PROFESSIONAL LEGAL CERTIFICATION PROGRAMME

Data Protection & GDPR Compliance

A Practical Course Manual for Legal & Compliance Practitioners

FRAMEWORK	COMPARED WITH	AUTHORITY	LEVEL
Kenya DPA 2019	UK GDPR / EU GDPR	ODPC Kenya	Practitioner

AUTHORED BY

Patrick Muchangi

Advocate of the High Court
Data Privacy Counsel & Governance Architect
Board Advisory on ODPC & GDPR Compliance
Data Protection Audits, Staff Training Manuals & Retainer Advisory

muchangi@lawyer.com | +254 722 878 607

DAY 1 · CHAPTER ONE

The Evolutionary Timeline of Privacy Law

Tracing the legal journey from post-war human rights declarations to enforceable digital data governance frameworks in Kenya and the United Kingdom.

1

PHASE 1 · 1948

The Post-WWII International Foundation

Article 12 — Universal Declaration of Human Rights

Adopted by the United Nations General Assembly in 1948, the UDHR was a direct response to the horrific state surveillance, arbitrary home invasions, and unchecked communications interceptions perpetrated by totalitarian regimes during World War II.

STATUTORY TEXT

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Analytical Legal Takeaways

Spatial & Physical Framing

Privacy was viewed through a spatial, physical, and territorial lens — protecting the body, home, and analog correspondence from state intrusion.

Negative Right

It functioned primarily as a negative right — a shield telling the state: "Keep out of the citizen's private domain."

! THE CONCEPTUAL GAP

Article 12 lacked any concept of informational self-determination or data governance, as modern computer networks, cloud databases, and digital profiles did not yet exist.

2

PHASE 2 · 1980–1995

The Digital Shift & The European Blueprint

As computers began processing data globally, international bodies realized that physical privacy protections were no longer sufficient to secure intangible digital records.

The OECD Privacy Guidelines (1980)

The OECD issued the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, introducing the concepts of Data Minimization and Purpose Limitation — the baseline vocabulary of modern data protection law worldwide.

The EU Data Protection Directive 95/46/EC (1995)

The Shift

Privacy evolved from basic protection against home invasions into a strict requirement for informational privacy.

The Mechanism

Legally defined Data Controllers and Data Processors for the first time, establishing that individuals have a right to know how their data is being used.

! THE LIMITATION

As a directive, it was not directly enforceable across borders — each EU member had to write its own national laws, creating an uncoordinated, fragmented regulatory landscape across Europe.

3

PHASE 3 · 2016/2018

The Golden Standard — The EU GDPR

The GDPR was adopted in 2016 and became fully enforceable in May 2018, replacing the 1995 Directive. It represents the global gold standard for modern data protection law.

Critical Legal Innovations of the GDPR

Extraterritorial Effect

Applies to any organization globally if it processes data of individuals inside the EU, regardless of where the company is based.

Severe Penalties

Up to €20 Million or 4% of global annual turnover — turning privacy into a critical corporate liability.

Enhanced Rights

The Right to be Forgotten (Erasure) and the Right to Data Portability became actionable digital rights.

Privacy by Design

Companies must build security and privacy directly into systems before launch — not as an afterthought.

4

PHASE 4 · 2010–PRESENT

The Kenyan Constitutional & Statutory Framework

Article 31 — Constitution of Kenya, 2010

STATUTORY TEXT

"Every person has the right to privacy, which includes the right not to have — a) their person, home or property searched; b) their possessions seized; c) information relating to their family or private affairs unnecessarily required or revealed; or d) the privacy of their communications infringed."

The Direct Bridge to the Data Protection Act, 2019

While Article 31 created the constitutional right, it lacked administrative machinery to punish private companies that misused data daily. Parliament enacted the Kenya Data Protection Act, 2019 (DPA) to give Article 31 real, operational teeth:

The ODPC
Established the Office of the Data Protection Commissioner as an independent regulator.

Art. 31(c) → Sec. 25
Translated "information unnecessarily required" into the statutory Principle of Data Minimization.

Art. 31(d) → Sec. 37
Translated "privacy of communications infringed" into strict Direct Marketing Penalties.

Financial Leverage
Brought the GDPR fine mechanism into Kenyan law — up to KES 5 Million.

EXAM & PRACTICE INSIGHT

Privacy is no longer just a passive human right to be left alone. In Kenya, it is an active, constitutionally mandated business obligation requiring technical access controls, formal portal registrations, and transparent data architectures.

MODULE 1 · LEGAL DEFINITIONS

The 5 Pillars of Section 2

Classifying actors, data types, and roles under the Kenya Data Protection Act

1 Data Subject

STATUTORY DEFINITION

"An identifiable natural person who is the subject of personal data."

LEGAL NUANCE

The law protects natural persons (living individuals). It does not apply to corporate bodies, registered companies, or deceased individuals.

PRACTITIONER APPLICATION

When auditing a private academy, the Data Subjects are the students, their parents, and the school staff. When auditing a property firm, the Data Subjects are the tenants.

2 Personal Data

STATUTORY DEFINITION

"Any information relating to an identified or identifiable natural person."

LEGAL NUANCE

This includes anything that can directly or indirectly identify a human being — online identifiers (IP addresses, location data, usernames) and physical identifiers (ID numbers, phone digits, vehicle plates).

PRACTITIONER APPLICATION

An M-Pesa transaction log, an open visitor book entry at a gate, or a student's full name on a report card are all legally classified as Personal Data.

3 Sensitive Personal Data (Special Category)

STATUTORY DEFINITION

"Data revealing the natural person's race, health status, ethnic origin, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of their children, parents, spouse or spouses, sex or the sexual orientation of the data subject."

LEGAL NUANCE

Processing these datasets triggers intense statutory scrutiny. Under Section 29, it is generally prohibited unless specific, strict exceptions apply (such as explicit consent).

PRACTITIONER APPLICATION

Healthcare Clinics: Patient diagnoses (health status). SACCOs / Landlords: Title deeds, payslips (property details). Schools: Birth certificates and parent logs (family details). Office Gates / Gyms: Fingerprint clocks or facial scans (biometric data).

4 Data Controller

STATUTORY DEFINITION

"A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data."

LEGAL NUANCE

This is the entity that calls the shots — deciding why data is collected and how it will be utilized. They carry the primary legal and financial liability under the Act.

PRACTITIONER APPLICATION

The business owners, directors, and boards running Dormans Coffee, Peponi School, Verona Hotel, or RFH Healthcare are all legally classified as Data Controllers — your primary target clients.

5 Data Processor

STATUTORY DEFINITION

"A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller."

LEGAL NUANCE

The processor does not own or decide anything about the data — they are hired by the Data Controller to perform a specific technical task.

PRACTITIONER APPLICATION

If a school uses a local tech platform to send automated bulk SMS report card alerts, the school is the Data Controller and the Bulk SMS Company is the Data Processor. Under Section 42, they must execute a formal Data Processing Agreement (DPA).

MODULE 1 · CORE PRINCIPLES

The 8 Core Data Protection Principles

Sections 25 & 30 of the Kenya DPA 2019 compared with Articles 5 & 6 of the UK GDPR

The systematic analysis below maps each of the eight foundational data protection principles against their dual statutory provisions — showing how Kenya's DPA and the UK GDPR align, where they diverge, and how each principle translates into observable corporate compliance obligations.

1 Lawfulness, Fairness & Transparency

Kenya: Section 25(a)
UK: Article 5(1)(a)

LEGAL MECHANICS

Data controllers must process personal identifiers strictly according to the law (Lawfulness), avoid deceptive gathering practices (Fairness), and clearly communicate the tracking, use, and distribution of data to the individual (Transparency).

UK GDPR
Interprets transparency through strict ICO guidelines mandating layered privacy notices.

Kenya DPA
ODPC focuses heavily on ensuring users understand how their data will be processed prior to ingestion.

PRACTITIONER APPLICATION
Businesses must place a clear Privacy Policy on their platforms and avoid hidden processing logic.

! AUDIT RED FLAG
A website tracking cookies or capturing intake profiles without displaying a clear privacy notice in the footer.

2 Purpose Limitation

Kenya: Section 25(b)
UK: Article 5(1)(b)

LEGAL MECHANICS

Personal information must be gathered for specific, explicit, and legitimate purposes. It cannot be repurposed for secondary objectives that are incompatible with those initial parameters.

UK GDPR

Permits broader secondary processing for public interest archiving, scientific research, or statistical compilation under Article 89.

Kenya DPA

Requires clear functional alignment with the primary reason for collection, unless explicit secondary consent is secured.

PRACTITIONER APPLICATION

A medical clinic collecting patient phone numbers for appointment updates cannot hand that database to an internal marketing unit without separate consent.

! AUDIT RED FLAG

Customer contact databases built for operational service delivery being repurposed for promotional marketing campaigns.

3 Data Minimization

Kenya: Section 25(c)
UK: Article 5(1)(c)

LEGAL MECHANICS

Data processing must be adequate, relevant, and strictly limited to what is necessary for the stated purposes.

UK GDPR

Enforces this by auditing whether alternatives that use less data are available.

Kenya DPA

Directly translates Article 31(c) of the Constitution of Kenya 2010 — "information unnecessarily required."

PRACTITIONER APPLICATION

A Wi-Fi landing page or contact form should only require a name and telephone number — not ID numbers or marital status.

! AUDIT RED FLAG

Customer intake forms mandating sensitive personal details that have no functional connection to the service being delivered.

4 Data Accuracy

Kenya: Section 25(d)
UK: Article 5(1)(d)

LEGAL MECHANICS

Data controllers must take every reasonable step to ensure inaccurate or misleading personal records are erased, corrected, or updated without delay.

UK GDPR
Links accuracy directly to automated financial credit scoring.

Kenya DPA
Grounded in Section 26 data subject correction rights. Applies heavily to utility databases and employee payroll records.

PRACTITIONER APPLICATION
Organizations must build functional profile updating tools or clear communication pathways allowing clients to correct their data records.

! AUDIT RED FLAG
Maintaining outdated customer contact registries or financial records without providing a mechanism for users to submit corrections.

5 Storage Limitation

Kenya: Section 25(e) + 39
UK: Article 5(1)(e)

LEGAL MECHANICS

Personal identifiers must not be retained indefinitely. They must be destroyed or anonymized once the primary objective for their collection is fulfilled.

UK GDPR
Enforces strict, industry-specific retention maximums under the Limitation Act 1980.

Kenya DPA
Section 39 allows retention for lawful optimization, historical tracking, or explicitly sanctioned legal mandates.

PRACTITIONER APPLICATION
Implementing an active corporate Data Retention and Secure Disposal Schedule.

! AUDIT RED FLAG
Storing complete digital profiles of past tenants, students, or clients who severed their contracts years ago.

6 Data Subject Rights Realization

Kenya: Section 25(f) + 26
UK: Articles 12–23

LEGAL MECHANICS

Data processing must explicitly support and facilitate the execution of the data subject's legal rights, including access, correction, erasure, and blocking.

UK GDPR
Outlines distinct timelines and processes for handling Data Subject Access Requests (DSARs).

Kenya DPA
Focuses broadly on ensuring clients are not blocked from exercising their rights.

PRACTITIONER APPLICATION
Providing accessible data access forms or a dedicated privacy email address (e.g., privacy@company.com) to handle client rights requests.

! AUDIT RED FLAG
An enterprise ignoring a client's formal email request to purge their contact records from its active marketing databases.

7 International Data Transfer Restrictions

Kenya: Section 25(g) + 48–50
UK: Articles 44–50

LEGAL MECHANICS

Personal identifiers cannot be transferred out of the domestic jurisdiction unless the destination country guarantees adequate data protection laws or explicit regulatory approvals are secured.

UK GDPR
Utilizes International Data Transfer Agreements (IDTAs) and Addendums to the EU Standard Contractual Clauses (SCCs).

Kenya DPA
Section 48 conditions require verifying that the recipient jurisdiction maintains equivalent privacy protections and filing transfer confirmations with the ODPC.

PRACTITIONER APPLICATION
Reviewing whether cloud infrastructure or bulk processing solutions host client databases on foreign servers that lack reciprocal data laws.

! AUDIT RED FLAG
Storing sensitive local datasets on overseas cloud hosting accounts without reviewing cross-border data rules or obtaining ODPC approvals.

8 Data Security & Technical Safeguards

Kenya: Section 25(h) + 41
UK: Article 5(1)(f)

LEGAL MECHANICS

Data controllers must implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration, or data leaks.

UK GDPR	Kenya DPA
Heavily penalizes failures to use modern security tools like multi-factor authentication (MFA).	Focuses on a mix of digital safety and physical file security — encryption plus physical access controls.

PRACTITIONER APPLICATION

Deploying secure HTTPS encryption across all web contact forms, configuring database access locks, and training staff on basic data safety.

! AUDIT RED FLAG

Operating a public-facing website on an unencrypted HTTP link while capturing customer names, telephone paths, and national identification numbers.

SECTION 2 — COMPARATIVE MAPPING: LEGAL GATEWAYS FOR DATA PROCESSING

Comparative Mapping — Legal Gateways for Data Processing

Processing personal data is unlawful unless it passes through at least one mandatory legal gateway under Section 30 of the Kenya DPA 2019 or Article 6 of the UK GDPR. Organizations cannot collect data first and look for a justification later.

1 Explicit Consent

Kenya: Section 30(1)(a)
UK: Article 6(1)(a)

LEGAL THRESHOLD

Consent must be a freely given, specific, informed, and unambiguous indication of the individual's wishes, confirmed by a clear affirmative action.

PRACTITIONER APPLICATION

A website user actively checking an un-ticked box that reads: "I agree to the privacy policy and consent to receiving marketing newsletters."

! COMMERCIAL TRAINING INSIGHT

Pre-ticked checkboxes or text that says "By continuing to browse this site you accept our terms" are invalid

and do not constitute valid legal consent in either jurisdiction.

2 Performance of a Contract

Kenya: Section 30(1)(b)
UK: Article 6(1)(b)

LEGAL THRESHOLD

Processing is lawful if it is necessary to enter into or perform a contract to which the data subject is a party.

PRACTITIONER APPLICATION

A logistics firm processing a client's home delivery address to ship a package they purchased online.

! COMMERCIAL TRAINING INSIGHT

This gateway only covers data strictly required to fulfill the contract. Collecting unrelated personal details under this ground violates the principle of data minimization.

3 Legal Obligation of the Data Controller

Kenya: Section 30(1)(b)
UK: Article 6(1)(c)

LEGAL THRESHOLD

Processing is permitted if it is required to comply with a statutory legal obligation imposed on the business.

PRACTITIONER APPLICATION

A company capturing employee national ID numbers, KRA PINs, and NHIF details to process monthly payroll taxes.

! COMMERCIAL TRAINING INSIGHT

Organizations must be able to cite the specific piece of legislation — such as the Employment Act or the Income Tax Act — that requires them to collect that data.

4 Protection of Vital Interests

Kenya: Section 30(1)(c)
UK: Article 6(1)(d)

LEGAL THRESHOLD

Processing is allowed if it is necessary to protect the life or essential physical safety of the data subject or another natural person.

PRACTITIONER APPLICATION

A hospital emergency room sharing an unconscious patient's blood type and medical history with an attending surgeon following an accident.

! COMMERCIAL TRAINING INSIGHT

This gateway is strictly reserved for life-or-death situations and cannot be used for routine business operations.

5 Public Task or Statutory Duty

Kenya: Section 30(1)(d)
UK: Article 6(1)(e)

LEGAL THRESHOLD

Processing is lawful if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

PRACTITIONER APPLICATION

A government agency or county enforcement unit collecting vehicle license plate data through traffic monitoring cameras.

! COMMERCIAL TRAINING INSIGHT

This ground is primarily used by public sector bodies and state agencies, rarely by private SMEs.

6 Legitimate Interests

Kenya: Section 30(1)(e)
UK: Article 6(1)(f)

LEGAL THRESHOLD

Processing is allowed if it is necessary for the legitimate interests of the business or a third party, provided those interests are not overridden by the fundamental rights and freedoms of the individual.

PRACTITIONER APPLICATION

An office complex recording visitor names at the reception desk to secure the physical building against trespassers.

! COMMERCIAL TRAINING INSIGHT

To safely rely on this ground, businesses must conduct and document a formal Legitimate Interests Assessment (LIA) balancing exercise. Note: In the UK GDPR, public authorities cannot rely on legitimate

interests for their official tasks.

SECTION 3 — THE COMPLIANCE AUDIT FRAMEWORK & RISK REGISTER

The Compliance Audit Framework & Risk Register

Use this practical audit framework during professional training sessions or corporate consulting engagements to identify operational privacy risks:

Operational Process	Observed Exposure	Likely Violation	Required Remediation
User Intake Channels	Public web forms capturing personal data over unencrypted HTTP lines.	Section 25(h) / Section 41 (DPA) Article 5(1)(f) (UK GDPR)	Force universal HTTPS encryption across all corporate web assets immediately.
Marketing Campaigns	Sending promotional SMS updates to clients without providing a free opt-out or "STOP" mechanism.	Section 37 (DPA) Article 6(1)(a) (UK GDPR)	Re-engineer communication systems to include a clear, functional opt-out tool.
Visitor Management	Open physical logbooks at reception desks that allow visitors to view past entries.	Section 25(a) & (h) / Section 41 Article 5(1)(a) & (f)	Replace open logbooks with secure individual passes or password-protected digital sign-in screens.
Data Retention Policies	Archiving historical customer profiles indefinitely without clear deletion schedules.	Section 25(e) / Section 39 (DPA) Article 5(1)(e) (UK GDPR)	Draft and enforce a formal Data Retention and Secure Disposal Schedule.

SECTION 4 — CURATED RESEARCH & BIBLIOGRAPHY: MODULE 1

Curated Research & Bibliography — Module 1

Statutory Foundations & Regulatory Texts

REGULATORY TEXT

ODPC Kenya: The Data Protection General Regulations, 2021. Access via ODPC Portal.

REGULATORY GUIDE

UK ICO: Guide to the UK GDPR. Comprehensive breakdowns of the 6 lawful bases and the Legitimate Interests Assessment (LIA) framework. Access via ICO Official Site.

STATUTORY TEXT

Kenya Law: The Data Protection Act, No. 24 of 2019. Access via Kenya Law Portal.

Authoritative Legal Articles & Publications

LEGAL ARTICLE

CIPIT: Data Protection Compliance Handbook for African SMEs — detailing how data minimization and consent operate within developing regional markets.

ACADEMIC TEXT

Bygrave, L. A. (2014): Data Privacy Law: An International Perspective. Oxford University Press.

JOURNAL

Kunghs, C. (2020): The Extraterritorial Reaches of Data Protection: Comparing GDPR Standards with Emerging Regulations. Journal of Internet Law.

Seminal Judicial Precedents

KENYAN PRECEDENT

Nisha v. ODPC [2023]: Landmark Kenyan ruling affirming that processing personal information without a documented legal basis under Section 30 results in immediate liability and regulatory fines.

EU PRECEDENT

Google Spain SL v. AEPD [2014] (ECJ): The historic global precedent formally establishing the "Right to be Forgotten," which heavily influenced Section 26 of the Kenyan DPA and Article 17 of the UK GDPR.

MODULE 2 · TECHNICAL & ORGANISATIONAL SAFEGUARDS

DPIAs, Risk Quantification & TOMs

Sections 31 & 41 of the Kenya DPA 2019 compared with Articles 32 & 35 of the UK GDPR

SECTION 1 — DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

Data Protection Impact Assessments (DPIAs)

Statutory Foundations & Legal Triggers

Kenya — Section 31

A DPIA is legally mandatory prior to initiating any automated processing operations likely to result in high risk to the rights and freedoms of data subjects.

UK GDPR — Article 35

Same mandatory DPIA obligation, with the ICO publishing an explicit "Blacklist" of operations that automatically mandate a DPIA.

THE 4 SPECIFIC MANDATORY TRIGGERS

1. **Systematic and Extensive Evaluation:** Profiling or automated decisions that produce legal or similarly significant effects on individuals.
2. **Large-Scale Processing of Special Categories:** Managing vast quantities of health records, political affiliations, genetic profiles, or criminal data.
3. **Systematic Monitoring of Publicly Accessible Areas:** Installing commercial-scale CCTV monitoring loops in public spaces, shopping centers, or residential estates.
4. **Use of New or Emerging Technologies:** Implementing AI, automated drone surveillance, or biometric tracking (fingerprints, facial recognition).

Comparative Jurisdictional Nuances

🇰🇪 Kenya — Section 31(1)

A data controller must submit their completed DPIA report to the ODPC for review sixty (60) days before launching the technology. If the ODPC determines risks are too high, they can issue a formal stop order.

🇬🇧 UK — Article 35 + 36

The controller runs the DPIA locally. They only formally consult the ICO under Article 36 if internal screening indicates they cannot bring residual risks to a safe level.

Practical Institutional Deployment Checklist

Systemic Description
A written flow mapping how data enters, travels, is stored inside, and is ultimately deleted from the company's servers.

Necessity Assessment
A clear justification proving that data collection is proportionate and cannot be achieved using less intrusive methods.

Risk Log
A detailed list of potential vulnerabilities, data leaks, unauthorized access points, or external security breaches.

Mitigation Matrix
The exact technical defenses (encryption, firewalls, tokenization, limited access windows) deployed to neutralize each identified threat.

SECTION 2 — THE MATHEMATICAL RISK QUANTIFICATION PROTOCOL

The Mathematical Risk Quantification Protocol

DPOs must not guess risk levels. They should utilize a standardized Mathematical Risk Matrix Formula to quantify vulnerability before and after applying technical controls.

THE RISK ASSESSMENT FORMULA

$$R = L \times I$$

Risk Score = Likelihood of Occurrence × Severity of Impact

Likelihood Scale (L) — 1 to 5
1 — Rare: Highly unlikely; requires exceptional circumstances. 2 — Unlikely: Might happen occasionally in specific conditions. 3 — Possible: Could easily occur in regular operations. 4 — Likely: Expected to happen repeatedly under standard workflows. 5 — Almost Certain: Highly probable; clear lack of existing defenses.

Severity Scale (I) — 1 to 5
1 — Negligible: Minor internal issue; zero external impact. 2 — Minor: Low consumer disturbance; data easily contained. 3 — Moderate: Medium impact; standard data leaks with regulatory warnings. 4 — Major: Severe; sensitive financial records exposed, identity fraud risk. 5 — Catastrophic: Mass breach; class-action lawsuits, maximum ODPC fines.

Practical Risk Assessment Case Study

The Target: Ruiru Private Hospital deploying an online patient registration app that passes clinical diagnoses over an unencrypted HTTP connection.

🔴 **Pre-Control Calculation**

Likelihood (L): 5 — Unencrypted networks are trivial for bad actors to intercept. Severity (I): 5 — Leaking medical histories causes immediate, severe harm. INITIAL RISK SCORE: 5 × 5 = 25 — CRITICAL EXPOSURE

🟢 **Post-Control Remediation**

Changes: Force TLS/HTTPS, restrict DB access to doctors via MFA, implement end-to-end data obfuscation. Likelihood (L): 1 | Severity (I): 2 RESIDUAL RISK SCORE: 1 × 2 = 2 — SAFE RANGE

SECTION 3 — TECHNICAL & ORGANISATIONAL MEASURES (TOMS)

Technical & Organisational Measures (TOMs)

Under Section 41 of the Kenya DPA and Article 32 of the UK GDPR, businesses must implement active technical and organizational security controls.

Essential Technical Safeguards (The Digital Code)

Encryption in Transit

Implementing TLS 1.3 across every company domain, registration page, and intake portal to secure data as it moves.

Encryption at Rest

Ensuring databases, server blocks, and hard drives hosting consumer indices utilize advanced encryption standards (AES-256).

Pseudonymization

Altering data strings so that a record cannot be linked back to a specific human being without a separate, securely locked key.

Vulnerability Scanning

Deploying automated system monitoring toolkits to discover data entry weaknesses and flag unusual traffic bursts.

Essential Organisational Safeguards (The Structural Controls)

Role-Based Access Control

Configuring corporate servers so that data access is restricted on a strict need-to-know basis. A front-desk receptionist should never access employee health records or complete financial databases.

Clean-Desk Policies

Instituting rules requiring physical paper files, visitor log records, and printed ID copies to be cleared from desks and locked away at night.

PRACTITIONER APPLICATION

Vendor Contract Integration: Requiring every external partner (e.g., bulk SMS services or cloud hosts) to execute a strict Data Processing Agreement (DPA) under Section 42 before receiving any company data.

SECTION 4 — RECONCILED TECHNICAL SAFEGUARDS AUDIT TOOLKIT

Reconciled Technical Safeguards Audit Toolkit

Operational Process	Observed Exposure	Likely Violation	Required Remediation
Data Transmission Encryption	App or website form using basic http:// configurations.	R = 5 × 4 = 20 🔴 HIGH LIABILITY	Deploy an active SSL/TLS certificate to force universal HTTPS security across all company assets.
Physical Entry Access Logs	Traditional visitor books sitting open and unguarded at reception desks.	R = 4 × 3 = 12 🟡 MEDIUM RISK	Transition to digital visitor software or individual, flip-cover privacy logs.
Sensitive Vendor Feeds	Exporting raw client contact sheets to third-party marketing tools without an active DPA contract.	R = 4 × 4 = 16 🔴 HIGH LIABILITY	Pause external data sharing until a legally binding Section 42 Data Processing Agreement is signed by both parties.

SECTION 5 — CURATED RESEARCH & BIBLIOGRAPHY: MODULE 2

Curated Research & Bibliography — Module 2

REGULATORY GUIDE

ODPC Kenya: Guidance Note on Data Protection Impact Assessments (DPIAs). Step-by-step frameworks for compiling risk profiles under the Kenyan Act. Access via ODPC Portal.

TECHNICAL STANDARD

NIST: NIST Privacy Framework — A Tool for Improving Privacy through Enterprise Risk Management. Access via NIST Digital Library.

LEGAL ARTICLE

Gellert, R. (2018): Understanding the Data Protection Impact Assessment under the GDPR. Computer Law & Security Review.

JOURNAL

Koops, B. J. (2021): The Technical and Organizational Measures Threshold. European Journal of Law and Technology.

KENYAN PRECEDENT

ODPC v. Roma School: Landmark Kenyan administrative decision penalizing an educational institution for

processing and publishing minors' image data without formal risk assessments or appropriate consent protocols.

UK PRECEDENT

In the Matter of British Airways PLC (2020) — ICO: Foundational UK GDPR precedent issuing a multi-million-pound fine for failing to implement multi-factor authentication and clear database access logs, directly violating Article 32 security obligations.

MODULE 3 · THE DPO & GOVERNANCE FRAMEWORKS

DPO Mandate, DSARs & Breach Notification

Sections 24, 26, 27 & 43 of the Kenya DPA 2019 compared with Articles 37, 38, 39 & 33 of the UK GDPR

SECTION 1 — THE STATUTORY DESIGNATION & MANDATE OF THE DPO

The Statutory Designation & Mandate of the DPO

Mandatory Appointment Criteria

Kenya — Section 24

An institution must formally designate a DPO if: processing is carried out by a public authority; core activities involve systematic and regular monitoring on a large scale; or core activities consist of large-scale processing of sensitive personal data.

UK GDPR — Article 37

Same three-tier mandatory designation criteria apply. The UK ICO provides sector-specific guidance on when the DPO designation is required for private sector entities.

PRACTITIONER APPLICATION

Kenyan Registration Mandatory Categories: Regardless of size or revenue turnover, the ODPC mandates DPO registration for: educational institutions (schools and universities), healthcare providers (clinics and hospitals), hospitality venues, and financial or micro-lending enterprises.

Legal Protections — Independence & Conflict of Interest

Kenya — Section 24(5) & (7)

The DPO must report directly to the highest management level. The law explicitly protects the DPO from being dismissed or penalized for performing their statutory monitoring duties.

UK GDPR — Article 38

Same protections apply. The DPO must have the resources necessary to carry out their tasks and maintain their expert knowledge.

! THE CONFLICT OF INTEREST TRAP

A DPO cannot hold a position within the company that requires them to determine the purposes and means

of processing data. Combining the DPO role with Chief Technology Officer (CTO), Head of Marketing, or Chief Executive Officer (CEO) constitutes an illegal conflict of interest. The DPO cannot effectively audit systems that they designed or manage for business growth.

SECTION 2 — DATA SUBJECT ACCESS REQUESTS (DSAR) MANAGEMENT

Data Subject Access Requests (DSAR) Management

Under Sections 26 and 27 of the Kenya DPA and Chapter III of the UK GDPR, individuals hold enforceable rights over their personal information. The DPO is the structural mechanism responsible for fulfilling these requests.

DATA SUBJECT RIGHTS — Section 26

› Right of Confirmation & Access
› Right of Rectification / Fix
› Right of Erasure / Right to be Forgotten
› Right to Object to Marketing

FULFILLMENT TIMELINES

› Kenya DPA: Respond within 21 days from request receipt.
› UK GDPR: Respond within 1 calendar month (Article 12).

Step-by-Step Corporate DSAR Intake Protocol

1 Identity Verification
Request secure identification credentials to ensure the applicant is the actual data subject. Do not disclose records to unverified email addresses.

2 Scope Assessment
Determine if the request seeks confirmation of processing, a readable digital copy of all records held (Access), the permanent purging of files (Erasure), or the correction of outdated financials (Rectification).

3 Third-Party Redaction
Before exporting any file extract or email chain to the applicant, redact the personal details, telephone numbers, or identifiers of any third parties to prevent an accidental data leak.

4 Issue the Formal Response
Deliver the structured data payload or confirmation of erasure to the subject within the legal statutory timeframe, entirely free of charge.

SECTION 3 — THE 72-HOUR DATA BREACH NOTIFICATION PROTOCOL

The 72-Hour Data Breach Notification Protocol

A data breach is not limited to external hacking events. It includes any unauthorized internal access, accidental deletion, ransomware attack, or physical loss of encrypted storage drives.

The Multi-Tiered Notification Timelines

Notify the Regulator (ODPC / ICO)

Under Section 43(1) Kenya DPA and Article 33 UK GDPR, the controller must notify the regulator within 72 hours of becoming aware of a breach, unless the leak is unlikely to result in a risk to individuals.

Notify Data Subjects

If the breach is highly likely to result in a high risk to the individual's security, identity, or finances, the controller must notify the affected person without delay.

PRACTITIONER APPLICATION

Processor-to-Controller Feed: Under Section 43(2) of the Kenya DPA, a Data Processor who discovers a leak must notify the Data Controller immediately after becoming aware of the incident.

Standardized Statutory Breach Notification Content

FORMAL DATA BREACH REPORT — REQUIRED CONTENT

1. **Nature of the Breach**
   Describe the incident, including the categories and approximate number of data subjects and personal data records compromised.
2. **The DPO Contact**
   State the name, email, and telephone lines of the independent DPO where further compliance metrics can be obtained.
3. **Risk Consequences**
   Detail the potential real-world harm resulting from the leak (e.g., financial fraud, social engineering, physical safety threats).
4. **Remediation Protocols**
   Detail the active technical steps implemented to contain the leak, patch the server vulnerability, and secure system backups.

SECTION 4 — THE CORPORATE PRIVACY REGISTER & DOCUMENTATION LOG

The Corporate Privacy Register & Documentation Log

Under the accountability principle, organizations must actively document their compliance history. The DPO must maintain an internal Corporate Privacy Register consisting of three foundational records:

RECORD OF PROCESSING ACTIVITIES (ROPA)

A master document detailing every data collection pipeline across the business (HR Payroll, Customer Marketing, CCTV Monitoring). It must state why the data is collected, who holds access, where it is stored, and when it will be destroyed.

INTERNAL DATA BREACH REGISTER

A continuous record tracking all internal security incidents, including minor leaks that did not hit the 72-hour regulatory reporting threshold. It must detail the facts, impact, and technical patches applied.

CONSENT LIFECYCLE LOG

A verifiable database recording exactly when and how consumers provided explicit consent (e.g., web timestamp logs of un-ticked checkboxes), alongside a record of when individuals opted out of marketing campaigns.

SECTION 5 — CURATED RESEARCH & BIBLIOGRAPHY: MODULE 3

Curated Research & Bibliography — Module 3

REGULATORY GUIDE

ODPC Kenya: Guidance Note on Data Protection Officers (DPOs). Detailed legal criteria on mandatory designations and workplace independent status. Access via ODPC Portal.

INTERNATIONAL STANDARD

EDPB: Guidelines on Data Protection Officers (WP 243 rev.01). The definitive international standard for analyzing conflicts of interest and corporate compliance governance. Access via EDPB Digital Archive.

ACADEMIC TEXT

Voigt, P. & Bussche, A. (2017): The Enforcement Mandate: Role and Responsibilities of the Data Protection Officer. Springer, Cham.

JOURNAL

Macenaite, G. (2018): The "72-Hour" Breach Notification Rule: Technical Reality vs. Statutory Expectation. International Data Privacy Law.

KENYAN PRECEDENT

ODPC v. Casa Vera Lounge (2023): Landmark precedent penalizing an establishment for publishing a customer's image on social media without consent or internal DPO authorization.

UK PRECEDENT

In the Matter of Carphone Warehouse LTD — ICO: Cornerstone UK decision penalizing systemic delays in internal data breach detection pipelines and failure to immediately surface vulnerabilities to the designated compliance officer.

FINAL CERTIFICATION CHECKLIST

Course Completion Summary

By completing all three modules, your students or institutional clients will have mastered the exact legal, technical, and operational workflows required to function as certified Data Protection Officers and Privacy Advisors.

- ✓ Evolutionary history of privacy law — Phases 1–4 (UDHR → GDPR → Kenya DPA)
- ✓ The 5 statutory definitions under Section 2 of the Kenya DPA
- ✓ The 8 core data protection principles — Sections 25 & 30 / Articles 5 & 6
- ✓ The 6 mandatory legal gateways for lawful data processing
- ✓ DPIA triggers, conduct protocols, and ODPC / ICO submission requirements
- ✓ Mathematical Risk Quantification Protocol (R = L × I)
- ✓ Technical & Organisational Measures (TOMs) — Section 41 / Article 32
- ✓ DPO statutory mandate, independence rules, and conflict-of-interest prohibitions
- ✓ DSAR management — rights, timelines, and the 4-step corporate protocol
- ✓ 72-hour breach notification pipelines and formal report content requirements
- ✓ Corporate Privacy Register — ROPA, Breach Register, Consent Lifecycle Log
- ✓ Full curated bibliography of statutory texts, precedents, and academic sources

Patrick Muchangi · Advocate of the High Court · muchangi@lawyer.com · +254 722 878 607