

APPLIED PRACTICE

The Kenya data lab

From a statutory provision to an operating control. A separately scoped, fictional practice exercise.

An optional application after C04/C06 and alongside A12. This is a separately scoped Kenyan exercise, not an assertion that English law governs Kenyan processing. All organisations and records are fictional. No real personal data is required.

What you will learn

Explain selected data-protection principles, distinguish lawful-basis analysis from notice and security, and complete a source-to-control record. The reading is Kenya Law's Data Protection Act, Cap. 411C, version dated 31 December 2022, identified by the publisher as its latest Act version at the 12 September 2026 check. That version date is not the retrieval date and does not incorporate every relevant regulation, decision or sector guideline into this lab. Check subsequent developments; a Kenyan-qualified reviewer must verify the applicable regime before professional use. [Kenya Law: Data Protection Act, Cap. 411C — version 31 December 2022](#)

Read the obligation before building the register

Start with definitions and scope in sections 2 and 4. In the supplied Act, section 25 addresses, among other matters, lawful/fair/transparent processing, specified purposes, necessity, accuracy, retention and transfers. These are distinct tests: a secure system can still collect unnecessary information or use it for an incompatible purpose.

Section 29 concerns information given in connection with collection. Section 30 requires an applicable lawful processing ground: consent is one route, not the name for every permitted use. If relying on contractual necessity, explain why that particular processing is needed for the data subject's contract; being a customer does not make all later uses necessary. Consent itself has conditions in section 32. A notice does not create a lawful basis merely by describing an activity.

Sections 41–42 connect appropriate technical/organisational measures to design, default settings, risk and implementation. Section 42(2) addresses sufficient processor guarantees and a written instructions-based contract; section 42(3) addresses processing outside instructions. Do not import a UK Article 28 checklist as the complete Kenyan analysis. Sections 25(g) and 39 concern retention; a period chosen by an author is not a statutory retention rule.

For incident triage, read section 43 carefully rather than copying one number into every register. Its controller notification provision addresses unauthorised access/acquisition and real risk of harm, with notification without delay and within 72 hours of awareness under the stated test. The processor provision separately requires notice to the controller without delay and, where reasonably practicable, within 48 hours of awareness. Recipient, trigger and qualification differ. These are not permission to wait until the last hour; preserve facts and escalate immediately for the applicable analysis. Current regulations and guidance need separate checking.

For foreign support access or storage, examine sections 25(h), 48 and related provisions with current regulations/guidance. A server's location or a processor contract alone does not prove every transfer condition is satisfied. Sensitive data, children's data, DPIAs, commercial use and registration introduce further workstreams; this lab does not decide them from a generic form.

Supplied fictional activity

Kito Training Ltd operates an adult training course in Kenya. It collects a learner name, work email, course choice and attendance. The form also asks every learner for a date of birth and free-text medical details, although Operations can identify no need for those fields in ordinary enrolment. An external platform stores the forms; its support locations are not yet known. A staff member exports an attendance spreadsheet to a shared folder. Marketing proposes reusing that export for a new campaign, not described in the supplied enrolment purpose.

Completed data map

Activity/copy	Purpose and access	Evidenced fact or gap	Decision
Enrolment form	Administer selected adult course; enrolment team	Form fields supplied; necessity for DOB/medical text unexplained	Remove those fields from ordinary flow pending a separate justified support process
Platform storage/support	Hosting and support	Contract, recipients and access locations not supplied	Obtain processing particulars, guarantees, written terms and transfer information
Attendance export	Attendance administration; shared - folder access	Copy exists; access list and retention decision not supplied	Restrict access and establish an evidenced retention/deletion decision

Activity/copy	Purpose and access	Evidenced fact or gap	Decision
Proposed campaign	New marketing purpose	New purpose not part of supplied enrolment analysis	Separate purpose/lawful-basis, notice and commercial-use review; do not approve from the original form

Completed source-to-control record

Field	Worked entry DP-01
Source and scope	Supplied Act, sections 25(d) and 41(3); fictional ordinary enrolment within the assumed Kenyan scope
Requirement explained	Limit processing by default to what is necessary for the specific purpose; do not collect extra fields merely because a form permits them
Fact/application	Operations states no ordinary-enrolment need for DOB or medical free text; any accessibility-support purpose requires a separately scoped decision
Proposed implementation	Remove those default fields; document the minimum enrolment field set; route support requests through a separately approved process
Owner and trigger	Fictional enrolment lead; before the form is used and when the purpose/fields change
Evidence	E-DP1 necessity decision; E-DP2 test-form configuration; E-DP3 test showing prohibited fields are absent; restricted handling plan for any existing copies
Status	Worked design accepted for this example; operating compliance not independently established
Residual work	Verify applicable current law, other field necessities, notice/basis, supplier terms, retention, sensitive-data conditions and any required DPIA/registration

The trigger “before using the form” implements the design decision; the lab has not invented a universal number of retention days. A real retained record may need restriction or a lawful retention exception rather than indiscriminate deletion. Separate that question from fixing a future default.

Guided attempt and feedback

Operations removes the medical field, but a weekly export still copies old responses into a broadly shared folder. Is DP-01 complete?

Compare after answering: the future form is improved, but existing copies and the ongoing export remain a distinct processing problem. Map recipients/access, stop unnecessary replication through an authorised process, determine lawful retention/handling, and obtain implementation evidence. A screenshot of the new form cannot prove the old copies were handled appropriately.

Independent work

Produce three entries: an external-source requirement, an explicitly labelled internal review policy, and a proposed contractual obligation. For each give source/type, applicability, control, owner, timing basis, evidence and residual question. Reuse the map but change the delivery to include adult learners accessing from another jurisdiction; identify the additional scope facts needed without asserting universal applicability.

Success means another reviewer can distinguish law, your interpretation and the organisation's chosen implementation. A completed register is not a certificate that Kito is compliant. Use the core submission format and peer/solo feedback route.