



WHITEPAPER

The Kenya Data Protection Act: An Engineering Checklist

What the Data Protection Act, 2019 actually asks engineering and security teams to build – translated out of legal language and into controls, logs and retention rules.

PUBLISHED

December 3, 2025

READING TIME

12 minutes

AUTHOR

SCIAT AFRICA Research

ABSTRACT

Compliance programmes stall when the obligations stay in the legal department. This brief translates the Data Protection Act, 2019 and its subsidiary regulations into the concrete things a technical team has to be able to do: locate every copy of a data subject's records, justify a retention period, produce a lawful basis, honour a deletion request across backups, and notify within seventy-two hours.

Topics: Data Protection · Compliance · Governance

WHAT TO TAKE AWAY

- Registration with the Office of the Data Protection Commissioner is a threshold obligation for many controllers and processors, not an optional step.
- Data subject rights are an engineering requirement: access, correction, deletion and objection all presuppose that you can find every copy of a record.
- A retention schedule that exists only on paper fails the moment a subject exercises the right to erasure.
- Breach notification runs to seventy-two hours from awareness, which only works if detection and escalation are instrumented.
- Cross-border transfer needs a documented basis before the data moves, not after an auditor asks.

CONTENTS

- 01 Start with the data map, because everything else depends on it
- 02 Registration and the role you are actually playing
- 03 Building for data subject rights
- 04 Seventy-two hours is an instrumentation problem
- 05 Transfers, impact assessments and vendors

01 Start with the data map, because everything else depends on it

Almost every obligation in the Act resolves, in practice, to a question about location: where is this person's data, which systems hold a copy, who can read it, and how long will it stay there. An organisation that cannot answer that cannot honour an access request, cannot evidence a retention period, and cannot scope a breach notification.

A usable data map is less elaborate than teams fear. For each system: what categories of personal data it holds, the lawful basis for holding them, who the data flows to downstream, where it is physically stored, and the retention rule. The discipline is in keeping it current as systems change, which is why it belongs in the change-management process rather than in an annual exercise.

02 Registration and the role you are actually playing

The Act and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 establish registration duties with the Office of the Data Protection Commissioner, with thresholds and exemptions set out in the regulations. The first step is determining, per processing activity, whether you are the controller deciding purpose and means, the processor acting on instruction, or a joint controller — the answer sets which duties attach to you.

That determination is frequently wrong in practice. Organisations that describe themselves as mere processors are often making independent decisions about purpose, and SaaS vendors that describe themselves as processors often process for their own analytics purposes as well. The contractual position and the engineering reality need to agree.

03 Building for data subject rights

Part V of the Act gives data subjects rights of access, correction, deletion, objection and portability. Each one has a technical precondition. Access requires that records can be assembled per subject rather than per system. Correction requires that the correction propagates to downstream copies. Deletion requires that you know which copies exist, including in analytics warehouses, exports, email attachments and backups.

Backups deserve particular attention because the obvious engineering answer — delete the row — leaves copies in every backup set taken before the request. The defensible position is a documented approach: deletion from live systems immediately, with backups aged out on a stated schedule and re-deletion applied if a restore reinstates the record. What matters is that the approach is reasoned, written and followed.

- Be able to produce every record held about one person, across systems, within the statutory response window.

- Hold a documented retention period for every data category, with a technical mechanism that enforces it.
- Define and write down how deletion requests interact with your backup cycle.
- Log every rights request and its outcome – the log is your evidence of compliance.

04 Seventy-two hours is an instrumentation problem

Section 43 requires a controller to notify the Data Commissioner without delay and within seventy-two hours of becoming aware of a breach where there is a real risk of harm, and to communicate with the affected data subject in writing. Processors must notify their controller within forty-eight hours of becoming aware.

Those clocks start at awareness, which makes detection the binding constraint. An organisation with no centralised logging does not become aware of a database export; it becomes aware when someone else tells it. Meeting the deadline reliably means instrumenting the paths that personal data can leave by – database access, bulk export, email forwarding rules, cloud storage permissions – and having an escalation route that reaches the privacy lead on a weekend.

05 Transfers, impact assessments and vendors

Cross-border transfer requires a basis established before the transfer: adequacy, appropriate safeguards, consent, or one of the specific grounds in the Act, with the Data Protection (General) Regulations, 2021 adding detail. For most organisations the practical work is inventorying which vendors hold data outside Kenya and securing the contractual terms that support the transfer.

Data protection impact assessments are required where processing is likely to result in high risk. Treat the trigger as a design-review gate: new processing of sensitive categories, large-scale monitoring, automated decision-making, or a new vendor receiving personal data. A short, honest assessment written at design time is worth more than a long one written retrospectively.

About this publication

This document is published by SCIAT AFRICA, a cybersecurity and digital forensics agency based in Nairobi, Kenya. It is free to read, print and circulate inside your organisation. The web edition, which carries the same content, is at <https://sciatafrica.com/research/kenya-data-protection-act-checklist>.

It is general guidance, not legal advice and not a substitute for an assessment of your own environment. Where it refers to a law, regulation or standard, read the instrument itself before relying on it – and talk to us if you want help applying it to your estate.

SCIAT AFRICA

info@sciatafrica.com · +254 794 946633 · <https://sciatafrica.com>