OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes for Data Protection Officer (DPOs)

2026

TABLE OF CONTENTS

DEFINITIONS

"Act" means the Data Protection Act, No 24. of 2019.

"Conflict of interest" occurs when the DPO's other roles, responsibilities or personal interests interferes with their ability to independently and objectively fulfill their data protection compliance.

"Data Protection Officer (DPO)" means an individual tasked with the responsibility for ensuring that the processing of personal data complies with applicable data protection laws and regulations.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data.

"Data Processor" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.

"Data Subject" means an identified or identifiable natural person who is the subject of personal data.

"Group of entities" means a collection of related business units, such as subsidiaries, parent companies, branches, or joint ventures that operate under common control or ownership.

"Regulations" means all the regulations enacted in accordance with section 71 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"**Processing**" means any operation or sets of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, or use, disclosure by transmission, dissemination, or otherwise making available; or alignment or combination, restriction, erasure or destruction.

"Regular and Systematic Monitoring" means the ongoing, recurring, organised, and methodical observation, tracking, profiling, or collection of personal data that takes place according to a structured plan or strategy for a defined purpose.

"Sensitive Personal Data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex, or the sexual orientation of the data subject.

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

ABBREVIATIONS

DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
KDPA	Kenya Data Protection Act, Cap 411C
ODPC	Office of the Data Protection Commissioner

FOREWORD

As organisations continue to process large volumes of personal data, the need for stronger internal accountability and compliance mechanisms has become more important than ever. In this regard, the Data Protection Officer (DPO) plays a central role in supporting organisations to meet their data protection obligations and handle personal data responsibly.

The Office of the Data Protection Commissioner (the "Office") has developed this Guidance Note in response to observed challenges across both the public and private sectors in the appointment, positioning and effective functioning of DPOs. In many instances, DPOs have been appointed without clearly defined responsibilities, reporting lines, institutional independence and/or the resources necessary to effectively discharge their functions. These gaps have underscored the need for clear, practical guidance on the designation, appointment and responsibilities of the DPO.

The Office recognises that organisations vary considerably in structure and the nature of their data processing activities. The applicability of this Guidance Note therefore extends across all sectors and organisations of all sizes, while providing sufficient flexibility to account for the diverse operational contexts within which data controllers and data processors operate. It is intended as a practical reference that organisations can apply to their specific circumstances, in a manner consistent with the provisions of the Data Protection Act, 2019.

The Office therefore encourages organisations to consider the role of the DPO as an integral part of their structures, not as an afterthought, but as a deliberate step towards strengthening data protection compliance. It is my hope that this Guidance Note will serve as a useful reference for organisations and DPOs alike, and foster a more deliberate and informed approach to data protection compliance.

Immaculate Kassait, SC, MBS
DATA COMMISSIONER
30th June 2026

INTRODUCTION

The Data Protection Act, Cap 411C (the "Act") under section 24 provides for the designation or appointment of a Data Protection Officer (DPO) on such terms and conditions as may be determined by the data controller or data processor. A data protection officer is responsible for overseeing and ensuring that an organisation's processing of personal data complies with the Act and attendant Regulations. The DPO serves as the central point of contact for all data protection matters within an organisation, ensuring that compliance obligations are understood and effectively implemented.

This guidance note provides organisations with clear guidelines on the appointment or designation, roles, responsibilities and qualifications of DPOs, to enable them to effectively oversee compliance with the Act and attendant Regulations.

This guidance note is applicable across all sectors and to all organisations subject to the Act irrespective of organisational size.

Purpose

The purpose of this Guidance Note is to provide practical guidance on the designation, appointment, positioning, independence, qualifications, roles and responsibilities of Data Protection Officers (DPOs) in accordance with the Data Protection Act, 2019 and the Regulations made thereunder.

The Guidance Note seeks to assist data controllers and data processors in establishing effective data protection governance structures by clarifying the circumstances under which a DPO should be appointed or designated, the competencies expected of a DPO, and the organisational measures necessary to enable the DPO to perform their functions independently and effectively.

The Guidance note further aims to promote a consistent understanding and application of the legal requirements relating to DPOs, strengthen organisational accountability, foster a culture of privacy and compliance, and support the protection of the rights and freedoms of data subjects.

Scope

This Guidance Note applies to all data controllers and data processors, whether public or private, that are subject to the Data Protection Act, 2019. The Guidance Note should be read together with the Data Protection Act, 2019, the Data Protection (General) Regulations, 2021, the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 and any other applicable laws, regulations and guidance issued by the Office of the Data Protection Commissioner relating to the protection of personal data.

POSITION OF THE DPO

Designation/Appointment of a DPO

Section 24(1) of the Act provides that a data controller or data processor may designate or appoint a Data Protection Officer, on 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.

Section 24(6) makes it mandatory for data controllers or data processors to publish the official contact details of the data protection officer on their websites and communicate the same to the Data Commissioner.

Practical examples of organisations required to appoint a DPO include:

Examples of DPO Appointment:

A national hospital processes thousands of patients' health records daily, including laboratory results and medical histories. Because this involves large-scale handling of sensitive health data, the hospital decides that they should designate a DPO.

A telecommunications company handles customer communications, call records, and location data as part of its core operations. The company resolves that this regular and systematic monitoring of individuals requires a DPO.

A digital lending company processes large volumes of financial data, credit histories, and identity documents. Given the sensitivity and scale of processing, the management realizes that they do require to have a DPO.

A county government collecting and managing residents' biometric data for service delivery decides that they should designate a DPO to ensure lawful processing and prevent misuse of citizen data.

Organisational Structure for DPO Role

The designated or appointed DPO may be:

Internal DPO

An internal DPO may be appointed from within the organisation's existing staff or as a new hire, provided that the individual's role allows for 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 be granted sufficient authority and direct access to senior management to effectively perform their duties.

Practical Examples — Internal DPO:

A commercial bank appoints its senior compliance analyst who is not involved in daily transaction processing as an internal DPO, reporting directly to the CEO or for the time being, reporting to the Chief Risk Officer.

A university designates one of its staff, after targeted training as their DPO. The DPO will oversee the handling of student, staff, and research data across multiple departments, ensuring independence from academic and administrative decision-making roles.

A hospital develops a new role for the DPO, complete with appropriate reporting lines and job description and then advertises and hires and fills the position accordingly.

External DPO

A data controller or processor may appoint an external DPO 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. However, such arrangements should be carefully structured to ensure the DPO does not also design or operate the systems, processes or controls they are required to oversee.

Practical Examples — External DPO:

A marketing agency contracts an external DPO consultancy to review its client data processing practices and manage compliance documentation, given that the agency's core staff are focused on creative operations.

A microfinance institution engages a certified privacy consultant on a retainer basis to monitor compliance and handle breach reporting, providing expertise without the cost of a full-time internal role.

A healthcare group, Kikundi Health Group, operating several hospitals across Kenya, engages an external consultancy firm. The firm appoints a staff member with relevant qualifications

as the DPO for Kikundi Health Group. Note: The DPO is the designated individual, not the consultancy firm.

A software startup processing user personal data through a mobile app outsources the DPO function to a specialist firm that conducts quarterly audits and provides policy updates as regulations evolve.

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.

Where the data controller or data processor is a public body, the DPO may be shared among several public bodies, taking into account their organisational structures. In determining whether a shared DPO arrangement is appropriate, public bodies should consider:

- **Size:** Public bodies typically handle higher volumes of personal data and have more complex administrative structures. The scale of data processing across participating entities should be proportionate to the capacity of a single DPO.
- **Complexity of data processing:** Public bodies with diverse mandates, specialised functions, or high-risk processing activities (e.g., health, security, social services) require a DPO with requisite expertise and sector-specific knowledge.
- **Reporting lines:** Clear and direct reporting lines should be established so the shared DPO can communicate effectively with senior management across all participating bodies.
- **Operational independence:** The DPO should be able to act without undue influence from any participating body and should be free from any conflict of interest.

Examples — Shared DPO (Private Sector):

Example 1: Kikundi PLC is a corporate group comprising a parent company and several subsidiaries operating under the same corporate umbrella. Kikundi PLC may appoint a single Group DPO at the parent company level, provided the officer is accessible by each entity within the group.

Example 2: Kikundi Group is a diversified private corporate group whose business lines are highly unrelated and operate independently across different sectors and jurisdictions. In this case, Kikundi Group may not appoint a single DPO across the entities, given the distinct and independent nature of their data processing activities.

Example 3: Several transport service providers collaborate to engage one shared DPO, who coordinates uniform privacy practices, templates, and training programs.

Examples — Shared DPO (Public Sector):

Example 1: A County Government may appoint or designate a single DPO at the county executive level to provide oversight across all County Executive Committee (CEC) departments, on the basis that the County's data processing activities are interrelated.

Example 2: A ministry, such as the Ministry of Information, Communications and the Digital Economy, may not appoint a single DPO to serve all its State Departments and affiliated agencies, as each undertakes distinct and independent data processing activities, often as separate data controllers or processors with differing legal mandates.

Data Protection Committee

A data controller or processor may, where appropriate, establish a Data Protection Committee at the organisational level, composed of senior representatives from key functions, to provide strategic oversight, coordination and governance of data protection matters. Additionally, the data controller or processor may appoint data protection champions within its respective units or departments to support the implementation of data protection requirements at the operational level and to act as focal points for day-to-day compliance.

For the avoidance of doubt, the data protection committee and data protection champions serve distinct but complementary roles within the governance framework: the Committee operates as a collective governance and decision-making body responsible for policy direction, oversight and coordination of data protection compliance across the organisation, while data protection champions are individual officers embedded within departments who facilitate implementation of data protection requirements within their respective departments/functional areas.

Note: *A data protection committee can either be a stand-alone committee, or the roles be incorporated into an existing committee.*

POSITIONING AND INDEPENDENCE OF THE DPO

Independence

The DPO should perform their duties with full independence and professional judgment. This means the DPO should not receive instructions from management or any other person regarding how to carry out their statutory responsibilities, such as conducting audits, issuing compliance advice, or liaising with the ODPC.

Independence ensures that the DPO can objectively assess risks, identify non-compliance, and advise the organisation without fear of interference or reprisal. The organisation shall ensure that:

- the DPO can perform their duties with autonomy and objectivity;
- periodic reviews and assessments are conducted on the DPO's role to guarantee independence in practice;
- management gives due consideration to the DPO's advice and provides adequate resources and support; and
- continuous training and professional development of the DPO is facilitated.

Practical Example — Independence:

A telecommunications company appoints a DPO who reports directly to the Board Audit and Risk Committee rather than to the Head of Operations or IT. When the marketing department proposes using customer call data for targeted advertising, management pressures the DPO to approve the plan quickly. Exercising independence, the DPO declines to authorise the project until a proper DPIA is conducted and lawful consent mechanisms are verified. The Board supports the DPO's position, reinforcing the company's commitment to ethical and compliant data processing.

Reporting Line

The DPO should have a direct reporting line to the highest level of management, such as the Chief Executive Officer, Managing Director, the Board, or the Board Audit and Risk Committee. This reporting structure reinforces the DPO's independence and ensures that 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.

Practical Example — Reporting Line:

A commercial bank structures its governance framework so that the DPO reports directly to the Board Audit and Risk Committee. During a quarterly review, the DPO identifies gaps in third-party data processing agreements that could expose customer information to risk. Because of the direct reporting line, the DPO presents the issue to the Committee, which immediately allocates resources to strengthen contractual safeguards and vendor oversight.

Resources and Support

Organisations should ensure that the DPO is adequately supported with the resources necessary to perform their role effectively. This includes:

- 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 management specialists when required.

Adequate resourcing demonstrates an organisation's genuine commitment to compliance and accountability, enabling the DPO to implement privacy frameworks, conduct audits, and respond to data protection risks in a timely and informed manner.

Practical Example — Resources:

A health insurance agency appoints a DPO to oversee the handling of millions of citizens' medical and identification records. The agency allocates an annual data protection budget that covers DPO remuneration and benefits, privacy management software, staff training, and external audit support. The DPO is also provided with a small compliance team and access to legal and IT specialists when conducting DPIAs. In addition, the organisation funds the DPO's participation in local and international privacy conferences to keep abreast of emerging regulatory and technological developments.

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. Holding such roles may create a conflict of interest, as the individual would be both monitoring and making decisions about data processing activities.

To maintain impartiality, the DPO's function should be clearly separated from operational or decision-making roles that influence how personal data is collected, used, or shared. The role of the DPO should not result in any conflict of interest by holding any position or performing any function within the organisation that influences decisions on data processing activities.

Practical Example — Conflict of Interest:

A manufacturing company initially considers appointing its Head of IT as the DPO, given their strong technical background. However, the IT Head is responsible for deciding how employee and supplier data are collected, stored, and shared functions that directly influence data processing decisions. Recognising the conflict, the company instead appoints a Compliance Officer with no operational control over data systems as the DPO. The IT Head continues to provide technical support, while the DPO independently oversees privacy compliance and audits data handling practices.

Protection and Non-Retaliation

The DPO should not be dismissed, penalised, or otherwise disadvantaged solely for carrying out their statutory duties under the Data Protection Act. Protecting the DPO from retaliation enables them to perform their compliance and advisory functions independently and in good faith, without fear of reprisal. While the DPO provides guidance and oversight, the ultimate responsibility for ensuring compliance with data protection obligations rests with the data controller or data processor. This distinction preserves the DPO's advisory role while affirming that organisational leadership remains accountable for all decisions and actions related to personal data processing.

Practical Example — Non-Retaliation:

A digital lending company appoints a DPO who identifies that the company's mobile app collects more personal data than necessary for credit assessment. The DPO advises management to revise the app's data collection forms and update the privacy notice. Some senior executives initially resist, citing potential business disruption. The Board upholds the DPO's recommendation and reminds management that the DPO cannot be penalised for performing their statutory duties, while management remains responsible for implementing the corrective actions.

ROLES AND RESPONSIBILITIES OF THE DPO

The roles of the data protection officer shall include:

- advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;
- ensure on behalf of the data controller or data processor that this Act is complied with;
- facilitate capacity building of staff involved in data processing operations;
- provide advice on Data Protection Impact Assessment;
- co-operate with the Data Commissioner and any other authority on matters relating to data protection, and
- Ensure that data protection compliance audits are carried out by the data controller or processor.

The DPO plays a pivotal role in ensuring that an organisation upholds the principles and obligations set out in the Act. Acting as the cornerstone of accountability, the DPO provides guidance, oversight, and coordination of all activities related to personal data protection. Their responsibilities encompass both advisory and operational functions aimed at embedding a culture of privacy, monitoring compliance, managing risks, and serving as the primary link between the organisation, data subjects, and the ODPC. In fulfilling this role, the DPO shall, at minimum:

Responsibility	Description
Advise the controller, processor, and staff on obligations under the Act	The DPO should provide continuous guidance to management and employees on their duties under the Data Protection Act and its Regulations. This includes interpreting legal requirements, advising on lawful bases for processing, and ensuring that new initiatives or technologies align with data protection principles from the outset. The DPO should also support the development and periodic review of data protection policies, privacy notices, and consent mechanisms to ensure they are clear, transparent, and compliant with the law.
Monitor compliance with laws, regulations, and internal policies	The DPO should regularly assess the organisation's data protection practices to confirm compliance with applicable laws and internal policies. This involves conducting audits, reviewing how personal data is collected, stored, shared, and retained, and recommending corrective measures where gaps are identified. Monitoring should extend to the organisation's third-party service providers and vendors, ensuring that data processing agreements are in place

	and that processors meet the same compliance standards as the controller.
Advise on and oversee Data Protection Impact Assessments (DPIAs)	The DPO should guide departments in conducting DPIAs for new projects, systems, or initiatives that may pose significant privacy risks. They should ensure that risks are identified early, mitigation measures are implemented, and outcomes are properly documented and reported to management. DPIAs should also assess potential risks arising from cross-border data transfers, vendor integrations, or new digital platforms.
Coordinate breach response and ensure timely notification to the ODPC and affected data subjects	In the event of a personal data breach, the DPO should lead the organisation's incident response process by investigating the cause, assessing its impact, and coordinating both internal and external communications. The DPO should ensure that notifications to the ODPC and affected individuals are made promptly in accordance with legal requirements, and that post-incident reviews are conducted to strengthen prevention and response mechanisms.
Facilitate data subject rights requests and maintain relevant logs	The DPO should establish and oversee efficient procedures for handling data subject requests, such as access, correction, erasure, or objection to processing. They should maintain detailed records of all requests received and ensure that responses are issued within statutory timelines. The DPO should also monitor third-party processors or partners involved in fulfilling these requests to ensure compliance across the data lifecycle.
Co-operate with the ODPC during audits, investigations, and compliance reviews	The DPO serves as the primary liaison between the organisation and the ODPC. They should facilitate access to documents, respond to regulatory enquiries, and provide accurate, timely information to support audits or investigations. This cooperation helps demonstrate transparency, good faith, and a culture of accountability.
Develop and deliver training and awareness programs	The DPO should design and implement regular training programs for employees, management, and third-party partners to build awareness of data protection principles, organisational policies, and emerging risks. These sessions should cover breach reporting procedures, handling of personal data, cross-border transfer safeguards, and vendor compliance management. Regular awareness campaigns reinforce the organisation's privacy culture and reduce the likelihood of violations.

Maintain and update the Record of Processing Activities (ROPA)	The DPO should develop, maintain, and regularly update the organisation's ROPA. This record should capture details of all personal data processed, including the purposes of processing, categories of data subjects, recipients of data, retention periods, and applicable safeguards for cross-border transfers. Keeping an up-to-date ROPA enables the organisation to demonstrate compliance and identify areas requiring additional privacy controls.
Ensure compliance audits are carried out	The DPO should ensure that data protection compliance audits are carried out by or on behalf of the data controller or processor, covering all aspects of the organisation's data processing activities and third-party relationships.
Prepare periodic compliance reports and escalate risks to senior management	The DPO should compile comprehensive periodic and annual reports summarising the organisation's compliance status, risk assessments, DPIA outcomes, and audit findings. These reports should include updates on policy implementation, privacy notices, third-party management outcomes, and cross-border data transfer arrangements. Findings should be presented to senior management or the Board to facilitate informed decision-making and strategic alignment between business objectives and data protection obligations.

COMPETENCE, QUALIFICATIONS AND PROFESSIONAL DEVELOPMENT

The designated or appointed DPO should have the relevant academic or professional qualifications, including knowledge and technical skills in matters relating to data protection. The effectiveness of a DPO depends on their professional competence, relevant qualifications, and commitment to continuous learning.

Given the multidisciplinary nature of data protection, a DPO should possess a blend of legal, technical, and organisational expertise. The technical skills and professional qualifications may include, but are not limited to:

Privacy Governance:

- Knowledge and understanding of the organisation's data processing activities, including the scale, complexity, sensitivity, technical platforms and sector.
- Knowledge of international and regional privacy frameworks.
- Expertise in Kenyan data protection law and practice, including a thorough understanding of the Data Protection Act, its subsidiary regulations, and relevant constitutional provisions on the right to privacy.
- Proficiency in developing privacy documentations such as data protection policies, privacy notices, data breach management policies, consent mechanisms.
- Competence to promote a data protection culture through staff awareness, training, and advisory to the organisation.
- Excellent communication and advisory skills across technical and legal contexts, enabling effective engagement with IT teams, management, regulators, and data subjects.
- Commitment to continuous professional development, including staying informed about emerging technologies and evolving data protection trends.

Privacy Risk Management & Compliance:

- Ability to interpret and apply legal and regulatory requirements to operational technical contexts, ensuring that organisational processes, contracts, and that technical, and administrative systems align with data protection obligations.

- Knowledge of sector-specific privacy compliance frameworks, including those governing finance, healthcare, education, telecommunications, insurance, public administration, e-commerce amongst others.

- Knowledge and understanding of information technologies, privacy enhancing & engineering technologies, data security for both digital and manual processes as well as cybersecurity principles.

- Experience in executing privacy /compliance audits, developing data maps(RoPA), including conducting internal privacy assessments & audits, developing privacy impact assessments, risk registers, and implementing corrective action plans.

- Knowledge of cross-border data transfer mechanisms and safeguards, such as Standard Contractual Clauses, adequacy assessments, and ODPC authorisation requirements.
- Practical understanding of third-party and vendor management, including drafting and reviewing data processing agreements and conducting due diligence on processors.
- Knowledge and ability to develop, budget, implement, monitor and regularly report on the effectiveness a privacy program
- Analytical and problem-solving abilities, particularly in identifying data protection risks and proposing practical, lawful and technical (privacy by design) solutions.

Professional Certification

Local and international certifications are strongly encouraged. Such certifications demonstrate a commitment to professional standards and provide assurance of the DPO's competence to both the organisation and the ODPC.

Continuous Professional Development (CPD)

Data Protection Officers (DPOs) are encouraged to undertake periodic refresher training and continuous professional development activities to maintain up-to-date knowledge of data protection laws, regulatory developments, emerging technologies, privacy by design techniques as well as best practices.

REMUNERATION GUIDANCE FOR DATA PROTECTION OFFICERS

The remuneration of a DPO should reflect the complexity, scope, and strategic importance of the role within an organisation. Since the DPO is responsible for ensuring compliance with the Data Protection Act, advising on high-risk processing, managing privacy risks, and liaising with the regulator, the position should be compensated in a manner that attracts and retains qualified professionals while maintaining independence and accountability.

Organisations should consider the following factors when setting remuneration for the DPO:

- **Organisational size and nature of operations:** The scale and complexity of an organisation's data processing activities.
- **Scope of responsibility and risk exposure:** That the DPO's responsibilities may include oversight of multiple departments, subsidiaries, or third-party processors.
- **Professional experience and qualifications:** Account for the DPO's academic background, professional certifications and practical experience in data protection, information security, legal compliance, or risk management.
- **Market benchmarks and sector standards:** Organisations should use relevant market data and industry benchmarks to ensure DPO compensation remains competitive and aligned with comparable governance or compliance roles.

Independence and non-conflict of interest: The DPO's compensation structure should not compromise their independence

For the public sector, the Public Service Commission (PSC) will provide the DPO career guidelines while the Salaries and Remuneration Commission (SRC) will set the remuneration.

PUBLISHING DPO 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 platforms through which data subjects may seek to exercise their rights or obtain information about the organisation's data processing activities.

In addition, the organisation shall communicate the designated or appointed DPO's details to the Data Commissioner using the prescribed DPO Contact Submission Form. ***(see Annexure 1)***

The DPO's published contact details may include but not limited to: full name, mailing address, dedicated telephone number, and official email address.

Note:

While it can be considered good practice, the published contact information need not contain the DPO's personal data. An organisation may, for example, publish a dedicated role-based email address (e.g. dpo@xxxx.xx.ke), rather than personal contact details provided the data subjects are able to reach the DPO without any difficulties.

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.

The ODPC calls upon all data controllers, processors, and public institutions to adopt this Guidance Note, empower their DPOs, and foster a culture of privacy by design and accountability by default.

Annexure 1 – DPO Contact Submission Form

Organisation Name	
ODPC Registration Number	
Sector	
Type of Entity	☐ Public Entity ☐ Private Entity
DPO Full Name	
DPO Job Title	
DPO Type	☐ Internal ☐ External ☐ Shared
Date of Appointment/Designation	
Official Email Address	
Telephone Number	

Completed forms should be submitted to:

The Office of the Data Protection Commissioner
Britam Towers, 12th Floor
P.O. Box 30920 – 00100
NAIROBI.

Or through email: registration@odpc.go.ke