ADALCI ADVOCATES

LEGAL INSIGHT · DATA PROTECTION AND PRIVACY

Data Protection in Uganda

What the law demands of organisations and individuals.



Harold Atukwatse
Managing Partner, Adalci Advocates
October 2026 · 13 min read

Introduction

Every Ugandan business, institution and organisation that collects a name, a phone number, a National Identification Number or a mobile money record is now a regulated data handler. That covers companies, partnerships, sole proprietorships, NGOs, SACCOs and cooperatives, trusts, churches and mosques, schools, hospitals, sports clubs, government ministries and local governments, right down to the small shop that keeps a customer WhatsApp list.

The Data Protection and Privacy Act has been in force since 2019 and its Regulations since 2021. The grace period that many businesses assumed they had is over. The Personal Data Protection Office (PDPO) now registers data handlers, investigates complaints, issues compliance orders and publishes its findings.

This article sets out what the law requires of registered entities of every kind and of individuals, what happens when they fall short, and how Adalci Advocates helps clients build compliance that survives scrutiny.

The legal framework

Uganda's data protection regime rests on four pillars.

INSTRUMENT	WHAT IT DOES
The Constitution of the Republic of Uganda, 1995, Article 27	Guarantees the right to privacy of person, home, correspondence, communication and property.
The Data Protection and Privacy Act, Cap. 97 (formerly Act No. 9 of 2019)	Sets the principles, duties, data subject rights, offences and penalties for anyone who collects, processes, holds or uses personal data.
The Data Protection and Privacy Regulations, 2021 (S.I. No. 21 of 2021)	Operationalise the Act: registration, data protection officers, impact assessments, breach handling, complaints and fees.
The Personal Data Protection Office (PDPO)	The regulator, established under the National Information Technology Authority, Uganda (NITA-U). It registers data handlers, investigates complaints and enforces compliance.

Sector rules sit on top of this. Financial institutions, telecom operators, gaming and betting companies, health providers and employers each carry additional confidentiality and record-keeping duties under their own statutes and licence conditions. Compliance with the Act does not excuse non-compliance with those rules, and the reverse is also true.

Who the law applies to

The Act applies to any person, institution or public body that collects, processes, holds or uses personal data within Uganda, and to those outside Uganda who process the personal data of people in Uganda. It recognises three roles:

- **Data collector:** the person who collects personal data, for example a bank taking an account opening form.

- **Data processor:** the person who processes data on behalf of a controller, for example a payroll bureau, cloud host or call centre.
- **Data controller:** the person who decides why and how personal data is processed.

One organisation often plays all three roles. "Personal data" means any information about an identifiable individual: names, ID numbers, phone numbers, addresses, photographs, CCTV footage, location data, biometric data, salary records and online identifiers.

The Act applies to "a person, entity or public body". Legal form does not matter. What matters is whether the entity handles personal data. The core duties therefore bind every registered entity in Uganda, including the following:

ENTITY	TYPICAL PERSONAL DATA IT HOLDS
Companies (private, public, limited by guarantee and foreign branches)	Customer, employee, shareholder and director records, KYC files, CCTV footage and marketing lists.
Partnerships, including law, audit and consultancy firms	Client files, identity documents, financial records and staff data.
Sole proprietorships and registered business names	Customer contacts, payment records, delivery addresses and employee details.
SACCOs, cooperatives and money lenders	Member registers, savings and loan histories, guarantor details, national ID numbers and next of kin.
NGOs, community-based and faith-based organisations	Beneficiary records, often including children, health status, refugee and household data, and donor information.
Trusts, foundations and incorporated trustees	Beneficiary, settlor and family records, bank details and succession information.
Schools, colleges and universities	Pupils' and students' records, parents' contacts, medical notes, results and staff files.
Hospitals, clinics, pharmacies and laboratories	Patient records, test results and insurance details, all special personal data.
Associations, sports clubs and federations	Member and player registers, contracts, medical and transfer records, and fan databases.
Government ministries, departments, agencies, statutory corporations and local governments	Citizen, taxpayer, licence-holder, beneficiary and public servant records, often at national scale.

The Act does not distinguish between multinationals and small organisations on the core duties. A sole proprietor running a clinic, a church running a school, or a community SACCO carries the same basic obligations as a listed company. Only registration fees scale with size.

Core obligations of registered entities

The obligations below apply to every entity listed above, whether incorporated, registered or established by statute. In this section, "entity" and "organisation" mean any of them.



1. Follow the data protection principles

Section 3 of the Act requires every data handler to be accountable to the data subject, to process data fairly and lawfully, to collect only what is necessary for a specific purpose, to keep data accurate, to retain it no longer than needed, to be transparent, and to apply appropriate security safeguards. Every other duty flows from these principles.

2. Have a lawful basis, usually consent

Personal data may only be collected or processed with the prior consent of the data subject, unless an exception in section 7 applies. The exceptions include processing authorised by law, performance of a contract with the data subject, compliance with a legal obligation, the prevention or detection of crime, national security, and protection of the data subject's vital interests. Consent must be informed and specific. A pre-ticked box buried in terms and conditions will not hold up.

3. Take extra care with children and special personal data

Data relating to a child may only be processed with the consent of a parent or guardian, or where the law permits. Special personal data, which includes religious or philosophical beliefs, political opinion, sexual life, financial information, health status and medical records, attracts heightened restrictions. Banks, insurers, SACCOs, fintechs, hospitals, schools, NGOs and betting companies handle this category every day.

4. Tell people what you are doing with their data

Before collecting data, the data subject must be informed of the nature and purpose of the collection, who will receive it, whether supplying it is voluntary or mandatory, and their rights. In practice this means a clear, accessible privacy notice at every point of collection: forms, websites, apps, USSD menus and CCTV signage.

5. Register with the PDPO

Every data collector, processor and controller must register with the PDPO under section 29 of the Act and the Regulations. Registration must be kept current and renewed as the Regulations require. Operating unregistered is itself a breach and is often the first thing the PDPO checks when a complaint arrives.

6. Designate a Data Protection Officer

The Act and Regulations require organisations to designate a Data Protection Officer (DPO) responsible for compliance. The DPO should have real authority, direct access to management

and enough independence to raise uncomfortable issues. A DPO in name only does not discharge the duty.

7. Secure the data and manage processors

Section 20 requires appropriate, reasonable technical and organisational measures to prevent loss, damage, unauthorised destruction, unlawful access and unauthorised processing. Where a third party processes data on your behalf, you remain responsible. You need a written agreement binding the processor to equivalent security and confidentiality standards.

8. Report data breaches without delay

Where personal data is accessed or acquired by an unauthorised person, section 23 requires the data handler to notify the PDPO immediately and to take steps to contain the breach. The PDPO may direct that affected data subjects also be notified. A business without an incident response plan will struggle to meet this timeline.

9. Control storage and transfers outside Uganda

Personal data may only be processed or stored outside Uganda on the conditions set by section 19 of the Act. Because this obligation now touches almost every organisation, it is discussed in detail in the next section.

10. Keep data only as long as necessary

Personal data must not be retained longer than necessary for the purpose for which it was collected, unless the law requires otherwise. Once that period ends, the data must be destroyed or de-identified securely. A documented retention schedule is the practical answer.

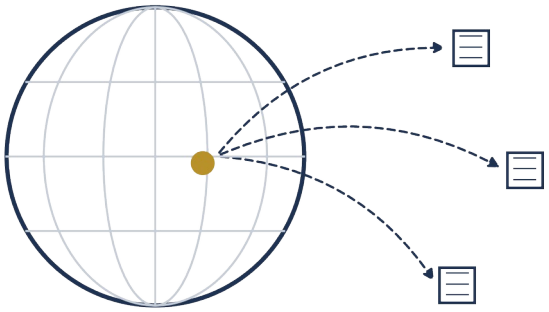
11. Respect data subject rights

Individuals have the right to access their data, to object to processing that causes them damage or distress, to stop direct marketing, to challenge decisions taken solely by automated means, and to have inaccurate data corrected, blocked, erased or destroyed. Every organisation needs a working process to receive, verify and answer these requests within the prescribed time.

12. Assess the risk of new processing

The Regulations require a data protection impact assessment where processing is likely to pose a high risk to data subjects, for example large-scale profiling, biometric systems, CCTV networks or new customer-facing apps. The assessment should happen before launch, not after a complaint.

Storing and transferring data outside Uganda



Most Ugandan organisations already store personal data outside the country, often without realising it. Email on Google Workspace or Microsoft 365, files on Dropbox or OneDrive, customer records in a foreign-hosted CRM, WhatsApp chats, payment gateways and backups on AWS or Azure all sit on servers abroad. The Act does not prohibit this, but it attaches strict conditions.

What the law requires

Under section 19 of the Act, a data collector, processor or controller based in Uganda that processes or stores personal data outside Uganda must ensure that one of two conditions is met:

- **Adequacy:** the country where the data is processed or stored has adequate measures in place for the protection of personal data, at least equivalent to the protection provided by Uganda's Act; or
- **Consent:** the data subject has consented to the data being processed or stored outside Uganda.

The duty rests on the Ugandan entity, not the foreign service provider. "Our cloud provider is compliant" is not a defence unless you have checked and documented it. The other duties also travel with the data: security safeguards, retention limits, breach notification and data subject rights continue to apply wherever the data sits.

Common scenarios

SCENARIO	KEY COMPLIANCE POINT
Cloud email, file storage and office software	Confirm where the provider hosts data, review its data processing terms, and record your adequacy assessment.
Foreign-hosted CRM, HR, payroll or core banking systems	Sign a data processing agreement binding the vendor to security, confidentiality, breach reporting and deletion obligations equivalent to the Act.
Group companies and regional head offices	Intra-group sharing is still a transfer. Put an intra-group data sharing agreement in place and limit what is shared to what is necessary.
International donors, partners and auditors	NGOs, schools and trusts often send beneficiary or student data abroad for reporting. Minimise, anonymise where possible, and cover the transfer in consent forms and partner agreements.
Payment gateways, betting and fintech platforms	Map every third party in the payment chain and confirm the hosting location of transaction and KYC data.

SCENARIO	KEY COMPLIANCE POINT
Medical referrals and diagnostics abroad	Health data is special personal data. Obtain explicit, informed patient consent before records leave Uganda.

Relying on consent

Consent is the simplest route but the most fragile. It must be specific, informed and freely given, and it can be withdrawn. A general clause in standard terms may not satisfy the PDPO, and consent is a poor fit for employees and other relationships where the individual has little real choice. Organisations should not rely on consent alone for large or systematic transfers.

Sector rules may go further

Some sector regulators and licence conditions impose stricter requirements, such as keeping certain records or systems in Uganda, or seeking approval before outsourcing data processing abroad. Financial institutions, payment service providers, telecom operators, gaming and betting operators and public bodies should check their sector rules alongside the Act. Public bodies should also consider national government data hosting policies.

Practical steps

- ☐ Map every system, vendor and partner that stores or accesses personal data outside Uganda
- ☐ Identify the country of hosting for each, including backups and disaster recovery sites
- ☐ Assess and document whether each country offers adequate protection
- ☐ Sign data processing or data transfer agreements with every foreign provider
- ☐ Update privacy notices and consent forms to disclose cross-border storage
- ☐ Apply encryption and access controls so data remains protected in transit and at rest
- ☐ Review sector-specific localisation or approval requirements
- ☐ Revisit the assessment whenever a vendor, hosting region or product changes

Obligations of individuals

The Act is not only a corporate statute. Its offences are framed against "a person", which means individuals can be prosecuted directly.

- **Employees and contractors** who handle customer or staff data must use it only for authorised purposes. Downloading a customer list before leaving for a competitor, or sharing a client's mobile money statement on WhatsApp, can amount to unlawful obtaining or disclosure.
- **Directors, partners, trustees and office bearers** are exposed where their organisation commits an offence with their consent, connivance or neglect. This includes company directors, partners in a firm, trustees, SACCO and cooperative board members, NGO board members, and accounting officers in public bodies. Data protection is therefore a governance duty, not an IT problem.

- **Sole proprietors and professionals** such as doctors, landlords, estate agents, accountants and advocates are data collectors and controllers in their own right, with the same duties as any organisation.
- **Data Protection Officers** carry personal responsibility for monitoring compliance and should document their advice, escalations and decisions.
- **Ordinary individuals** who obtain, disclose, sell or offer to sell another person's personal data without authority commit an offence. Publishing a stranger's ID card, phone records or medical details online is not a private matter.

Consequences of non-compliance

The exposure is criminal, civil, regulatory and commercial, and the four often arrive together.

UGX 4.8m
maximum fine per individual offence

10 years
maximum term of imprisonment

2%
of gross annual turnover for corporate bodies

EXPOSURE	WHAT THE LAW PROVIDES
Criminal offences by individuals	Unlawfully obtaining or disclosing personal data, unlawfully destroying, deleting, concealing or altering it, and selling or offering to sell it are offences. Each carries a fine of up to 240 currency points (UGX 4,800,000), imprisonment of up to 10 years, or both.
Criminal liability of corporate bodies	A corporation that commits an offence under the Act is liable to a fine of up to 2% of its gross annual turnover. This reaches companies, incorporated trustees, cooperatives, SACCOs and other bodies corporate. For a large bank, telco or betting operator, that figure runs into billions of shillings.
Liability of officers and unincorporated entities	Directors, partners, trustees and office bearers who knowingly authorised or permitted the contravention may be prosecuted alongside the organisation. Where the entity is unincorporated, such as a partnership, sole proprietorship or unincorporated association, the individuals who run it carry the exposure personally.
Civil compensation	A data subject who suffers damage or distress because of a contravention may claim compensation from the data collector, processor or controller.
Regulatory enforcement	The PDPO investigates complaints, issues compliance and enforcement directions, and may publish its findings naming the organisation. Public bodies are not exempt.
Institutional fallout	Sector regulators, licensors, donors, banks, investors and multinational counterparties increasingly ask for evidence of compliance. A finding against you can cost licences, tenders, grants, membership trust and contracts.

The PDPO is actively receiving complaints, investigating Ugandan organisations and publishing its decisions. Enforcement is no longer theoretical.

Practical compliance checklist

A business that can tick every box below is in a defensible position.

- ☐ Registered with the PDPO, with registration current
- ☐ Data Protection Officer designated, trained and reporting to management
- ☐ Data inventory mapping what personal data is held, where, why and who can access it
- ☐ Lawful basis recorded for each processing activity, with consent forms that meet the Act
- ☐ Privacy notices at every point of collection, including websites, apps, USSD and CCTV
- ☐ Written data processing agreements with every vendor that touches personal data
- ☐ Cross-border transfer review for cloud, group IT and payment platforms
- ☐ Information security policy with access controls, encryption and staff confidentiality undertakings
- ☐ Breach response plan, tested, with a named team and PDPO notification template
- ☐ Retention and destruction schedule
- ☐ Procedure for handling access, correction, objection and erasure requests
- ☐ Impact assessments for high-risk processing before launch
- ☐ Annual staff training and periodic compliance audit

How Adalci Advocates can assist

Adalci Advocates combines regulatory depth with commercial practicality. Our partners advise companies, partnerships, SACCOs, NGOs, trusts, schools, health providers, sports clubs and public bodies across financial services, gaming and betting, sports and media, real estate and technology, and serve in designated Data Protection Officer roles. We know what the PDPO asks for because we answer to it.

SERVICE	WHAT WE DELIVER
Compliance gap audit	A structured review of your data flows, documents and systems against the Act and Regulations, with a prioritised remediation plan.
PDPO registration	Preparation and filing of registration and renewals for any type of entity, and handling of PDPO queries.
Outsourced Data Protection Officer	An experienced DPO service for organisations that lack in-house capacity, including periodic compliance reports to the board and the PDPO.
Policies and notices	Privacy policies, consent forms, CCTV notices, employee data policies, retention schedules and information security policies drafted for Ugandan law.
Contracts	Data processing agreements, data sharing agreements and vendor due diligence.
Cross-border data review	Mapping of offshore storage and transfers, adequacy assessments, data transfer agreements, consent wording and sector localisation checks.

SERVICE	WHAT WE DELIVER
Impact assessments	Data protection impact assessments for new products, apps, biometric systems and marketing campaigns.
Breach response	On-call support to contain incidents, notify the PDPO and data subjects, and manage regulatory and reputational fallout.
Disputes and investigations	Representation in PDPO complaints and investigations, criminal matters and civil compensation claims.
Training	Board, trustee and management briefings and staff training tailored to your sector and type of entity.

Conclusion

Data protection compliance in Uganda is a legal duty with personal consequences, not a box to tick once. The cost of building a defensible framework is a fraction of a 2% turnover fine, a compensation claim or a public PDPO finding. The organisations that start now will set the standard others are measured against.

To arrange a compliance audit or discuss your obligations, contact:

Harold Atukwatse
Managing Partner, Adalci Advocates
4th Floor Block C, Lugogo House, Plot 42 Lugogo Bypass, Kampala
info@adalci.co.ug · +256 774 088 156
www.adalci.co.ug

This article is for general information and does not constitute legal advice. Specific advice should be sought on particular facts.