Finnet
Building a Better Tomorrow, Today

CYBER RESILIENCE & DATA PRIVACY

Pension Strategy Formulation Excellence & Innovation Driven Transformation

PRESENTATION OBJECTIVES

Objective 1

To understand data privacy obligations for pension schemes under the Data Protection Act (DPA-K).

Objective 2

To learn how to strengthen cyber resilience and protect member data effectively against breaches and threats.

Finnet
Building a Better Tomorrow, Today

REGULATORY FRAMEWORK

Constitutional Anchor

The Constitution of Kenya 2010

Article 31 — Guarantees the fundamental Right to Privacy.

Primary Statute

The Data Protection Act, 2019

Enacted to enforce and regulate privacy rights.

THE DATA PROTECTION ACT, 2019

The Data Protection Act, 2019, was assented into law on **8th November 2019** and commenced on **25th November 2019**.

Purpose of the Act: First, to establish the Office of the Data Protection Commissioner (ODPC); to make provisions and regulation for processing personal data; to provide for the rights of data subjects and obligations of data controllers and processors.

WHAT IS THE DPA & ITS PURPOSE?

Finnet
Building a Better Tomorrow, Today

It is a law governing the processing of personal data, anchored on Article 31 of the Constitution that guarantees the right to privacy.

The Act seeks to govern:

How personal data is used by private and public entities

The rights of data subjects (in this case, the Scheme's Members)

The legal justification for processing personal data of clients and employees

The precautions that handlers of personal data must observe when handling data

Finnet
Building a Better Tomorrow, Today

KEY CONCEPTS UNDER DPA

Definition

Personal Data

Data that identifies an individual (data subject) either directly or indirectly such as a person's name, address, telephone number, email, ID number, location data, online address, e.t.c.

Special Category

Sensitive Personal Data

Data revealing race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of children, parents, spouse(s), sex or sexual orientation.

Data Controllers (DC) & Processors (DP)

Rights of Data Subject (Sec. 26)

Consent Requirement (Sec. 32)

Finnet
Building a Better Tomorrow, Today

PROCESSING OF DATA

What is "Processing"?

Processing means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means.

Collection & Structuring
Collection, recording, organisation, structuring

Storage & Alteration
Storage, amending or alteration

Retrieval & Use
Retrieval, consultation or use

Disclosure & Sharing
Disclosure by transmission, dissemination, sharing

Erasure & Destruction
Alignment, combination, restriction, erasure

Finnet
Building a Better Tomorrow, Today

DATA PROCESSING PRINCIPLES (SEC. 25)

Principle 1

Right to Privacy

Processed in accordance with the right to privacy of the data subject.

Principle 2

Lawfulness, Fairness & Transparency

Processed lawfully, fairly and in a transparent manner in relation to any data subject.

Principle 3

Purpose Limitation

Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.

Principle 4

Data Minimisation

Adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed.

Finnet
Building a Better Tomorrow, Today

DATA PROCESSING PRINCIPLES (SEC. 25 CONT'D)

Principle 5

Valid Explanation

Collected only where a valid explanation is provided whenever information relating to family or private affairs is required.

Principle 6

Accuracy & Rectification

Accurate and, where necessary, kept up to date, with every reasonable step taken to ensure inaccurate data is erased or rectified without delay.

Principle 7

Storage Limitation

Kept in a form which identifies data subjects for no longer than is necessary for the purposes for which it was collected.

Principle 8

Cross-Border Transfer Safeguards

Not transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

SCHEME TRUSTEES: CONTROLLERS & PROCESSORS

Role 1

Scheme Trustees as DATA CONTROLLERS

Determine the purpose of collection and means of processing Members' Personal data.

Role 2

Scheme Trustees as DATA PROCESSORS

Trustees are data processors through their operative functions of collection of Member's personal data.

Data Processors can also be persons/entities to whom Trustees have outsourced data processing roles (e.g., Administrators and Custodians).

Parties in a contractual relationship with Trustees granted access to Members' personal data are also data processors:

- a) Administrators
- b) Actuaries

Finnet
Building a Better Tomorrow, Today

DATA PROTECTION OFFICER & COMPLIANCE ROADMAP

Sec. 24 DPA

Data Protection Officer (DPO)

A DPO is a person appointed by a DC or DP to ensure personal data is handled in compliance with the DPA.

The DPA stipulates that where core activities involve regular and systematic monitoring of data subjects, or processing of sensitive personal data, a DPO may be appointed.

Action Plan

Roadmap to Compliance

1. Registration of BOTs as DCs & DPs

Boards of Trustees are required to register as Data Controllers and/or Data Processors with the ODPC.

2. Policy Promulgation

Promulgate Policies to ensure full operational compliance with the DPA.

SCHEME IMPACT & COMPLIANCE REQUIREMENTS

How Might DPA Affect Your Scheme?

Schemes should review how Members' personal data is handled:

- How is personal data handled?
- Which personal data or sensitive personal data is collected and for what purpose?
- What is the Scheme's response mechanism/procedure to a complaint of data breach?
- What is the retention period of personal data collected by the Scheme?

Compliance Documentation & Actions

- Data Protection Policy
- Data Privacy Statement/Policy & Info Security Policy
- Review Scheme forms (onboarding, Beneficiary nomination forms)
- Appoint a Data Protection Officer (single DPO allowed for group entities if accessible)
- Undertake Data Protection Impact Assessment (DPIA) prior to high-risk processing operations

PENALTIES & INFRINGEMENT CONSEQUENCES

Sec. 58 Offence

Enforcement Notice Non-Compliance

Failure to comply with an enforcement notice from the DC is an offence liable upon conviction to a fine not exceeding **KES 5 Million** or imprisonment for **2 years**, or both.

Sec. 63 Penalty

Administrative Fines

Data Commissioner may impose a maximum penalty of **KES 5 Million**, or up to **1% of annual turnover** of the preceding financial year, whichever is lower.

Real Enforcement Precedents & Right of Appeal

Precedents: Oppo was the 1st company fined 5M in Dec 2022 for failure to comply with an enforcement notice. Whitepath Co. Ltd and Regus Limited were both fined 5M in April 2023.

Right of Appeal (Sec. 64): Right of Appeal to the High Court against enforcement or penalty notices.

CASE STUDIES & SECTOR VULNERABILITIES

ODPC Complaint 0586/2023

Harrison Kisaka v Faulu Microfinance Bank

Facts: Harrison interviewed for a job, consented to background check. Bank withdrew offer & refused to release background check report.

Determination: Complainant's right to personal data was violated.

Unlawful Processing Case

Eric Munene v Chapeo Capital & Okota

Facts: Listed as loan guarantor without knowledge. Personal data disclosed to lender without verification or consent.

Determination: Constituted Sec 72 offence; recommended prosecution.

Complaints by Sector — Report by DPGSK

Finance & credit institutions accounted for the largest share of ODPC penalties due to handling high volumes of sensitive personal data.

Pension Schemes Takeaway: Pension schemes similarly handle large volumes of member data and must prioritize robust safeguards, consent management, and oversight to reduce breach exposure and regulatory risk.

CYBER RESILIENCE — LEGAL PILLAR

CMCA 2018

Computer Misuse & Cybercrimes Act

Purpose: To detect, prevent, and prosecute cybercrimes including hacking, identity theft, and data interference.

Key Relevant Offenses

- **Unauthorized Access (Sec. 14):** Criminalizes gaining system access without permission.
- **Unauthorized Interference (Sec. 16):** Addresses malicious deletion, alteration, or suppression of data.
- **Cyber Extortion (Sec. 24):** Targets ransomware attacks demanding payment.

Interplay & Duty of Care

While DPA 2019 protects member privacy, CMCA 2018 provides tools to prosecute criminals. Organizations must report cybercrimes to NC4 in addition to ODPC breach reporting.

Finnet
Building a Better Tomorrow, Today

CYBER RESILIENCE: DEFINITION & PILLARS

Definition

What is Cyber Resilience?

The ability of an entity to continuously deliver the intended outcome, despite adverse cyber events.

Distinction

Cybersecurity vs. Resilience

Cybersecurity aims to keep threats out. Cyber Resilience assumes no defense is perfect, focusing on how an organization survives an attack and continues operations.

The Four Pillars of Resilience

1. Anticipate

Predicting & preparing for potential threats before they occur.

2. Withstand

Absorbing breach impact to maintain critical business functions.

3. Recover

Restoring systems and data quickly after a disruption.

4. Adapt

Learning from incidents to improve future security posture.

Finnet
Building a Better Tomorrow, Today

TECHNICAL MEASURES FOR CYBER RESILIENCE

Zero Trust Architecture

A "never trust, always verify" model requiring strict identification and verification for every user and device.

Identity & Access Management

Implementing Least Privilege, ensuring staff only access specific member data required for their role.

Data Integrity Controls

Utilizing digital signatures and hashing to ensure pension records have not been secretly altered.

Endpoint Detection and Response (EDR)

AI-driven monitoring of all devices (laptops, servers) to detect and stop suspicious behavior in real-time.

Redundancy & Failover

Maintaining "Immutable Backups" in separate geographic locations for immediate recovery after ransomware attacks.

Finnet
Building a Better Tomorrow, Today

ORGANIZATIONAL MEASURES: GOVERNANCE & PEOPLE

BCP

Business Continuity Planning

Comprehensive strategy ensuring the whole organization knows how to operate manually if digital systems go down.

Supply Chain

Supply Chain Risk Management

Actively auditing the security & resilience of third-party service providers (Administrators, Custodians) handling member data.

Crisis Governance

Establishing clear chain of command for instant crisis decisions.

Cyber Hygiene Culture

Making every employee a "human firewall" through regular phishing simulations.

Post-Incident Analysis

Conducting "Lessons Learned" sessions to update Information Security Policies.

THANK YOU FOR LISTENING

Questions & Answers Session

Thank You

ADDRESS

5th Floor, Crescent Business Centre (CBC), Parklands.
P.O. Box 48179-00100, GPO Nairobi, Kenya

CALL US

+254 719 560656, +254 740 257777, +254 111052230

WEB & SOCIAL

www.finnettrust.com | Facebook/LinkedIn: Finnet Trust