
# FINTECH DATA LAW & REGULATORY COMPLIANCE (KENYA)

## Companion Workbook & Practitioner Study Guide

**Patrick Muchangi · Advocate of the High Court of Kenya**

Data Protection Counsel & Governance Architect · GDPR Specialist · AI & Law

Muchangi Patrick & Co. Advocates · Technology Law Firm

patrick@dataprivacyadvocates.co.ke · 0722 878 607

# How to Use This Workbook

This workbook is the companion to the Fintech Data Law & Regulatory Compliance (Kenya) slide deck. It is designed for practitioners who need to move from knowledge to implementation — not simply to understand the law, but to apply it across real compliance decisions.

Each module contains:

- Full expanded content — going deeper than the slide deck on statutory interpretation and practical application
- Statutory citations — every legal reference includes the exact section, subsection and regulation number
- Practitioner boxes — real-world scenarios from Kenyan fintech enforcement practice
- Worked examples — drafted documents, clauses, and frameworks you can adapt immediately
- Reflection questions — self-assessment prompts to consolidate learning
- Module checklists — practical action items you can tick off as you implement

> This workbook is a legal reference document, not legal advice. Every organisation's compliance situation is fact-specific. If you are unsure whether a particular analysis applies to your operations, obtain advice from a qualified data protection practitioner before acting.

MODULE 1

# Regulatory Landscape & Registration Architecture

Key Statutes: Constitution of Kenya 2010 (Article 31) · Data Protection Act No. 24 of 2019 · Data Protection (General) Regulations 2021 · Data Protection (Registration) Regulations 2021 · CBK (Digital Credit Providers) Regulations 2022 · POCAMLA Cap. 59B

## 1.1 The Constitutional Foundation

Article 31(c) and (d) of the Constitution of Kenya, 2010 provides that every person has the right to privacy, including the right not to have information relating to their family or private affairs unnecessarily required or revealed, and the privacy of their communications infringed. This is not a procedural right — it is a fundamental right enforceable by the courts independently of the Data Protection Act 2019. In Petition No. E009 of 2021, the High Court confirmed that data protection obligations on financial institutions are strict liability — the defendant cannot escape liability by showing that the breach was accidental or that appropriate systems were generally in place.

PRACTITIONER NOTE: Every time a fintech platform collects, processes, or shares a borrower's personal data, Article 31 is engaged. This means the constitutional right to privacy is your starting point — not the DPA 2019 — when assessing whether a new processing activity is lawful.

## 1.2 The Regulatory Stack — Six Instruments in Detail

Digital Credit Providers operate under a concurrent regulatory architecture. All six instruments below apply simultaneously:

| Instrument | Key Obligations for DCPs | Enforced By |
|---|---|---|
| Constitution of Kenya, 2010 — Art. 31 | Fundamental privacy right; basis for judicial review of any DPA violation | High Court / Tribunal |
| Data Protection Act, No. 24 of 2019 | Registration, DPO, data subject rights, breach notification, DPIA, cross-border transfers, fines | ODPC |
| Data Protection (General) Regulations, 2021 | Consent mechanics, automated decisions, impact assessments, GDPR-equivalent standards | ODPC |
| Data Protection (Registration) Regulations, 2021 | Mandatory registration tiers, fees, documentation requirements, renewal obligations | ODPC |
| CBK (DCP) Regulations, 2022 | DCP licensing, anti-harassment mandates, CRB reporting, consumer protection, pricing transparency | CBK |
| POCAMLA, Cap. 59B | 7-year KYC retention, transaction records, AML compliance — creates tension with DPA erasure rights | FRC / CBK |

## 1.3 ODPC Regulatory Powers — What Section 8 Authorises

The Office of the Data Protection Commissioner is established under Section 5 of the DPA 2019. Section 8 enumerates the Commissioner's powers, which include: maintaining the register of data controllers and processors; monitoring and enforcing compliance with the Act; reviewing data protection impact assessments submitted by data controllers; investigating complaints from data subjects; issuing enforcement notices; imposing administrative fines up to KES 5,000,000 per breach or 1% of annual turnover (whichever is lower); and referring criminal violations to the Director of Public Prosecutions.

ENFORCEMENT REALITY: As of 2025, the ODPC has issued over 40 formal enforcement notices to digital credit providers. Common violations: unregistered operation (Section 18), invalid consent flows (Section 32), failure to appoint a DPO (Section 18(5)), and debt-shaming via contact-list scraping (Section 72). Do not underestimate the ODPC's willingness to impose maximum fines.

## 1.4 The POCAMLA vs DPA Retention-Erasure Conflict — Resolved

This is the most common compliance question raised by digital lenders: a borrower whose loan account has been closed requests deletion of all their personal data under Section 28 of the DPA 2019. The DCP wants to comply but knows that POCAMLA Section 40 requires all customer identification records and transaction logs to be retained for a minimum of seven (7) years after the end of the business relationship.

The legal resolution is as follows:

1. The DCP should NOT delete the data. Section 28(2)(c) of the DPA 2019 explicitly exempts erasure obligations where retention is required to comply with a legal obligation.
2. Instead, the DCP must RESTRICT processing: archive the data in a secure, non-operational repository. The archived data must not be used for credit scoring, marketing, or any active business purpose.
3. The DCP must notify the data subject in writing of: (a) the applicable statutory retention obligation; (b) the specific date on which the data will be permanently destroyed; and (c) their right to complain to the ODPC.
4. Upon expiry of the 7-year POCAMLA window, automated deletion protocols must execute. Destruction must be logged, timestamped, and auditable.

GDPR INTERSECTION: Article 17(3)(b) GDPR contains an identical exemption — processing necessary for compliance with a legal obligation. Where a platform processes EU data subjects' data, the same resolution applies under both regimes simultaneously.

## 1.5 ODPC Registration — Step by Step

| Step | Action | Documentation Required |
|---|---|---|
| 1 | Determine your registration tier based on employees and annual turnover | Audited accounts or board resolution confirming turnover |
| 2 | Create an account on the ODPC portal at odpc.go.ke | Certificate of Incorporation, CR12 form, KRA PIN Certificate |

| Step | Action | Documentation Required |
|---|---|---|
| 3 | Specify your data processing activities: categories of data subjects, data types, purposes, legal bases | Completed data mapping inventory (see Module 2) |
| 4 | Declare your security architecture: encryption standards, access controls, backup protocols | IT security policy or architecture summary |
| 5 | Upload your Data Protection Policy (must be board-approved and publicly accessible) | Signed Data Protection Policy |
| 6 | Pay the applicable registration fee via eCitizen (M-Pesa Express or bank card) | Payment receipt — retain for renewal |
| 7 | Await issuance of the Data Controller / Processor Certificate (valid 2 years) | Certificate — display on website and in ODPC correspondence |

### ✍️ Reflection Question

Your organisation currently processes borrower biometric data for KYC verification and uses an automated credit scoring algorithm. How many ODPC registration obligations does this create, and which registration tier applies to your organisation?

Your answer: _____
_____
_____

### ✓ Module Completion Checklist

- ☐ ODPC registration status confirmed and certificate on file (not expired)
- ☐ Data Protection Officer appointed in writing and registered with ODPC
- ☐ Registration tier correctly determined (Micro/Medium/Large) with fee paid
- ☐ Data Protection Policy board-approved, signed and published on website
- ☐ Dual-regulator conflict matrix completed: identified all areas where CBK and ODPC obligations overlap
- ☐ POCAMLA retention policy documented for each data category — overrides erasure requests mapped

MODULE 2

# Data Architecture, Lineage & Mapping

Key Statutes: DPA 2019 Sections 2, 3(c), 25 · Data Protection (General) Regulations 2021 Reg. 4–6 · Section 2 — Definitions of 'personal data' and 'sensitive personal data'

## 2.1 Understanding Data Lineage — Why It Matters in Enforcement

Data lineage is the auditable trail of every personal data element from the moment it is captured from the borrower through every system, vendor, and process it touches, to the moment of its permanent deletion. The ODPC does not merely ask what data you hold — it asks to see the documentary evidence of how that data moved through your organisation, who accessed it, when, and for what stated purpose.

For a licensed Digital Credit Provider, the standard data lineage path traverses: the mobile application front-end → the API gateway → the core lending engine → external KYC validation (IPRS) → CRB credit history retrieval → M-Pesa identity matching → secure encrypted storage. Every node in this chain creates a separate compliance obligation.

AUDIT EXPERIENCE: In 2024 ODPC inspections, 73% of enforcement findings related not to the fact that data was processed unlawfully, but to the fact that the DCP could not produce a documented lineage trail showing that the processing was lawful. If you cannot prove it was done correctly, the ODPC treats it as having been done incorrectly.

## 2.2 Standard vs Sensitive Personal Data — The Section 2 Classification

Section 2 of the DPA 2019 distinguishes between personal data and sensitive personal data. The distinction has profound implications for your legal basis requirements, storage architecture, and security obligations:

| Data Type | Classification | Legal Basis Required | Storage Rule |
|---|---|---|---|
| Full Legal Name | Standard Personal Data | Contract performance (Section 30(1)(b)) | Encrypted at rest, standard access controls |
| National ID Number | Standard Personal Data (border case) | Contract performance + Legal obligation | Encrypted at rest, strict IAM, 7-year POCAMLA retention |
| Mobile Phone Number (MSISDN) | Standard Personal Data | Contract performance | Encrypted, access limited to Ops and Credit teams |
| Biometric Selfie / Face Verification | Sensitive Personal Data | Explicit consent (Section 30 + Section 2) | Isolated storage, unique AES-256 key, 90-day maximum retention |
| Precise GPS Coordinates | Sensitive Personal Data | Explicit consent (or LIA for fraud — coarse only) | MongoDB cluster, 12-month rolling deletion |

| Data Type | Classification | Legal Basis Required | Storage Rule |
|---|---|---|---|
| Bank / M-Pesa Statement (uploaded) | Sensitive Personal Data | Explicit consent covering all downstream uses | Separate S3 bucket, zero marketing use, user-controlled deletion |
| Racial or Ethnic Origin | Sensitive Personal Data | Prohibited from credit scoring use (Art. 27 Constitution) | If held, isolated; prohibited from any model training |
| Religious Beliefs | Sensitive Personal Data | Prohibited from credit scoring use | Same as above |

## 2.3 Building Your Compliant Data Mapping Registry — Worked Template

A data mapping registry is not optional — it is the primary document the ODPC requests on the first day of any audit. It must be maintained as a live document, updated whenever a new data category is introduced, a vendor is added or replaced, or a processing purpose changes.

> PRACTITIONER TIP: Your data map must be cross-referenced against your Data Protection Policy, your vendor Data Processing Agreements, and your ODPC registration application. If any element in your data map does not appear in all three documents, you have a gap — and the ODPC will find it.

The following is an operational template showing the minimum fields required in a compliant fintech data map:

| Data Element | Legal Basis | Storage Location | Access Level | External Sharing | Retention Peri |
|---|---|---|---|---|---|
| National ID Number | Contract + Legal Obligation (Sec. 30(b)(c)) | AWS EC2 eu-west-1, AES-256 | Compliance & Credit Risk only | IPRS / CBK / Licensed CRBs | 7 years post ac close |
| Biometric Face Image | Explicit Consent (Sec. 30(a) + Sec. 2) | AWS S3 Isolated Bucket | KYC Engine only (automated) | Third-party KYC platform (under DPA) | Deleted within days |
| Coarse Geo-Location | Legitimate Interest — Fraud Prevention | MongoDB Log Cluster | Anti-Fraud & Security Team | Never shared externally | 12-month rollin deletion |
| M-Pesa Transaction Metadata | Consent — Credit Scoring (Sec. 32) | Encrypted Data Warehouse | Data Science Team only | Licensed CRBs (under CBK mandate) | 24 months post settlement |
| Next of Kin Contact Details | Consent + Legitimate Interest (Sec. 30(f)) | Core DB — encrypted at rest | Recovery Team (restricted) | Debt collection agency (under DPA only) | Loan term + 1 y maximum |

## 2.4 Role-Based Access Control (RBAC) — Implementing the Principle of Least Privilege

Section 3(c) of the DPA 2019 establishes the data minimization principle: personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. In technical architecture, this principle is implemented through Role-Based Access Control (RBAC) — ensuring that every system user and automated process accesses only the minimum data necessary for their specific function.

The four core access tiers for a licensed DCP are:

- **CUSTOMER CARE PORTAL: Data masking applied. Agents see masked National ID (ID_XXXXX_254), partial phone number (+254 7XX XXX 123), loan status (ACTIVE/SETTLED), and repayment schedule only. Zero export rights. Zero access to raw sensitive data or scoring algorithm outputs.**
- **CREDIT RISK / SCORING ENGINE: Machine-to-machine access only. Full raw data accessed programmatically, with no persistent human visibility. Every data read generates an immutable audit log entry recording: data element accessed, timestamp, system process ID, and query purpose.**
- **COMPLIANCE & LEGAL: Highest human access tier. Can access full data map, SAR processing tools, breach logs, vendor DPA files, and ODPC correspondence. Every access logged with purpose justification. DPO must approve access requests outside routine compliance operations.**
- **DATA SCIENCE / ANALYTICS: Pseudonymised and anonymised datasets only for model training. No individual borrower profiles. De-identification verified by the DPO before any data release to this team. Output: model parameters and aggregate statistics only.**

### ✍️ Reflection Question

Map your current organisation against the four RBAC tiers above. For each tier, list the specific individuals or teams who currently have access. Are there any access rights that exceed what is strictly necessary? What is your plan to remediate?

Your answer: _____

_____

_____

### ✓ Module Completion Checklist

☐ Data lineage diagram completed for every personal data element: capture → processing → storage → deletion

☐ All data elements classified as standard personal data or sensitive personal data per Section 2 DPA 2019

☐ Data mapping registry built, maintained as a live document, cross-referenced against DPAs and ODPC registration

☐ RBAC implemented across all four tiers: customer care, scoring engine, compliance, analytics

☐ Audit logs confirmed as immutable: append-only storage with no database-administrator delete rights

☐ Retention schedules set per data category: biometrics (90 days), geo-location (12 months), financial records (7 years POCAMLA)

MODULE 3

# Lawful Bases, Consent Architecture & User Journey Design

Key Statutes: DPA 2019 Sections 30, 32 · Data Protection (General) Regulations 2021 Regulation 20 · GDPR Articles 6, 7, 13 (for EU data subjects)

## 3.1 The Seven Lawful Bases — Practical Application for DCPs

Section 30 of the DPA 2019 establishes seven lawful bases for processing personal data. A Data Controller must identify and document a valid lawful basis before any processing begins — not retrospectively after a complaint is filed.

| Basis | Statutory Foundation | Fintech Application | Risk Level if Relied Upon Incorrectly |
|---|---|---|---|
| Consent | Section 30(1)(a) | SMS metadata scanning, marketing, contact-list access (where permitted) | HIGH — invalid consent makes all downstream processing unlawful |
| Contract Performance | Section 30(1)(b) | Core KYC, credit underwriting, loan disbursement, repayment processing | LOW — strongest basis for core lending operations |
| Legal Obligation | Section 30(1)(c) | AML/KYC under POCAMLA, CRB reporting under CBK DCP Regulations | LOW — statute provides clear mandate; document the specific provision |
| Vital Interests | Section 30(1)(d) | Not applicable to standard lending operations | N/A — do not stretch this basis to cover commercial activities |
| Public Interest | Section 30(1)(e) | AML reporting to FRC, CBK data requests under statutory mandate | LOW — limited to regulatory reporting functions only |
| Legitimate Interests | Section 30(1)(f) | Fraud prevention (coarse location), system security logging, network monitoring | MEDIUM — requires documented Legitimate Interests Assessment (LIA) |
| Research / Statistics | Section 30(1)(g) | Aggregate, anonymised lending trend analysis — not individual profiling | LOW if truly anonymised; HIGH if re-identification risk exists |

## 3.2 Constructing the Four Pillars of Valid Consent

Section 32 of the DPA 2019 establishes four structural requirements for valid consent. If consent fails any one pillar, it is legally void — and all processing based on that consent becomes unlawful ab initio. The GDPR Article 7 standard is identical, meaning that for any platform with EU data subjects, the same four pillars apply under both regimes.

**PILLAR 1 — FREELY GIVEN:**

The borrower must have a genuine, unconstrained choice. The DCP cannot make the provision of a loan — or even the ability to view loan terms — conditional on the borrower consenting to non-essential processing. If a borrower must consent to contact-list access to proceed with their loan application, that consent is not freely given and is therefore void. The ODPC has consistently struck down bundled consent structures where refusing optional data processing resulted in denial of service.

**PILLAR 2 — SPECIFIC:**

One consent, one purpose. A single consent checkbox covering credit scoring + marketing + third-party data sharing is invalid as to all three purposes. Separate, standalone consent is required for each distinct processing activity. In UI/UX terms, this means a separate toggle switch per data category and processing purpose.

**PILLAR 3 — INFORMED:**

The data subject must be told: (a) the identity of the Data Controller; (b) the exact categories of data being processed; (c) the specific processing purposes; (d) the retention period; (e) any third-party recipients; (f) whether data will be transferred outside Kenya; and (g) how consent can be withdrawn. Generic 'we may use your data to improve our services' language fails this test.

**PILLAR 4 — UNAMBIGUOUS:**

Affirmative action is required. Silence, scrolling, pre-ticked boxes, or proceeding past a terms-and-conditions screen do NOT constitute valid consent under the DPA 2019 or GDPR. The borrower must actively click, toggle, or sign. In the context of a mobile loan application, this means every data permission must be represented by an unchecked checkbox or OFF-by-default toggle that the user deliberately activates.

> GDPR ARTICLE 7 INTERSECTION: GDPR Article 7(2) additionally requires that where consent is given in a document covering other matters, the consent request must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which is not in compliance with GDPR shall not be binding. The practical effect: even if the rest of your T&Cs are valid, a non-compliant consent clause within them is struck out independently.

## 3.3 Production-Ready Consent Screen Copy — Module 3 Deliverable

### Screen 1: Core Registration Consent

> [ ] I have read and agree to the [Company Name] Privacy Policy [hyperlink] and confirm that I understand how my personal identity data, KYC documentation, and credit history will be processed to evaluate my loan application. I understand that this processing is necessary for the performance of a loan agreement, and that I may withdraw non-essential consents at any time via Settings → Privacy.  [ ] I authorise [Company Name] to process my personal data for direct marketing communications, including SMS, email, and in-app promotional messages regarding financial products. I understand this is optional and will not affect my loan application. I may withdraw this consent at any time by texting STOP to [shortcode].

### Screen 2: CRB Access Authorisation

> Pursuant to Section 30 of the Kenya Data Protection Act (2019) and the Central Bank of Kenya (Digital Credit Providers) Regulations (2022), [Company Name] requires your explicit authorisation to evaluate your financial history. By clicking 'Authorise CRB Assessment', you grant explicit permission to [Company Name] to query licensed Credit Reference Bureaus (including Metropol, TransUnion, and Creditinfo) to retrieve your credit score, active loan balances, and repayment performance records. Your own performance on this loan will also be reported to licensed CRBs as required by CBK statutory mandates. [ AUTHORISE CRB ASSESSMENT ]

## 3.4 Contract Clause Reconstruction — From Non-Compliant to Compliant

| Non-Compliant Clause (Do Not Use) | Why It Fails | Compliant Replacement |
|---|---|---|
| "By downloading this application, you grant us complete authority to access all device sensors, photos, SMS records and contact lists for credit calculations." | All-in-one consent; conditions app access on non-essential data; prohibitions on contact-list access in Google Play policy; no purpose limitation | "We access your device's coarse location to prevent fraudulent account access. We will never access your contacts, photos or SMS records. Additional optional data processing requires your separate, explicit consent on the permissions screen." |
| "We may share all consumer data with any external partner at our discretion without further notice." | No purpose limitation; no specification of recipients; eliminates transparency and notification rights | "We share your repayment data with licensed CRBs under CBK mandate. All other third-party sharing requires a signed DPA and your specific consent or a documented statutory basis. You will be notified within 7 days of any new sharing arrangement." |
| "Your use of this app constitutes acceptance of all data processing described in these Terms." | Processing-by-usage clause; not an affirmative act; fails the unambiguity requirement of Section 32 | Replaced with a separate consent screen with individual unchecked checkboxes per processing purpose, appearing as the first meaningful screen after installation. |

> ✍️ **Reflection Question**
>
> Review your current loan application consent flow. Identify one dark pattern (pre-ticked box, bundled consent, or hidden decline option) in your current UI. Draft the compliant replacement copy below.
>
> Your answer: _____
> _____
> _____

**✓ Module Completion Checklist**

- ☐ Lawful basis documented in data map for every processing activity
- ☐ Consent flows redesigned with one toggle/checkbox per purpose — all defaulting to OFF
- ☐ Pre-ticked boxes eliminated from all consent screens
- ☐ CRB access authorisation screen implemented as a standalone, blocking consent — not embedded in T&Cs

☐ Marketing consent separated from core service consent — declining marketing does not affect loan application
☐ Consent withdrawal mechanism accessible within 2 taps from the home screen and fully functional
☐ Immutable consent log implemented: records user ID, policy hash, device IP, timestamp, and per-category decision

MODULE 4

# Automated Decision-Making & Algorithmic Underwriting

Key Statutes: DPA 2019 Section 35 · Data Protection (General) Regulations 2021 Regulation 7 · GDPR Article 22 (for EU data subjects) · Constitution of Kenya Article 27 (equality and non-discrimination)

## 4.1 What Makes a Decision 'Automated' for the Purposes of Section 35

Section 35(1) of the DPA 2019 provides that a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects them. The operative words are 'solely' and 'significantly affects'. A decision is automated for Section 35 purposes where: (a) no human being reviews the individual application before the decision is communicated; (b) the decision is generated by an algorithm, machine learning model, or rule-based system; and (c) the decision produces a legal or analogously significant effect.

For digital credit providers, loan approval or rejection is plainly a significant effect on the data subject — it determines whether they can access credit, at what cost, and in what amount. This means Section 35 is triggered by the core business activity of virtually every DML platform operating in Kenya.

GDPR ARTICLE 22 INTERSECTION: GDPR Article 22 contains an equivalent prohibition, but with a broader scope — it protects data subjects from solely automated decisions that produce 'legal or similarly significant effects.' Kenyan and EU standards are substantively identical. Build your appeal framework to satisfy both from the start.

## 4.2 Section 35 Obligations — The Three Mandatory Safeguards

- **MANDATORY TRANSPARENCY (Section 35(2)(a)): The data controller must proactively disclose — during the onboarding process and before the first processing activity — that the borrower's application will be evaluated by an automated system. The disclosure must include: the logic of the system (in plain language); the data inputs used; the significance and expected consequences of the processing; and the availability of a human review option. This disclosure must be a standalone, legible notice — not a footnote in the terms and conditions.**
- **RIGHT TO HUMAN INTERVENTION (Section 35(2)(b)): Every borrower whose application is automatically rejected has the right to request a human review. The data controller must provide a clear, accessible mechanism for this request — an in-app appeal button is best practice. The reviewing human must be a qualified compliance officer with the authority to override the algorithm's decision. A customer service agent reading the same algorithm output is not sufficient.**
- **RIGHT TO EXPRESS A VIEW (Section 35(2)(c)): The borrower must be given a meaningful opportunity to provide additional information before the manual review concludes. This might include uploading additional income evidence, correcting errors in the data used by the model, or explaining anomalous transaction patterns. The reviewer must demonstrably consider this input before confirming or overriding the automated decision.**

## 4.3 Algorithmic Discrimination — The Hidden Legal Risk Under Article 27

Article 27 of the Constitution of Kenya prohibits discrimination on grounds including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth. An automated credit scoring model that does not explicitly use any of these characteristics can nonetheless violate Article 27 if it uses 'proxy variables' that correlate with protected characteristics.

Examples of proxy discrimination in fintech models:

- Using the borrower's neighbourhood as a credit feature when certain neighbourhoods are demographically homogeneous (ethnic/socio-economic proxy)
- Using SMS contact frequency patterns that reflect religious observance (e.g., reduced transaction activity on Fridays or Saturdays as a negative credit signal)
- Training a model on historical loan data that has embedded historical discrimination — the model learns to replicate past discriminatory outcomes as if they were credit risk signals
- Using social network size or contact-list characteristics that correlate with tribal or community-based social structures

COMPLIANCE SHIELD: The only defensible position is a documented, independent bias audit conducted by a qualified data scientist every 6 months. The audit must test for disparate impact across all protected characteristics listed in Article 27. Audit reports must be retained and must be producible in response to any ODPC inquiry or legal challenge.

✍️ **Reflection Question**

Your automated credit scoring model currently uses the borrower's home location (city and neighbourhood) as one of 15 input features. After reading this module, assess whether this feature creates a proxy discrimination risk, identify the protected characteristic potentially affected, and state what remediation action you would take.

Your answer: _____
_____
_____

✓ **Module Completion Checklist**

- ☐ Section 35 transparency disclosure added as a standalone onboarding screen — not buried in T&Cs
- ☐ In-app Section 35 appeal button implemented and routes to a human compliance review queue
- ☐ Human reviewer has authority to override the algorithm — not merely to explain the outcome
- ☐ Right-to-express-a-view mechanism implemented: borrowers can upload additional evidence pre-review
- ☐ Bias audit conducted in last 6 months by a qualified independent data scientist
- ☐ Bias audit report retained and available for ODPC production if requested
- ☐ Appeal outcome communicated to borrower with written reasons — regardless of outcome

MODULE 5

# Ethical Debt Collection & Third-Party Data Risk

Key Statutes: DPA 2019 Sections 3, 25, 72 · CBK (DCP) Regulations 2022 Regulation 19(2) · DPA 2019 Section 30(2) — Purpose Limitation · Consumer Protection Act Cap. 46 of 2012

## 5.1 The Legal Parameters of Borrower Contact in Recovery Operations

The interaction between DPA Section 3 (data processing principles) and CBK Regulation 19(2) (prohibited debt collection conduct) creates a dual-liability zone for every debt recovery contact. A single debt-shaming call to a borrower's employer creates: (a) a DPA breach under Section 25 (unauthorised disclosure); (b) a CBK market conduct violation under Regulation 19(2)(c); (c) potential civil liability to the data subject for damage under Section 73; and (d) potential criminal liability for the individuals involved under Section 72.

| Contact Type | Legal Status | Statutory Basis |
|---|---|---|
| Direct call to borrower's registered MSISDN | Authorised — contractual basis | DPA Section 30(1)(b); CBK Reg 19(1) |
| In-app notification to borrower | Authorised — contractual basis | DPA Section 30(1)(b) |
| Email to borrower's registered address | Authorised — contractual basis | DPA Section 30(1)(b) |
| SMS to borrower's registered number re: repayment | Authorised — contractual basis | DPA Section 30(1)(b) |
| Call to guarantor to verify borrower's location | Conditionally authorised — must not disclose debt | DPA Section 30(1)(f) — Legitimate Interest (narrow) |
| Call to borrower's employer disclosing debt status | PROHIBITED — civil and criminal liability | DPA Sections 25, 72; CBK Reg 19(2)(c) |
| WhatsApp message to borrower's contact list members | PROHIBITED — criminal liability (Section 72) | DPA Section 72; CBK Reg 19(2) |
| Social media posting of borrower debt details | PROHIBITED — criminal liability + ODPC fine | DPA Section 72; Consumer Protection Act |
| Contacting borrower outside agreed hours | PROHIBITED — harassment | CBK Reg 19(2)(a); Consumer Protection Act |

## 5.2 Data Sharing Agreements with Debt Collection Agencies — Full Mandatory Clause Set

When a DCP assigns non-performing accounts to an external Debt Collection Agency (DCA), the DCA operates as a Data Processor under Section 2 of the DPA 2019. The DCP remains the Data Controller and is fully liable for the DCA's actions with the shared data. The Data Processing Agreement (DPA) with the DCA must contain, at minimum, the following clauses:

5. PURPOSE LIMITATION CLAUSE: The DCA shall process the shared borrower data solely for the purpose of recovering the specific overdue debt amounts assigned under this Agreement. The DCA is prohibited from using the shared data for cross-selling, marketing, credit analysis for other clients, or any purpose other than the specific collections mandate.
6. MANDATORY 48-HOUR DESTRUCTION CLAUSE: Within 48 hours of the earlier of: (a) full collection of the outstanding debt; or (b) recall of the account by the DCP; the DCA shall securely destroy all copies of the shared data from active systems using certified data destruction protocols (DoD 5220.22-M or equivalent). Written evidence of destruction shall be provided to the DCP within 72 hours of the destruction event.
7. SUB-PROCESSING PROHIBITION: The DCA shall not sub-contract any element of the collections mandate, share the borrower data with any third party, or assign the account to any secondary recovery vendor without the prior written approval of the DCP.
8. AUDIT RIGHTS: The DCP reserves the right to conduct unannounced compliance audits of the DCA's systems and call recordings at any time. Identified violations must be remediated within 14 calendar days, failing which this Agreement terminates automatically.
9. INDEMNIFICATION: The DCA shall indemnify and hold harmless the DCP against all ODPC fines, enforcement costs, legal fees, and compensation claims arising from any DCA action that violates the DPA 2019 or this Agreement.
10. PROHIBITED CONDUCT SCHEDULE: Annexed hereto as Schedule 1 are the prohibited contact methods, prohibited phrases, required call scripts, maximum contact frequency per borrower, and mandatory data protection training requirements for all DCA agents handling this portfolio.

LITIGATION NOTE: In any ODPC enforcement action arising from DCA misconduct, the ODPC will pursue both the DCA (as Processor) and the DCP (as Controller). The Controller indemnification from the DCA only shifts financial exposure — it does not eliminate the DCP's primary regulatory liability. Choosing compliant DCAs with strong data governance is as important as the contract.

### ✍️ Reflection Question

List all external Debt Collection Agencies currently engaged by your organisation. For each: (a) is a DPA in place? (b) does it contain all six mandatory clauses above? (c) when was the DCA last audited for compliance? What is your remediation plan for any gaps?

Your answer: _____

_____

_____

### ✓ Module Completion Checklist

- ☐ All debt recovery contact activities audited against the authorized/prohibited matrix in Section 5.1
- ☐ Data Processing Agreements executed with every DCA — containing all six mandatory clauses
- ☐ 48-hour destruction protocol verified: DCA has evidenced destruction capability in last audit
- ☐ DCA agent call scripts reviewed: prohibited phrases identified and removed from scripts
- ☐ Collection call recording system in place: all calls recorded and retained for audit purposes
- ☐ DCP retains contractual right to conduct unannounced DCA audits — right exercised at least annually

MODULE 6

# Subject Access Requests & Data Portability

Key Statutes: DPA 2019 Sections 26–33 · Data Protection (Complaints Handling) Regulations 2021 · DPA 2019 Section 50 (right to complain to ODPC) · GDPR Articles 15–22 (for EU data subjects)

## 6.1 The Eight Data Subject Rights — Operational Implications

| Right | Section | Operational Implication for a DCP | Response Deadline |
|---|---|---|---|
| Access | Section 26 | Must provide full copy of all personal data held, plus explanation of processing. First request free of charge. | 21 days |
| Rectification | Section 27 | Correct inaccurate data — critical for CRB-reported defaults logged in error. Must notify CRBs of correction. | 14 days |
| Erasure | Section 28 | Most requests will be declined on POCAMLA grounds. Must restrict processing and notify of retention timeline. | 21 days |
| Restriction | Section 29 | Suspend active processing (scoring, marketing, sharing) while a dispute is under investigation. | Without undue delay |
| Portability | Section 33 | Provide data in structured, machine-readable format (JSON). Cannot obstruct transfer to another DCP. | 21 days |
| Objection | Section 31 | Object to legitimate-interests processing. Burden shifts to DCP to show compelling grounds to continue. | 21 days |
| Automated Decisions | Section 35 | Right to human review. See Module 4 — this right cannot be waived in T&Cs. | Reasonable promptness (recommend 5 working days) |
| Complaint to ODPC | Section 50 | Data subject can escalate directly to ODPC. ODPC acknowledges within 21 days and investigates. | ODPC: 21 days to acknowledge |

## 6.2 The SAR Processing Workflow — Statutory Compliance Protocol

11. RECEIPT & LOGGING: Log the SAR immediately upon receipt with date, time, and channel (email/in-app/written). This is Day 0 of the 21-day statutory window — the clock does not pause for identity verification or for the complexity of the request.
12. IDENTITY VERIFICATION: Verify identity using your standard authentication protocol (OTP to registered MSISDN + National ID confirmation). This must not be so onerous as to constitute a barrier to the exercise of the right. The ODPC has fined organisations that required notarised documents or in-person identity verification for digital SAR requests.
13. SCOPE ASSESSMENT: Identify all data held across all systems: production database, CRB pull logs, third-party API transmission records, call recordings, in-app chat transcripts, internal compliance notes, automated decision outputs, and archived data.

14. APPLY EXEMPTIONS: Redact only what is explicitly protected: proprietary scoring model logic (trade secrets), other data subjects' personal information, active AML investigation records, and legally privileged communications. Every redaction must be individually justified in the response letter, citing the specific statutory exemption relied upon.
15. PACKAGE THE RESPONSE: Compile into a structured, readable format — PDF for human consumption, JSON for portability requests. Include a cover letter explaining the scope of the response, any redactions, the specific exemptions relied upon, and the data subject's right to escalate to the ODPC if dissatisfied.
16. DELIVER WITHIN 21 DAYS: Use encrypted email or an in-app secure download. Retain proof of delivery. Log the response in your SAR register, including the date of delivery.

## 6.3 Building an In-App Data Portability Feature — Technical Standard

Section 33 of the DPA 2019 entitles data subjects to receive their personal data in a structured, commonly used, machine-readable format. For a digital credit provider, best practice is to embed this capability directly into the application as a self-service feature, reducing support workloads and demonstrating active compliance.

The portability response should be formatted as a JSON payload containing: verified identity (masked), account history (all loans, disbursement dates, repayment records), third-party transmission logs (recipients, purposes, timestamps), and consent history (what was consented to and when). This format satisfies both the DPA 2019 Section 33 obligation and the GDPR Article 20 portability right for EU data subjects.

✍️ **Reflection Question**

A borrower submitted a SAR on Day 1 requesting all data held about them. On Day 18, your team discovers that your archived call recordings from 2023 were stored in a separate legacy system and were not included in the initial scope assessment. What are your obligations? What are the risks? What should you do?

Your answer: _____
_____
_____

✓ **Module Completion Checklist**

- ☐ SAR intake process documented: designated recipient email, maximum 2-hour internal escalation to DPO
- ☐ SAR register maintained: logs request date, identity verification date, response date, and response content
- ☐ All data systems mapped against SAR scope: production DB, archives, call recordings, third-party logs
- ☐ Exemption justification template created: standard language for redactions with statutory basis pre-drafted
- ☐ 21-day alert set in compliance calendar: DPO notified at Day 14 if response not yet dispatched
- ☐ In-app data portability feature implemented or roadmapped — JSON export functional

MODULE 7

# Data Protection Impact Assessments (DPIA)

Key Statutes: DPA 2019 Section 35(2) · Data Protection (General) Regulations 2021 Regulation 7 · GDPR Article 35 (for EU data subjects) · ODPC Guidance on DPIAs (2023)

## 7.1 The DPIA — What It Is and When It Is Mandatory

A Data Protection Impact Assessment is a formal prospective risk assessment conducted before a new processing activity is launched or a material change is made to an existing processing activity. Section 35(2) of the DPA 2019 makes it legally mandatory wherever a proposed processing activity is 'likely to result in high risk to the rights and freedoms of individuals.'

The six statutory triggers for a mandatory DPIA in the fintech context are:

- Using automated systems to evaluate credit eligibility or perform behavioural profiling (MANDATORY for all ML-based credit scoring systems)
- Processing sensitive personal data on a large scale — biometric data, precise location, financial statements
- Systematic monitoring of data subjects' financial behaviour or geographic movement over time
- Deploying new technology or migrating to a new cloud infrastructure — even if the underlying data flows do not change
- Linking your internal borrower database with external commercial registries, CRBs, or government databases
- Transferring personal data outside Kenya — to any cloud provider hosting data in a non-Kenyan jurisdiction

ODPC CONSULTATION: Where your DPIA concludes that residual risk remains HIGH after all mitigation measures are applied, Section 35(6) of the DPA 2019 requires that you consult the ODPC before commencing the processing. The ODPC has up to 8 weeks to respond. Commencing the processing before the ODPC responds is a criminal offence under the Act.

## 7.2 The Six-Section DPIA Document — Worked FinTech Example

The following is a completed DPIA for a machine-learning credit scoring system processing 50,000 borrower profiles. Use this as a template, adapting the specific details to your own processing activity.

**SECTION 1 — EXECUTIVE SUMMARY:**

Processing Activity: Deployment of a machine-learning credit scoring algorithm that processes borrower mobile metadata, financial transaction patterns, and CRB credit history to generate automated loan approval decisions for the ApexLoan digital lending platform. Data Controller: Apex Digital Credit Limited (ODPC Ref: DCP-2022-09841) Data Protection Officer: [Name] DPIA Prepared By: [Name, Title] DPIA Review Date: [Date] DPIA Approval Status: [APPROVED / PENDING / REQUIRES ODPC CONSULTATION]

**SECTION 2 — DESCRIPTION OF PROCESSING:**

Data subjects: active borrowers (approx. 50,000 registered users). Data categories: biometric face verification (90-day retention), National ID (7-year POCAMLA retention), mobile transaction metadata (consent-based, 24-month retention), coarse geo-location (LIA-based, 12-month retention), CRB credit history (7-year POCAMLA retention). Legal basis: contract performance (Section 30(1)(b)) for core processing; explicit consent (Section 30(1)(a)) for SMS metadata; legal obligation (Section 30(1)(c)) for CRB reporting.

**SECTION 3 — NECESSITY & PROPORTIONALITY:**

| Data Category | Necessary? | Proportionate? | Alternative Considered |
|---|---|---|---|
| National ID | Yes — statutory KYC requirement | Yes — minimum required for IPRS verification | None — statutory mandate removes discretion |
| Biometric Face Image | Yes — liveness detection and fraud prevention | Proportionate for first-use KYC; deleted at 90 days | Text-based OTP considered but rejected as insufficient for liveness |
| SMS Transaction Metadata | Yes — primary alternative credit signal | Proportionate only with explicit, specific consent | CRB data alone considered; SMS adds predictive value without over-collection |
| Contact List Data | NO — not necessary for credit assessment | Not proportionate — disproportionate privacy intrusion | No acceptable alternative that uses contact data — processing prohibited |

**SECTION 4 — RISK IDENTIFICATION:**

| Risk | Likelihood | Severity | Inherent Risk | Mitigation | Residual Risk |
|---|---|---|---|---|---|
| ML model produces biased rejections based on proxy discrimination | High | Critical | CRITICAL | 6-monthly bias audit; human review for all rejections; diverse training data | MEDIUM |
| Biometric data breach | Medium | Critical | HIGH | Isolated S3 bucket; unique AES-256 key; 90-day deletion; access log per query | LOW |
| DCA agent misuses shared borrower data | High | Medium | HIGH | 48hr destruction clause; unannounced audit rights; call recording requirement | MEDIUM |
| Cross-border transfer to AWS Cape Town without adequate safeguards | Low | High | HIGH | SCCs executed; AWS DPA signed; transfer risk assessment completed | LOW |

**SECTIONS 5 & 6 — MITIGATION & DPO SIGN-OFF: [Complete per your specific activity]**

> ✍️ **Reflection Question**
>
> Identify the single highest-risk processing activity in your current DCP operations. Using the Section 7.2

template above, complete Sections 1–4 of a DPIA for that activity. Where does the residual risk land? Does it require ODPC consultation under Section 35(6)?

Your answer: _____
_____
_____

### ✓ Module Completion Checklist

- ☐ All processing activities screened against the six DPIA triggers in Section 7.1
- ☐ DPIA completed for ML credit scoring system — minimum 4 sections documented
- ☐ Residual risk rating confirmed by DPO in writing before launch
- ☐ ODPC consultation initiated if any residual risk remains HIGH after mitigation
- ☐ DPIA review scheduled for 12 months from initial completion or upon any material change
- ☐ DPIA register maintained: one entry per processing activity, showing status and DPO sign-off date

# Quick Reference Glossary — Statutory Definitions

| Term | Statutory Definition | Source |
|---|---|---|
| Personal Data | Any information relating to an identified or identifiable natural person | DPA 2019, Section 2 |
| Sensitive Personal Data | Data revealing racial/ethnic origin, political opinions, religious beliefs, genetic data, biometric data used for identification, health data, sexual orientation, or similar | DPA 2019, Section 2 |
| Data Controller | A natural or legal person who determines the purpose and means of processing personal data | DPA 2019, Section 2 |
| Data Processor | A natural or legal person who processes personal data on behalf of a data controller | DPA 2019, Section 2 |
| Consent | Any freely given, specific, informed, and unambiguous indication by a data subject of their agreement to processing | DPA 2019, Section 2 |
| Processing | Any operation performed on personal data including collection, recording, storage, use, disclosure, erasure or destruction | DPA 2019, Section 2 |
| DPIA | A systematic description and assessment of data processing operations to identify and mitigate risks to data subjects' rights | DPA 2019 Section 35(2) |
| DPO | Data Protection Officer — appointed under Section 18(5), registered with ODPC, advises on compliance | DPA 2019, Section 2 / Section 18 |
| Profiling | Automated processing of personal data to evaluate personal aspects, particularly financial situation, behaviour, or movements | DPA 2019, Section 2 |
| Pseudonymisation | Processing so that data can no longer be attributed to a specific subject without additional information | GDPR Article 4(5) — incorporated by reference |

# Contact & Further Advisory Services

For bespoke compliance advisory, ODPC registration assistance, Data Protection audits, DPIA preparation, staff training, and retained data protection counsel:

**Patrick Muchangi — Advocate of the High Court of Kenya**

Data Protection Counsel & Governance Architect — Muchangi Patrick & Associates Advocates

Email: muchangi@lawyer.com · Phone: +254 722 878 607