SecureZaidi
CYBERSECURITY & COMPLIANCE

COMPLIANCE GUIDE 01 / 04

The Kenya Data Protection Act Compliance Guide

A comprehensive guide for organisations operating in Kenya — covering ODPC registration, lawful bases, data subject rights, breach notification, and enforcement.

Produced by	SecureZaidi Limited
Website	securezaidi.com
Email	info@securezaidi.com
Phone	+254 700 000 000
Edition	2026 Edition — For East African Organisations

This guide is produced for educational and informational purposes and does not constitute legal advice. For a tailored compliance assessment, contact SecureZaidi.

Contents

1. Introduction

The Kenya Data Protection Act 2019 (DPA) is the primary legislation governing the collection, processing, storage, use, and disclosure of personal data in Kenya. Enacted on 8 November 2019 and operationalised through the Data Protection (General) Regulations 2021, the Act establishes enforceable rights for individuals and binding obligations for any organisation that handles their personal data.

Modelled closely on the European Union's General Data Protection Regulation (GDPR), the Kenya DPA represents a significant shift in the country's data governance landscape. Non-compliance exposes organisations to regulatory investigation, enforcement notices, and financial penalties of up to KES 5 million or 1% of annual turnover — whichever is higher — as well as serious reputational damage.

This guide provides a practical walkthrough of the Act's key requirements, designed for compliance managers, legal teams, IT leaders, and business owners operating in Kenya. It covers every major obligation and explains what each means in practice for your organisation.

2. Scope and Applicability

The Kenya DPA applies broadly to any person or organisation — whether public or private, Kenyan or foreign — that:

- Collects, stores, processes, uses, or discloses personal data about an individual located in Kenya;
- Offers goods or services to individuals in Kenya, even if operating from outside the country; or
- Monitors the behaviour of individuals who are in Kenya.

This means a foreign company with no physical presence in Kenya may still be subject to the Act if it processes data of Kenyan residents. Small businesses, NGOs, fintech startups, multinationals, and government agencies are all covered.

Practical implication	If your organisation collects names, email addresses, phone numbers, financial details, health information, or any other information that can identify a living individual — you are subject to the Kenya DPA.

3. Key Definitions

Understanding these definitions is foundational to compliance:

Term	Definition

Personal Data	Any information relating to an identified or identifiable natural person — including name, ID number, location data, IP address, and any factors specific to that person's identity.
Data Controller	The person or organisation that determines the purposes and means of processing personal data. Must register with the ODPC.
Data Processor	A person or organisation that processes personal data on behalf of a data controller (e.g. cloud provider, payroll bureau, marketing platform). Must also register.
Processing	Any operation performed on personal data — including collection, recording, storage, adaptation, retrieval, use, disclosure, erasure, or destruction.
Data Subject	The identified or identifiable individual to whom the personal data relates.
Consent	A freely given, specific, informed, and unambiguous indication by which a data subject agrees to their personal data being processed.
Sensitive Personal Data	A special category of data requiring heightened protection: race, health, genetic, biometric, sex life, religious beliefs, criminal records, financial data, and data of minors.
ODPC	Office of the Data Protection Commissioner — the regulatory authority responsible for enforcing the Kenya DPA.

4. ODPC Registration

Both data controllers and data processors operating in Kenya are required to register with the Office of the Data Protection Commissioner (ODPC). This is a legal obligation — not optional — and failure to register is itself an offence under the Act.

Who must register?

- All data controllers processing personal data of Kenyan residents.
- All data processors processing on behalf of Kenyan-regulated controllers.
- Foreign organisations processing data of individuals in Kenya.

How to register

Registration is completed online through the ODPC portal (www.odpc.go.ke). Applicants must provide details about their organisation, the categories of personal data processed, the purposes of processing, data flows, and security measures in place. Certificates of registration are renewed annually.

Registration fees (2024)	Individual/sole trader: KES 2,000. Small entity (under KES 5M revenue): KES 5,000. Medium entity: KES 10,000. Large entity (over KES 500M revenue): KES 50,000.

5. Lawful Bases for Processing Personal Data

You may only process personal data if you have a lawful basis. The Kenya DPA recognises the following bases:

Basis	When it applies
Consent	The data subject has given freely given, specific, informed, and unambiguous consent. Must be as easy to withdraw as to give.
Contract	Processing is necessary for the performance of a contract with the data subject, or to take pre-contractual steps at their request.
Legal obligation	Processing is required to comply with a legal requirement binding on the controller (e.g. KRA tax records, employment law).
Vital interests	Processing is necessary to protect the vital interests (life or safety) of the data subject or another person.
Public task	Processing is necessary for the performance of a task in the public interest or in the exercise of official authority.
Legitimate interests	Processing is necessary for the legitimate interests of the controller or a third party, provided those interests are not overridden by the rights of the data subject. Requires a documented balancing test.

Important You must identify your lawful basis before processing begins and document it. You cannot switch bases retrospectively if challenged by a data subject or the ODPC.

6. Data Subject Rights

The Kenya DPA grants individuals significant rights over their personal data. Organisations must have processes in place to receive, verify, and respond to these rights requests within prescribed timelines — typically 30 days from receipt.

Right	What it means in practice
Right to be informed	Individuals must be told who you are, why you are processing their data, who it will be shared with, and how long it will be kept — typically through a Privacy Notice.

Right of access	Individuals can request a copy of all personal data you hold about them (a Subject Access Request). You must respond within 30 days with a description of the data and why it is processed.
Right to rectification	Individuals can ask you to correct inaccurate or incomplete personal data. You must respond within 21 days.
Right to erasure	Individuals can request deletion of their data where it is no longer needed for its original purpose, consent has been withdrawn, or the data was processed unlawfully.
Right to restrict processing	Individuals can ask you to pause processing of their data — for example while disputing its accuracy.
Right to data portability	Individuals can receive their data in a structured, commonly used, machine-readable format and transfer it to another controller.
Right to object	Individuals can object to processing based on legitimate interests or for direct marketing. Direct marketing objections must be honoured immediately with no exceptions.
Rights re. automated decisions	Individuals have the right not to be subject to decisions based solely on automated processing (including profiling) that produce significant legal or similarly significant effects.

7. Data Protection Officer (DPO)

Certain organisations are required to appoint a Data Protection Officer (DPO) under the Kenya DPA. The DPO is responsible for overseeing compliance with data protection obligations and acting as a point of contact for both the ODPC and data subjects.

Who must appoint a DPO?

- Public authorities or bodies processing personal data.
- Organisations conducting large-scale systematic monitoring of individuals.
- Organisations processing special categories of data at scale (health, biometric, financial records).

DPO responsibilities include:

- Advising the organisation on data protection obligations.
- Monitoring compliance with the DPA and internal policies.
- Conducting or overseeing DPIAs.
- Acting as the first point of contact for data subjects and the ODPC.
- Training staff and raising awareness of data protection obligations.

DPO-as-a-Service	Organisations that do not have the internal expertise or resources to appoint a full-time DPO can engage a third-party DPO service provider. SecureZaidi offers DPO-as-a-Service for organisations of all sizes.

8. Data Breach Notification

The Kenya DPA imposes a legal obligation to notify the ODPC of personal data breaches. A data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data — including ransomware attacks, accidental email misdirection, lost devices, and unauthorised access by staff.

What must you do?

- Notify the ODPC: as soon as reasonably practicable after becoming aware of a breach that is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected individuals: where the breach is likely to result in a high risk to their rights, you must also notify them directly — for example if financial data or health records were compromised.
- Document all breaches: maintain an internal breach register regardless of whether ODPC notification is required, including details of what happened, the data involved, and what remediation steps were taken.

What to include in your ODPC notification:

- Nature of the breach, including categories and approximate number of individuals affected.
- Name and contact details of the DPO (or other contact point).
- Likely consequences of the breach.
- Measures taken or proposed to address and mitigate the breach.

Key action	Every organisation should have an Incident Response Plan that specifically covers data breach identification, internal escalation, ODPC notification, and individual notification procedures before a breach occurs — not after.

9. Cross-Border Data Transfers

The Kenya DPA restricts the transfer of personal data to recipients located outside Kenya unless adequate safeguards are in place. This is particularly relevant for organisations using foreign cloud providers, outsourcing to overseas processors, or sharing data with international parent companies.

Permitted transfer mechanisms:

- Transfer to a country with an adequate level of data protection (as determined by the ODPC).
- Transfer subject to appropriate safeguards, such as binding contractual clauses or binding corporate rules approved by the ODPC.
- Transfer with the explicit consent of the data subject, who has been informed of the risks.
- Transfer necessary for the performance of a contract between the data subject and the controller.
- Transfer necessary for important public interest reasons.

Cloud providers	Using AWS, Azure, Google Cloud, or any foreign SaaS platform likely constitutes a cross-border transfer. Ensure your agreements with these vendors include appropriate data processing and transfer clauses.

10. Special Categories of Personal Data

The Kenya DPA provides heightened protection for specific categories of personal data that are considered particularly sensitive. Processing these categories is prohibited unless specific conditions are met.

Special categories include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data processed for unique identification
- Health or medical data
- Sex life or sexual orientation
- Financial data
- Personal data of a child (under 18 years)

Conditions for processing special category data:

Processing special category data requires explicit consent in addition to a standard lawful basis, or one of a limited set of additional conditions — such as necessity for employment law obligations, medical treatment, or prevention of serious harm. Legal advice should be obtained before processing any special category data.

11. Enforcement and Penalties

The ODPC has broad investigative and enforcement powers under the Kenya DPA, including the power to:

- Conduct audits and investigations of any data controller or processor.
- Issue enforcement notices requiring organisations to take or stop specific actions.
- Issue assessment notices requiring access to premises, systems, and documentation.
- Impose administrative fines of up to KES 5,000,000 or 1% of annual gross turnover — whichever is higher.
- Recommend criminal prosecution for serious offences (e.g. unlawful disclosure of personal data, obtaining data by deception).

Criminal offences under the Act can result in imprisonment of up to 10 years for individuals. Data subjects also have the right to bring civil claims against organisations for damages caused by a breach of their rights.

ODPC enforcement activity	The ODPC has been increasingly active since 2022, conducting investigations into major Kenyan corporates, financial institutions, and telecommunications providers. Enforcement action is no longer theoretical.

12. Practical Compliance Checklist

Use this checklist to assess your organisation's current DPA compliance posture:

#	Requirement	Status
1	Registered as data controller/processor with ODPC	■ Done ■ In Progress ■ Not Started
2	Data inventory (Record of Processing Activities) documented	■ Done ■ In Progress ■ Not Started
3	Lawful basis identified and documented for each processing activity	■ Done ■ In Progress ■ Not Started
4	Privacy Notice / Policy published and accessible to data subjects	■ Done ■ In Progress ■ Not Started
5	DPO appointed (where required) and registered with ODPC	■ Done ■ In Progress ■ Not Started

6	Data Processing Agreements in place with all processors	■ Done ■ In Progress ■ Not Started
7	Process for handling data subject rights requests documented	■ Done ■ In Progress ■ Not Started
8	Data breach response plan documented and tested	■ Done ■ In Progress ■ Not Started
9	Cross-border transfer mechanisms documented and compliant	■ Done ■ In Progress ■ Not Started
10	DPIA process in place for high-risk processing activities	■ Done ■ In Progress ■ Not Started
11	Staff trained on data protection obligations (annual minimum)	■ Done ■ In Progress ■ Not Started
12	Data retention policy documented and enforced	■ Done ■ In Progress ■ Not Started

How SecureZaidi Can Help

SecureZaidi is a Kenya-based cybersecurity and GRC consultancy specialising in helping East African organisations achieve and maintain compliance, reduce cyber risk, and build lasting security cultures. Our consultants bring deep, practical expertise in the Kenyan regulatory environment and the realities of doing business in the region.

Kenya DPA Compliance	ODPC registration, DPIA support, DPO-as-a-Service, policy development, and staff training.
ISO 27001 Certification	Gap analysis, ISMS implementation, internal audit support, and certification readiness preparation.
Security Awareness Training	Customised staff workshops, phishing simulation campaigns, and 12-month culture programmes.
GRC Advisory	Risk register development, threat modelling, board-level reporting, and policy frameworks.

vCISO Services	Fractional CISO leadership — strategy, oversight, and executive reporting without a full-time hire.
Penetration Testing	Authorised simulated attacks on networks, web applications, and cloud environments.

Ready to take the next step? Contact us today for a no-obligation consultation.

Email	info@securezaidi.com
Phone	+254 700 000 000
Website	securezaidi.com