OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE ON DATA PROTECTION OFFICER

TABLE OF CONTENTS

1. Definitions....3
2. Introduction....6
3. Position of the DPO....7
3.1 Designation/Appointment of a DPO....7
3.1.1 Data Protection Committee....9
3.2 Roles and Responsibilities of the DPO....9
3.3 Qualifications (Skills and Professional Qualifications)....10
3.4 DPO Reporting structure....10
4. Publishing DPO Contacts....12

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.

"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

DPO	Data Protection Officer
ODPC	Office of the Data Protection Commissioner

1. Introduction

The Data Protection Act, 2019 (the "Act") under section 24 provides for 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 applicable Regulations and serves as a central point of contact for data protection matters, 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, enabling them to effectively oversee compliance with the Act and attendant Regulations.

This guidance note is applicable across all sectors irrespective of the organisational size.

2. Position of the DPO

2.1 Designation/Appointment of a DPO

Section 24 (1) of the Act provides for the designation or appointment of a Data Protection Officer by a data controller or processor on terms they determine if:

a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;
b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects; or
c) the core activities of the data controller or the data processor consists of processing sensitive categories of personal data.

The designated or appointed DPO may be:

a) A staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest;
b) Shared by a group of entities (refer to definition), provided that such officer is accessible by each entity;

Example 1:
A corporate group, Kikundi PLC and its subsidiaries and affiliated entities (including digital financial and technology-related subsidiaries operating under the same corporate umbrella) may appoint/designate a single Group Data Protection Officer (DPO) at the parent company level provided the officer is accessible by each entity.

Example 2
Kikundi Group is a diversified private corporate group operating under a single holding company structure with full ownership of its subsidiaries. However, its business lines are highly unrelated and operate independently across different sectors and jurisdictions. In this case Kikundi group cannot appoint/designate a single DPO.

c) Shared among several public bodies where the data controller or a data processor is a public body, taking into account their organisational structures. The shared DPO arrangement among public bodies must consider:

   i) size of the institutions;
   ii) complexity of data processing;
   iii) reporting lines; and
   iv) operational independence.

Example 1:
A County Government may appoint or designate a single Data Protection Officer (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 or designate a single Data Protection Officer (DPO) to serve all its State Departments and affiliated agencies, as each entity undertakes distinct and independent data processing activities, often as separate data controllers or processors with differing legal mandates and operational contexts.

d) A data controller or processor may appoint/designate an outsourced/external Data Protection Officer (DPO) to support compliance, provided the DPO remains independent, accessible, qualified and has no conflicts of interest while performing their duties. The external/outsourced model is suitable where an organisation lacks in-house expertise or needs independent oversight, but it must be carefully structured, so the DPO does not also design or operate the systems they are meant to oversee.

Example

A healthcare group, "Kikundi Health Group," operating several hospitals across Kenya, may appoint/designate an external privacy consultancy as its group DPO. The consultant advises all hospitals on compliance with the Data Protection Act, reviews DPIAs for new electronic medical record systems, trains hospital staff on handling patient data, and reports directly to the group board. However, the same consultancy

is not allowed to implement the hospital's IT systems or manage its cybersecurity operations, ensuring independence and avoiding conflicts of interest.

Data Protection Committee

A data controller or processor may 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.

In addition, the data controller 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: 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 at the operational level, support awareness and compliance activities within their units, and escalate issues to the Committee or the Data Protection Officer as appropriate.

2.2 Roles and Responsibilities of the DPO

The roles of the data protection officer shall include:

a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;
b) ensure on behalf of the data controller or data processor that this Act is complied with;
c) facilitate capacity building of staff involved in data processing operations;
d) provide advice on Data Protection Impact Assessment; and

e) co-operate with the Data Commissioner and any other authority on matters relating to data protection.

2.3 Skills and Professional Qualifications

The designated or appointed data protection officer should have the relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

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

i) Knowledge and understanding of the organisation's data processing activities, including the scale, complexity, sensitivity and sector;
ii) Knowledge in the national data protection laws and practices;
iii) Knowledge and understanding of information technologies and data security for both digital and manual processes.
iv) Competence to promote a data protection culture through staff awareness, training and advisory to the organisation.

2.4 DPO Reporting structure

The DPO should hold a position that allows them to operate effectively at strategic, technical, and operational levels. The role may be integrated within the organisation's governance, risk and compliance structures, ideally reporting directly to the appointing authority or senior management.

The organisation shall ensure that:

i. The DPO is able to perform their duties with autonomy and objectivity. Independence is essential to ensure impartial advice and oversight in the best interests of the organisation and data subjects.
ii. Management acts on the DPO's advice and provides adequate resources and support, where necessary.
iii. Continuous training and professional development of the DPO.

iv. The role of the DPO does 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.

3. Publishing DPO Contacts

The data controller or data processor shall publish the contact details of the data protection officer on their website. The organisation shall communicate the designated or appointed DPO's details to the Data Commissioner.

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

While it can be considered good practice, the published contact information does not have to contain the DPO's personal data.