (DPOs) under the Data Protection Act, 2019 and its regulations.

The Guidance Notes apply to all data protection controllers and data processors that are subject to the Data Protection Act, 2019 (DPA). It should be read together with the Data Protection (General) Regulations, 2021, the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 and any other applicable laws and regulations issued by the ODPC.



DPOs
GUIDE

What does the Data Protection Act (DPA) say about a Data Protection Officer (DPO)?

Section 24 (1) of the DPA provides that a data controller or data processor may designate or appoint a Data Protection Officer, on any terms they determine, where the processing is carried out by a public body or private body, except for courts acting in their judicial capacity; the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects; or the core activities of the data controller or data processor consist of processing sensitive categories of personal data.

Organisational Structure for DPO role?

Internal DPO

An internal DPO may be appointed from within the organisation's existing staff or as a new hire, provided the individual's role allows functional independence and freedom from conflicts of interest.

The internal DPO should ideally not hold any position that determines the purposes or means of data processing and should have sufficient authority and direct access to senior management to perform their duties effectively.

External DPO

An external DPO is appointed to support compliance, provided the DPO remains independent, accessible, qualified, and has no conflicts of interest in the performance of their duties. The external DPO arrangement is particularly suitable where an organisation lacks in-house expertise or needs independent oversight.

Shared DPO

A shared DPO arrangement is permissible for groups of related entities, such as subsidiaries, associations, or organisations operating under a common structure. In such cases, the shared DPO should have the capacity, expertise, and resources to serve each entity effectively and should remain accessible to all data subjects across participating organisations.

Positioning and Independence of the DPO?

Independence

To ensure objective risk assessment without fear of reprisal, the DPO must perform all statutory duties with complete independence, free from external or management instructions.

Reporting Line

The DPO should report directly to the highest level of management, such as the Chief Executive Officer, Managing Director, the Board, or the Board Audit and Risk Committee, to ensure data protection considerations are integrated into the organisation's strategic and operational decisions. By having direct access to top leadership, the DPO can escalate compliance risks, recommend corrective actions, and influence policy and governance matters without unnecessary administrative barriers.

Resources and Support

Organisations should ensure that the DPO is adequately supported with the resources necessary to perform their role effectively. This includes but is not limited to allocating a dedicated budget for data protection activities; providing sufficient staffing or technical support; facilitating continuous professional training; and granting access to legal, IT, and risk

Types of DPOS

Internal, External and Shared

management specialists when required.

Conflict of Interest

The DPO should not simultaneously hold any position within the organisation that determines the purposes or means of processing personal data, such as Head of IT, Human Resources Director, Legal Counsel, or Compliance Manager.

Roles and Responsibilities of the DPO?

Some of the roles of the DPO should include:

Advise the controller, processor, and staff on obligations under the Act by interpreting legal requirements and ensuring new initiatives or technologies align with data protection principles from the outset.

Monitor compliance with laws, regulations, and internal policies by regularly assessing the organisation's data protection practices.

Advise on and oversee Data Protection Impact Assessments for new projects, systems, or initiatives that may pose significant privacy risks. Ensure risks are identified early, mitigation measures are implemented, and outcomes are properly documented and reported to management.

Conduct a breach investigation and assessment, coordinate breach response, and ensure timely notification to the ODPC and affected data subjects in the event of a data breach.

Prepare periodic compliance reports and escalate risks to senior management by summarising the organisation's compliance status, risk assessments,

DPIA outcomes and audit findings.

Competence, Qualifications and Professional Development

An effective Data Protection Officer (DPO) requires a multidisciplinary blend of legal, technical, and organisational expertise to navigate the modern privacy landscape.

The technical skills and professional qualifications may include but are not limited to:

Privacy Governance

The DPO must possess deep knowledge of international frameworks as well as local legislation, specifically the DPA, subsidiary regulations, and constitutional privacy guarantees. Beyond legal mastery, they are responsible for understanding the organisation's unique data ecosystem, drafting essential privacy documentation, and cultivating a proactive compliance culture through clear stakeholder communication and staff training.

Privacy Risk Management & Compliance

Competent DPOs bridge the gap between regulatory mandates and IT infrastructure by conducting Data Protection Impact Assessments (DPIAs), managing Records of Processing Activities (RoPA), and integrating privacy-enhancing technologies into data workflows. Their scope also extends to evaluating cybersecurity protocols, governing cross-border data transfers including ODPC authorisations, and enforcing "privacy by design" across vendor agreements, system budgets, and administrative processes.

Roles of the DPO

Conduct a breach investigation and assessment, coordinate breach response, among others.

Professional Certification & Continuous Professional Development (CPD)

To demonstrate this specialised capability, pursuing local and international Professional Certifications provides tangible assurance of competence to both organisational leadership and regulatory authorities like the ODPC. Furthermore, because technology and regulatory standards constantly evolve, DPOs must sustain initial qualifications through Continuous Professional Development (CPD). By committing to ongoing training and industry learning, DPOs ensure their expertise remains sharp enough to address emerging privacy trends, dynamic cyber risks, and evolving legal standards.

Remuneration Guidance for DPOs

The remuneration of a DPO should reflect the complexity, scope, and strategic importance of the role within an organisation. Organisations should consider organizational size and nature of operations, the scope of responsibility and risk exposure, professional experience and qualifications, and the market benchmarks and sector standards.

Publishing DPOs Contacts

A data controller or data processor is required to publish the contact details of their designated or appointed data protection officer. Such details shall be made available on their official website and/or on any other appropriate platform through which data subjects may seek to exercise their rights or obtain information about the organization's data processing activities.

Conclusion

The Data Protection Officer is central to operationalising the right to privacy and ensuring responsible innovation in Kenya's digital economy. This Guidance Note provides a structured framework for building capacity, enhancing accountability, and aligning national practice with global standards.

Publishing DPOs CONTACTS

A data controller or data processor is required to publish the contact details of their designated or appointed data protection officer.

How We Can Help

O'Bang Law (Ong'anya Ombo Advocates LLP), for the last eight (8) years, advises investors, lenders, and multinational entities that are entering Kenya across various sectors such as energy, agribusiness, real estate, and fintech. Our Kenya-focused team combines corporate, commercial, tax, employment, and dispute resolution specialists with on-the-ground regulatory relationships, providing clients with a single point of contact for structuring, licensing, and cross-border transaction needs. Our sectors include:

Corporate & M&A:	entity formation, joint ventures, debt financing, perfection of securities, acquisitions, outcomes based financing, and exit structuring.
Employment & Immigration:	work permits, local content compliance, and workforce structuring.
Data, Technology & IP:	Data Protection compliance, IP commercialisation, IP franchising, brand protection, and technology transaction support.
Dispute Resolution & Arbitration:	contract enforcement, regulatory disputes, and international arbitration.
Regulatory Compliance & Licensing:	specific licensing applications (banking, insurance, telecoms, energy, capital markets), regulatory approvals from bodies such as the CMA, CBK, CA, and EPRA, and ongoing compliance monitoring for regulated entities.
Tax & Regulatory:	incentive applications, transfer pricing, and compliance with the Kenya Revenue Authority.

The analysis in this report is general market information and does not constitute legal advice for any specific transaction. If you are evaluating an investment, acquisition, or market entry into Kenya, our team can provide a tailored assessment specific to your structure and objectives.

Authored by: Ombo Malumbe and George Philip.

To discuss your plans, contact:



Ombo Malumbe,
Partner
Corporate, Commercial, Tax & Cross
Border Practice
e: om@onganyaombo.com
m: +254 724 026 355



Jack Ong'anya,
Managing Partner,
Litigation & ADR
e: jb@onganyaombo.com
m: +254 711 185 636



Allan Mukuki (PhD Cand.),
Lead Consultant,
Public Policy, Regulatory &
International Law
e: am@onganyaombo.com
m: +254 721 416 578



Flora Ouma,
Director,
Public Affairs & Policy Intelligence
e: fo@onganyaombo.com
m: +254 717 025 792

Your Partner IN KENYA

**8 years advising multinationals. One
team for structuring, licensing, tax, and
disputes.**