



Legal Alert

September 2026

Guidance Note on the appointment, roles and responsibilities of Data Protection Officers

This legal alert highlights the key provisions of the Guidance Note and the practical considerations that data controllers and data processors should be aware of when implementing the requirements.

Introduction

The Office of the Data Protection Commissioner (“ODPC”) recently issued the Guidance Note for Data Protection Officers (“DPOs”) 2026 (the “Guidance Note”) on 30 June 2026.

The Guidance Note has been developed in response to challenges observed across the public and private sectors, including instances where DPOs have been appointed without clearly defined responsibilities, appropriate reporting lines, institutional independence, or the resources necessary to effectively discharge their functions in line with the Data Protection Act (Chapter 411C, Laws of Kenya) (the “Act”) and the Data Protection (General) Regulations, 2021 (the “Regulations”) issued under the Act.

Highlights of the Guidance Note

This legal alert highlights the key provisions of the Guidance Note and the practical considerations that data controllers and data processors should be aware of when implementing the requirements.

1. Legal Status and Enforcement Relevance

The Guidance Note is not a statutory instrument and does not create obligations beyond those imposed by the Act and the Regulations. However, it sets out the ODPC’s supervisory expectations and is likely to inform



the benchmark applied in audits, investigations and enforcement action. Organisations should therefore treat it as an important compliance reference while distinguishing its recommendations from binding statutory requirements.

From an international compliance perspective, the ODPC's approach broadly aligns with the GDPR framework. However, the Guidance Note places additional emphasis on expertise in Kenyan data protection law and regulatory practice.

Organisations with an existing GDPR-compliant DPO framework should therefore treat it as a useful foundation, but undertake a Kenya-specific assessment and implement any necessary local adjustments.

2. Scope of Application

The Guidance Note applies to all data controllers and data processors subject to the Act irrespective of sector or organisational size. It should be read together with the Act, the Regulations, the Data Protection (Registration of Data Controllers and

Data Processors) Regulations 2021 and other applicable guidance issued by the ODPC.

3. Roles and responsibilities of the DPO

While the Act already prescribes the core functions of a DPO, the Guidance Note provides additional clarity on the scope of the role by including the following:

- a) advising the data controller or data processor and its employees on data processing requirements under the Act or other written law,
- b) ensuring compliance with the Act on the entity's behalf,
- c) facilitating capacity building of staff involved in data processing,
- d) advising on Data Protection Impact Assessments,
- e) cooperating with the Data Commissioner and other authorities, and
- f) ensuring that data protection compliance audits are carried out.

Organisations should assess not only the volume of personal data processed, but also the nature, sensitivity and monitoring activities associated with their processing operations when determining whether a DPO should be designated.

Organisations should ensure their DPO's job description and operational mandate reflect the full scope of these responsibilities. Where a DPO lacks the necessary mandate or organisational support, the organisation may face challenges demonstrating compliance with the accountability and governance requirements under the Act, increasing its exposure to regulatory investigations, enforcement notices and administrative fines.

4. Clarification on when a DPO should be appointed

The Act provides for the designation or appointment of a DPO by a data controller or data processor. The Guidance Note clarifies that a DPO should be appointed where processing is carried out by a public or private body, where core activities require regular and systematic monitoring of data subjects, or where core activities involve the processing of sensitive categories of personal data.

Organisations should therefore reassess whether their processing activities trigger the need for a designated DPO taking into account the nature, scope and sensitivity of their processing activities, including whether they conduct regular and systematic monitoring or process sensitive personal data.

The ODPC cites examples including hospitals processing sensitive health data, telecommunications operators undertaking regular and systematic monitoring of customer activity, digital lenders processing large volumes of financial and identity data, and county governments managing biometric information.

These examples indicate that organisations should assess not only the volume of personal data processed, but also the nature, sensitivity and monitoring activities associated with their processing operations when determining whether a DPO should be designated.





5. Recognition of internal, external and shared DPO models

The Guidance Note recognises that a DPO may be appointed internally, externally, or on a shared basis within an appropriate group structure. This provides flexibility for businesses that may not require or be able to maintain a full-time internal privacy function.

An internal DPO, appointed from existing staff or as a new hire, should not hold any position determining the purposes or means of processing and should be granted sufficient authority and direct access to senior management.

For example, a university may appoint a trained staff member as its DPO to oversee compliance across departments. However, the individual should not hold a role that determines how student, staff, or research data is collected, used, or shared, thereby preserving the DPO's independence and avoiding conflicts of interest.

An external DPO, engaged where the organisation lacks in-house

expertise, must be appointed under an arrangement ensuring that the external provider does not also design or operate the systems, processes, or controls it is engaged to oversee, and the designated individual (not the consultancy firm itself) is the DPO.

Appointment of an external DPO does not transfer the data controller's or data processor's statutory accountability to the service provider. The engagement should therefore allocate responsibilities and address service standards, regulatory cooperation, incident escalation, indemnities, limitations of liability and evidence of appropriate professional indemnity insurance. The Guidance Note does not establish a separate personal liability regime for the designated individual; any personal regulatory exposure will depend on the applicable statutory provisions and the individual's conduct.

A shared DPO may serve a group of entities or, for public bodies, several public bodies, provided the shared officer has the capacity, expertise, and resources to serve each entity effectively and remains accessible to all data subjects; a shared arrangement is only appropriate where the participating entities' processing activities are sufficiently interrelated, and for public bodies, organisations should weigh institutional size, the complexity of data processing, reporting lines, and operational independence.

The Guidance Note is particularly relevant to multinational groups that operate centralised privacy functions across multiple jurisdictions. The Guidance Note does not expressly require the DPO to be resident in Kenya. Accordingly, a regional or group DPO based outside Kenya may support a Kenyan entity,



provided the arrangement ensures effective accessibility to data subjects, sufficient capacity and resources, independence, effective engagement with the ODPC and demonstrable expertise in Kenyan data protection law and regulatory practice.

Multinational organisations should also recognise that DPO requirements differ across jurisdictions. A group DPO structure designed to comply with the European Union's General Data Protection Regulation, South Africa's Protection of Personal Information Act or Nigeria's Data Protection Act may provide a useful foundation but should not be treated as automatically sufficient for Kenya.

Organisations should undertake and document a Kenya-specific gap assessment and establish appropriate local support, training and escalation arrangements where the group DPO does not possess sufficient Kenya-specific capability.

The Guidance Note's emphasis on knowledge of Kenyan law and encouragement of local and international professional certifications does not, by itself, impose a residency requirement or mandate the appointment of a locally based DPO.

Additionally, the Guidance Note makes clear that any DPO arrangement must preserve independence, accessibility, competence and absence of conflict. Organisations should carefully evaluate which model best fits their operational structure

and document the rationale for the arrangement chosen in internal governance records, such as board, management, or compliance committee minutes.

6. Independence, reporting lines and conflict management

The Guidance Note places emphasis on the independence of the DPO. The DPO should exercise professional judgment without receiving instructions on how to perform statutory responsibilities such as audits, compliance advice or engagement with the ODPC.

Additionally, the DPO should have a direct reporting line to the highest level of management, including the Chief Executive Officer, Managing Director, Board, or Board Audit and Risk Committee.

Organisations should confirm that their DPO has a clear mandate, sufficient authority and direct access to senior management or the Board. Existing reporting lines may need to be revised where the DPO currently reports through functions that could impair independence.

Depending on the organisation's existing governance framework, implementation could require amendments to board and committee charters, revisions to committee mandates and governance policies, updates to delegated-authority and escalation frameworks, and the inclusion of material data protection matters as standing agenda items for the relevant board or committee.

A shared DPO may serve a group of entities or, for public bodies, several public bodies, provided the shared officer has the capacity, expertise, and resources to serve each entity effectively and remains accessible to all data subjects.

Public sector organisations should note that the Public Service Commission will provide DPO career guidelines while the Salaries and Remuneration Commission will set remuneration.

Organisations should also establish a clear mechanism through which the DPO can escalate significant data protection risks directly to the appropriate governance body without prior operational approval.

These arrangements should be documented in the DPO's terms of reference or appointment instrument and, where applicable, the relevant board or committee charter, governance manual and reporting protocol.

The Guidance Note also warns against appointing individuals whose operational roles determine the purposes or means of processing personal data, such as heads of IT, human resources, legal or compliance, where this would create a conflict of interest.

This requirement also presents practical challenges for regulated entities, particularly within the banking, insurance, telecommunications and capital markets sectors, where individuals frequently perform multiple compliance, risk management or governance functions.

The relevant consideration is whether another role enables the individual to determine the purposes or means of processing personal data that the same individual is expected to oversee independently.

Where responsibilities overlap, organisations should conduct and document a conflict-of-interest assessment, establish appropriate segregation between operational decision-making and oversight functions, and implement independent escalation and reporting mechanisms. Where such conflicts cannot be effectively managed,

organisations should appoint a separate DPO.

7. Competence, professional development and remuneration

The Guidance Note sets out the ODPC's expectations on the competence of DPOs, including knowledge of Kenyan data protection law, privacy governance, information security, cybersecurity principles, cross-border data transfer requirements, vendor management and privacy risk assessments.

Local and international professional certifications are strongly encouraged, together with continuous professional development. The Guidance Note also states that remuneration should reflect the complexity, scope and strategic importance of the DPO role, and should not undermine the DPO's independence.

Public sector organisations should note that the Public Service Commission will provide DPO career guidelines while the Salaries and Remuneration Commission will set remuneration.

As organisations, particularly in the financial services and telecommunications sectors, deploy artificial intelligence, profiling and automated decision-making systems, the DPO's advisory and impact-assessment role will require sufficient understanding of the associated data flows, risks, safeguards and vendor arrangements.

Organisations should therefore provide targeted training and budget for specialist technical support where these capabilities are not available internally.

The Guidance Note also states that remuneration should reflect the complexity, scope and strategic importance of the DPO role, and should not undermine the DPO's independence.

Data controllers and processors are required to publish the official contact details of their DPO on their websites or other appropriate platforms and communicate the same to the Data Commissioner.

Organisations also should review whether their DPO has the appropriate legal, technical and governance expertise to meet the ODPC's expectations.

This may require updating the DPO role profile, investing in professional certifications and continuous training, and ensuring that remuneration reflects the complexity and strategic importance of the role while preserving the DPO's independence.

Public sector entities should also monitor the forthcoming career and remuneration guidance from the Public Service Commission and the Salaries and Remuneration Commission.

8. Provision of resources and support

Organisations must ensure the DPO is adequately resourced to perform their role effectively, including through a dedicated budget for data protection activities, sufficient staffing or technical support, continuous professional

training, and access to legal, information technology (IT), and risk management specialists where required.

Organisations should therefore budget for privacy governance as part of their wider compliance and risk management programmes.

9. Publication and notification of DPO contact details

Data controllers and processors are required to publish the official contact details of their DPO on their websites or other appropriate platforms and communicate the same to the Data Commissioner.

The Guidance Note confirms that organisations may use dedicated role-based contact details, such as a DPO email address, provided data subjects are able to reach the DPO without difficulty.

The Guidance Note also includes a DPO Contact Submission Form for notifying the ODPC of the appointed or designated DPO's details.



The DPO should not be dismissed, penalised, or otherwise disadvantaged solely for performing their statutory duties under the Act.



Businesses should ensure that DPO contact details are published through appropriate channels and submitted to the ODPC using the prescribed contact submission process.

10. Protection and non-retaliation

The DPO should not be dismissed, penalised, or otherwise disadvantaged solely for performing their statutory duties under the Act. While the DPO provides guidance and oversight, ultimate responsibility for data protection compliance remains with the data controller or data processor, and organisations should put in place safeguards to ensure the DPO can exercise independent judgment without fear of reprisal.

Organisations should ensure that the DPO's appointment terms, reporting lines and internal policies expressly protect the DPO from dismissal, penalties or adverse treatment arising from the proper discharge of statutory duties.

Businesses should also clarify that accountability for data protection compliance remains with the organisation, while enabling the DPO to provide independent oversight and advice without undue influence or fear of reprisal.

11. Timing and implementation approach

The Guidance Note does not prescribe a transition period. Accordingly, no particular implementation period should be treated as a requirement of the Guidance Note. As a practical governance measure, organisations may structure their review in stages by assessing existing DPO arrangements, identifying and prioritising any areas requiring adjustment, assigning responsibility for agreed measures, and recording target dates appropriate to their circumstances.

The review, decisions taken and progress against the resulting internal roadmap should be documented, including the rationale for any phased measures, having regard to the organisation's processing activities, governance structure and applicable obligations under the Act and the Regulations.



Contact us

Titus Mukora

Partner,
Legal Business Solutions
+254 20 285 5000
titus.mukora@pwc.com

Caroline Wanja

Associate Director,
Legal Business Solutions
+254 20 285 5000
caroline.wanja@pwc.com

Herbert Njoroge

Senior Manager,
Legal Business Solutions
+254 20 285 5000
herbert.njoroge@pwc.com

Jackline Mongare

Senior Associate,
Legal Business Solutions
+254 20 285 5000
jackline.mongare@pwc.com

www.pwc.com/ke

The material on this alert is for general information purposes only and does not constitute legal advice. While reasonable care is taken to ensure accuracy, the material may not reflect the most current legal developments. PwC disclaims liability for actions taken based on the material. Always consult a qualified lawyer for specific legal matters.

© 2026 PricewaterhouseCoopers Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Limited which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.