The KDPA Developer & Founder Checklist

Kenya Data Protection Act — practical compliance starting points

Prepared by	Nazline Mwita, CompTIA Security+
Practice	HarLyn Digital Partners
Scope	Self-assessment starting point — not a substitute for a scoped audit

1. Data Minimization & Payload Sanitization

- Only the fields actually required for the stated purpose are collected at intake.
- API responses don't leak extra PII fields beyond what the consuming UI needs.
- Log statements are scrubbed of raw PII (national ID numbers, phone, email) before write.
- File uploads (ID scans, statements) are validated for type/size before storage.

2. Explicit Consent Architecture

- Consent is a distinct, logged action — not bundled into a generic “I agree to terms” checkbox.
- Consent records capture what was agreed to, when, and the applicable privacy notice version.
- Users have a working path to withdraw consent and request deletion.
- Third-party data sharing (analytics, ad pixels, AI vendors) is disclosed and consented to separately.

3. Column-Level Encryption & Zero-Trust Access

- Sensitive columns (national ID, financial data, health data) are encrypted at rest, not just the disk.
- Row-level security or equivalent is enforced at the database layer, not only in application code.
- Service-role/admin credentials are not embedded in client-side code or logged in plaintext.
- Access to production PII is role-scoped and auditable — not “everyone with the DB password.”

4. Breach & Audit Readiness

- There is a documented, rehearsed process for detecting and confirming a data breach.

- The 72-hour ODPC breach-notification clock and its trigger conditions are understood by the team.
- Audit logs record who accessed or modified sensitive records, and are tamper-evident.
- A Data Protection Impact Assessment (DPIA) exists for any high-risk processing activity (Section 31).

5. Registration & Governance

- The organisation's data-controller/processor registration status with the ODPC is confirmed.
- A named person owns data-protection compliance internally (even if fractional/outsourced).
- Vendor and sub-processor agreements (cloud, email, AI APIs) include data-protection terms.

How to use this checklist

This is a starting-point self-assessment, not a substitute for a scoped engagement. Items checked “no” or “unsure” are candidates for a Secure Digital Workflow Assessment.

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.