DPO PRIVACY CENTRE EAST AFRICA

A STRATEGIC GUIDE TO

Data Protection and Privacy in East Africa

A 2026 Outlook

5 Jurisdictions
6 Contributing Experts
7 Thematic Areas

April, 2026

Table of Contents

Foreword

The enactment of the European Union's General Data Protection Regulation (GDPR) in 2016 marked a turning point not only for European data governance but for data protection globally. Its influence has been felt across jurisdictions on every continent, and the East African region is no exception. While the African Union's Malabo Convention on Cyber Security and Personal Data Protection represented an earlier and deliberate effort to address data governance at a continental level, its practical impact has been constrained by slow ratification across member states. The GDPR's reach, by contrast, derives in large part from the cross-border reality that organisations and governments operating globally must engage, in one way or another, with data connected to EU member states. That practical compulsion has been among the forces shaping the region's legislative trajectory.

Against this backdrop, Kenya, Uganda, Tanzania, Rwanda, and most recently Burundi have each enacted dedicated data protection legislation. The legal frameworks that have emerged across these five jurisdictions are not uniform replicas of the GDPR — they reflect the distinct legal traditions, institutional capacities, and policy priorities of each country. Yet there is a clear convergence around core principles: lawful processing, meaningful data subject rights, supervisory oversight, and organisational accountability. What is perhaps most encouraging is not the legislation itself, but what it has set in motion: regulators being operationalised, enforcement proceedings being initiated, landmark decisions being handed down, and a growing community of practitioners building expertise in this field.

This first edition of the Guide provides a structured analysis of the data protection and privacy landscape across five East African jurisdictions. It examines seven thematic areas — the legislative and regulatory landscape, core compliance requirements and definitions, governance and accountability, enforcement and practical reality, cross-border data transfers, sector-specific and emerging challenges, and the outlook for reform — through the lens of legal and compliance professionals with direct, on-the-ground experience in each country.

The Guide is intended as a practical reference for practitioners, organisations, businesses, investors, students, regulators, and all others with a stake in understanding the current state and future direction of data protection and privacy in East Africa. We hope it proves both reliable and useful.

We extend our sincere gratitude to the six contributing experts whose knowledge, time, and commitment made this publication possible.

ABOUT THE EDITOR

Namugera Joel Peter is an Advocate of the High Court of Uganda, specialising in data protection and privacy law. He heads the Training, Research and Capacity Building Desk at DPO Privacy Centre East Africa, where he leads the organisation's knowledge development and professional training initiatives. He is also an Associate at Onyango and Co. Advocates within the Corporate and Commercial Department, with a broader practice spanning Banking and Finance, Technology, Media and Telecommunications, and Intellectual Property. He is a member of the Association of Privacy Lawyers in Africa (APLA), where he serves on the Research and Legal Team.

About DPO Privacy Centre East Africa

DPO Privacy Centre East Africa is a specialist professional services organisation dedicated to building a culture of data protection and privacy across the region. With a presence spanning six countries, the Centre brings together a team of experienced legal and data protection professionals committed to advancing the profession and promoting the highest standards of privacy practice.

The Centre operates as more than a consultancy. It is an advocate for stronger data governance frameworks, an educator for the next generation of privacy professionals, and a strategic partner for organisations navigating an increasingly complex regulatory landscape. Its work encompasses data protection advisory and compliance services, cybersecurity and AI governance, policy advocacy and research, and training and capacity building programmes for individuals, organisations, and institutions across the region.

Through publications such as this Guide, the Centre seeks to contribute to the broader development of data protection knowledge and practice in East Africa, supporting practitioners, businesses, and regulators in building frameworks that are both effective and trusted.

For permissions and enquiries, contact us at **privacycentreeastafrica@gmail.com**

01 Burundi

1. The Legislative and Regulatory Landscape

1.1 Primary Legal Framework

Burundi's data protection landscape is now defined by a modern, comprehensive framework. The primary legislation is Law No. 1/03 of March 10, 2026 on the Protection of Personal Data, promulgated on 10th March 2026. The law establishes the core principles and obligations for the processing of personal data and marks a significant step in Burundi's digital governance reform.

The right to privacy is constitutionally guaranteed. Article 28 of the Constitution of the Republic of Burundi affirms the right to privacy in personal and family life, the home, and communications, providing a strong foundational principle for the data protection regime.

Beyond the general data protection law, several sectoral laws impose specific privacy and confidentiality obligations that interact with and complement the new regime.

Health Law (Law No. 1/07 of March 12, 2020)
This law mandates strict confidentiality for patient information, extending protection even after death. It grants patients control over how their medical details are shared and treats hospital rooms as private spaces. This creates a high baseline for data handling in the healthcare sector.

Banking Law (Law No. 1/17 of August 22, 2017) and Regulation No. 001/2019
Financial institutions are bound by bank secrecy provisions and specific data protection rules. These include obligations to protect customer data and transactions, limit access to authorised staff, train employees, and implement secure systems for ATMs and online banking, reflecting the heightened sensitivity of financial data.

CONTRIBUTOR

Kankindi Florence is a Senior Associate at KTA Advocates Burundi with over ten years of experience in the legal profession. She specialises in labour law, technology law, and intellectual property, advising businesses and organisations on regulatory compliance and digital infrastructure security. Her practice combines legal expertise with an understanding of the challenges of digital innovation, enabling clients to grow within secure and sustainable legal frameworks. Florence is committed to advancing legal systems that foster innovation and inclusive economic transformation.

Communication Law
Decree-Law No. 100/153 of June 17, 2013 regulates the monitoring of incoming international calls, mandating the use of passive traffic control systems that do not record call content. Operators may only share basic call details — origin, destination, duration — and must exclude content, emails, or texts. Ministerial Order No. 730/1056 of November 7, 2007 governs network interconnections and explicitly requires telecom operators to detail privacy measures in their interconnection agreements, ensuring protection of personal data, private life, and confidential information during transmission or storage.

Labour Code (Law No. 1/11 of November 24, 2020)
The Labour Code imposes a duty of confidentiality on labour and social security inspectors and any personnel involved in inspections or investigations, ensuring that employee-related information gathered during these processes is protected.

Cybercrime Law (Law No. 1/10 of March 16, 2022)
This law provides a broad definition of personal data and establishes criminal penalties for privacy violations. It covers offences such as unauthorised interception of electronic data, fraudulent access to data systems, and the storage of sensitive information without consent. For businesses, particularly in fintech and e-commerce, this law translates into strict consent requirements and heightened scrutiny of data breach incidents.

Press Law (Law No. 1/21 of 12 July 2024)
This law — giving notice of Law No. 1/19 of 14 September 2018, which itself amended Law No. 1/15 of 9 May 2015 governing the press in Burundi — requires journalists and media professionals to respect individuals' private lives while exercising free speech, creating a specific privacy duty for the media sector.

1.2 The Supervisory Authority

The 2026 Data Protection Law provides for the creation of an independent oversight body. Article 42 establishes the Personal Data Protection Agency, which will be responsible for enforcing the law, monitoring how personal data is handled, and ensuring that all data processing follows legal rules.

The Agency is not yet operational. Its duties, structure, staffing, and operational powers will be defined in a separate decree.

2. Core Compliance Requirements & Definitions

2.1 Scope and Applicability

The 2026 Data Protection Law has a broad, extraterritorial scope. It applies to any data controller or processor that uses processing facilities located in Burundi, regardless of whether the entity is established in the country, with the exception of facilities used solely for transit purposes. Where a controller or processor is not established in Burundi, they must designate a local representative, unless the processing they carry out is occasional.

For multinational organisations, this means regulatory exposure may arise even where the parent entity is incorporated abroad, provided processing facilities or operations are based in Burundi.

Lawful Bases for Processing
Under Article 8 of the law, processing of personal data must always be fair, honest, and legal. Processing is permitted only where at least one of the following lawful bases applies:

- The data subject's explicit, specific consent.
- Performance of a contract requested by the data subject.
- Compliance with a legal obligation.
- Protection of a person's vital interests.
- Performance of a public duty.
- A legitimate business interest that does not override the individual's rights — with particular care required where children are involved.

While consent is a common basis in consumer-facing contexts, the availability of other lawful grounds means organisations are not solely reliant on consent for all processing activities.

Sensitive Personal Data
The law imposes heightened restrictions on sensitive categories of personal data. Article 9 prohibits the processing of data revealing racial or ethnic origin, political, philosophical or religious opinions, trade union membership, health data, and biometric data used for selective identification. Limited exceptions are recognised under Article 10, including:

- Explicit consent of the data subject, where the law does not disapply consent.
- Protection of life where consent cannot be obtained.
- Processing by non-profit associations, religious groups, or unions for their legitimate activities.
- Legal proceedings — to initiate, defend, or manage a legal claim.
- Medical emergencies and urgent therapeutic care.
- Health research with the consent of the data subject.

The Minister responsible for civil status may also authorise exceptions for reasons of public interest. Whenever sensitive data is processed, organisations must implement strong security measures, including encryption, strict access controls, secure storage, and regular audits.

2.2 Data Subject Rights

The 2026 law aligns with international standards by granting individuals a suite of enforceable rights over their personal data:

- Right of Access — to know what data is collected and how it is used.
- Right to Rectification — to correct inaccurate or incomplete data.
- Right to Erasure — to request deletion of data under certain conditions.
- Right to Data Portability — to obtain data in a readable format transferable to another service.
- Right to Object — to refuse certain processing, including for direct marketing.

Practical Mechanisms for Exercising Rights

Requests to exercise these rights must be addressed directly to the data controller. Under Article 33, the controller must respond within one month of receiving the request. If the organisation cannot meet this deadline, it must inform the requester and report the delay to the supervisory authority once it is operational.

The law does not prescribe a specific standard form for submitting requests. However, Article 25 sets out the framework for the right of access in particular: any individual may request a copy of their personal data, and the controller must provide it free of charge. Where a request is made electronically, the information must be provided in a commonly used electronic format unless the data subject requests otherwise. Where additional copies are requested, the controller may charge a reasonable fee, the amount of which is determined by reference to the type of data processing and is set by the Ministry of Finance.

Limitations and Exemptions

The exercise of data subject rights is not absolute. Where personal data is linked to matters of national security, defence, or public safety, requests must be channelled through the national data protection authority rather than submitted directly to the controller. The authority appoints one of its members to act on the data subject's behalf, who may be assisted by a colleague. Information obtained may be shared with the individual only to the extent it does not interfere with ongoing investigations, criminal proceedings, protection of public safety, or national security interests.

For medical information, access is not granted directly to the data subject. Instead, the individual must designate a doctor, who receives the information on their behalf to ensure that sensitive medical details are properly explained and understood. These safeguards seek to balance individual rights with broader state and public interest considerations.

3. Governance, Accountability & Ongoing Compliance

3.1 Directors' Duties and Corporate Accountability

The law places significant responsibility on the data controller — defined as the person in charge of data processing. Article 44 outlines a comprehensive list of technical and organisational measures that controllers must implement to protect personal data. These include:

- Controlling access to ensure only authorised staff can view data for which they are responsible.
- Maintaining records of who receives data and verifying their identity.
- Logging access to systems, including what data was viewed or entered and when.
- Preventing unauthorised physical access to premises or rooms where data is stored.
- Protecting storage devices from being read, copied, altered, destroyed, or moved without permission.
- Blocking unauthorised changes, deletions, or additions to the system.
- Preventing unauthorised use of data systems through communication networks.
- Ensuring that data sent or transported cannot be read, copied, changed, or deleted without authorisation.
- Creating backup copies to safeguard data.
- Updating or converting data when needed to ensure long-term usability as technology evolves.

The 2026 law does not create explicit personal liability provisions specifically targeting directors or senior officers. Accountability for governance failures leading to data protection breaches is currently derived from general civil law principles applicable to persons in positions of responsibility. As the enforcement regime matures and secondary regulations are issued, more specific corporate accountability obligations may be introduced.

Data Protection Officer

The 2026 law does not explicitly mandate the appointment of a named Data Protection Officer. However, Article 43 establishes a confidentiality-based governance framework that functions as a practical equivalent. The provision requires that the processing of personal data be carried out exclusively by persons acting under the authority of the data controller and only on the controller's instructions. In selecting such persons, the controller must ensure they offer every guarantee in terms of both technical and legal knowledge and personal integrity. All persons required to process personal data must sign a written undertaking to comply with the Act.

Board Oversight

Boards of Directors are expected to provide active oversight of data protection compliance programmes. This includes ensuring that appropriate internal policies, risk assessments, and reporting mechanisms are in place. As the enforcement environment develops, boards will be expected to demonstrate that they actively supervise compliance rather than delegating responsibility entirely to operational or technical teams.

3.2 Key Annual Compliance Cycle Requirements

The 2026 law establishes ongoing compliance obligations, though some details regarding the annual cycle are expected to be elaborated in secondary regulations.

Data Protection Impact Assessments (DPIAs)

A DPIA is mandatory before commencing any project that involves the processing of personal data and could create serious risks for individuals' rights and freedoms. It is always required where sensitive data — such as health, religious, or ethnic information — is involved. The Data Protection Authority may designate additional situations where DPIAs are required.

The assessment must examine both legal and technical risks, particularly those relating to data security, and must identify the measures to be put in place to mitigate those risks. Once completed, the DPIA must be independently reviewed by the designated data protection officer, whose feedback must be taken into account. The final assessment is then submitted to the Data Protection Authority along with a request for authorisation to proceed.

Breach Notification Requirements

The law sets clear, short timelines for reporting data breaches. Where a breach could put individuals' rights or freedoms at risk, the controller must report it to the supervisory authority within 48 hours of discovery. The report must explain the nature of the breach, its possible consequences, and the steps taken to reduce or fix the damage. If the report is delayed, the reason must be provided.

Where the breach poses a high risk to individuals, affected persons must be notified within 96 hours of the controller discovering the problem. The notification must be clear, explaining the nature of the breach, its potential consequences, the remediation steps taken, and what the affected individuals can do to protect themselves.

Annual Compliance Obligations

The law does not currently specify other recurring annual obligations such as mandatory audits, renewal of certifications, or submission of annual reports to the Authority. It is anticipated that these details will be addressed in the implementing regulations to be developed.

4. Enforcement and Practical Reality

4.1 Regulatory Activity

As the Personal Data Protection Agency is not yet operational, there is no enforcement track record to report. However, the law establishes significant penalties for violations, signalling the direction of future enforcement.

Criminal Penalties

The law establishes a comprehensive criminal penalty framework across Articles 47 to 51. The following provisions are of particular relevance to businesses.

Under Article 47, any person who causes a personal data breach — through loss, leakage, or allowing unauthorised access — faces criminal penalties. For an individual, this means imprisonment of between six months and five years, and/or a fine of between 2 million and 15 million Burundian Francs (BIF). For a company or organisation, the fine ranges from 20 million to 50 million BIF. Where the offending entity is also a major data processor — one that handles large or sensitive datasets — additional consequences apply: suspension from operating for up to six months in cases of repeat offending, and closure of premises where the breach was committed deliberately in furtherance of another crime.

Article 48 addresses unlawful or unfair handling of personal data even where no actual breach occurs. This includes collecting or using data in a dishonest, illegal, or unclear manner, or for purposes not clearly explained, not legitimate, or incompatible with the original purpose of collection. For an individual, penalties include imprisonment of six months to five years and/or a fine of between 500,000 and 10 million BIF. For a company or organisation, fines range from 5 million to 20 million BIF. Where the offending organisation is a major data processor, the fine is doubled — reaching between 10 million and 40 million BIF.

Articles 49 to 51 impose additional penalties for specific violations: blocking or refusing the use of personal data for important public purposes — such as archiving, scientific or historical research, or statistical studies — may result in imprisonment of one to ten years or fines of 500,000 to 10 million BIF, with senior data controllers facing fines of 10 to 50 million BIF. Unlawfully processing sensitive personal data may attract fines of between 1 and 5 million BIF. All penalties under the 2026 law operate in addition to any charges that may be brought under Burundi's Cybercrime Law or the general Penal Code.

It should be noted that the penalty regime established by the 2026 law is primarily criminal in nature. The law does not, at this stage, establish a distinct category of administrative fines — civil sanctions imposed by the Agency independently of criminal proceedings. This distinguishes Burundi's approach from more mature data protection regimes such as the GDPR, where administrative fines are a primary enforcement tool. As the Agency becomes operational and secondary regulations are issued, the development of administrative enforcement mechanisms may follow.

Advisory and Awareness Role

Once operational, the Agency will be expected to provide guidance, develop codes of conduct, and engage with stakeholders to support compliance. These functions are anticipated but not yet active given the Agency's pre-establishment status.

4.2 Private Litigation

The 2026 Data Protection Law does not explicitly establish a statutory right for individuals to seek civil compensation directly through the courts for data protection violations. The law's enforcement architecture is primarily criminal, as set out in the penalty provisions discussed above. However, individuals are not without civil recourse: general civil claims for damages may be pursued under Burundi's Code of Civil Procedure where loss or harm can be demonstrated.

Given the law's recent promulgation, no significant class actions or landmark court cases have yet been brought on data privacy grounds. As awareness of privacy rights develops and the Agency becomes operational, civil society engagement with data protection remedies is expected to grow.

5. Cross-Border Data Transfers

5.1 Transfer Mechanisms

The 2026 Data Protection Law permits cross-border data transfers only where the destination country or organisation ensures an adequate level of protection for the personal data concerned. Adequacy is assessed based on the applicable laws, security measures, processing details, and the nature of the data involved.

Legal Mechanisms

- **Adequacy Decisions:** The Minister of Digital Economy may issue a whitelist of countries deemed to provide adequate protection. In assessing adequacy, the relevant factors include: whether the destination country respects the rule of law, human rights, and fundamental freedoms; whether it has effective general and sector-specific laws on privacy, national security, and public safety; whether it has one or more independent and functioning data protection authorities; and whether it has signed and respected international agreements on the protection of personal data (Articles 15 and 16 of the 2026 law). No such whitelist has yet been published following the law's promulgation in March 2026.
- **DPA-Approved Safeguards:** For transfers to countries not on the adequacy whitelist, organisations must use safeguards approved by the Data Protection Authority. These may include contractual arrangements or other mechanisms that ensure adequate protection for the personal data concerned.
- **Explicit Consent:** Consent may serve as a basis for transfer where it is consistent with other applicable legal grounds.

Practice for Multinational Organisations

In the current environment, multinational companies are managing cross-border and intra-group data transfers through a combination of contractual mechanisms — including intra-group agreements and binding corporate rules — and proactive compliance preparation. Many organisations are already conducting impact assessments for high-risk transfers, particularly where sensitive data categories are involved, in anticipation of the Agency's authorisation processes once it becomes operational.

6. Sector-Specific & Emerging Challenges

6.1 Critical Sectors

Although the 2026 Data Protection Law establishes a general framework applicable across all sectors, industries such as financial services, telecommunications, and public health process personal data at a scale that attracts heightened regulatory attention. These sectors are subject to stricter confidentiality and security obligations under their own regulatory frameworks, which operate alongside the general data protection law rather than replacing it.

This creates a layered compliance environment. Organisations in regulated industries must therefore comply simultaneously with sector-specific requirements and the general data protection principles established under the 2026 law.

- **Financial Services:** Banks and fintech companies handle large volumes of sensitive financial data, including identification records, transaction details, and payment information. These institutions must align their data handling practices with both banking confidentiality obligations under Law No. 1/17 of 2017 and the data protection principles of the 2026 law.
- **Telecommunications:** Telecom operators process extensive subscriber data, including identification records and communication metadata. Because of their role as infrastructure providers for digital services, telecom operators are often among the largest holders of personal data in the economy and must comply with both telecommunications regulation and the personal data protection framework.
- **Healthcare:** Health institutions handle sensitive personal data as defined under the law, including medical histories and biometric information. Processing such information requires enhanced safeguards and strict controls over internal access.

Data Localisation Requirements

Burundi does not currently impose general data localisation requirements. There is no legal obligation to store citizen data or payment information on servers physically located within the country. However, cross-border data transfers remain subject to regulatory oversight and authorisation under the law, creating a controlled transfer regime rather than unrestricted data mobility.

6.2 Technology Frontiers

The legal framework for emerging technologies is still developing. The 2026 Data Protection Law, the Law on Electronic and Postal Communications, and the Cybercrime Law serve as the primary pillars. Key features relevant to technology include the planned

establishment of an independent Data Protection Authority, mandatory impact assessments for high-risk technologies, and criminal penalties for misuse of personal data.

The 2026 law and current guidance do not yet grant individuals a clear right to object to decisions made solely by automated systems or artificial intelligence. Unlike some comparable frameworks — such as the GDPR, which explicitly addresses automated decision-making — Burundi's current regime applies only the general data protection principles to AI-driven processing. This is, however, an emerging area and may be addressed in future implementing regulations as the regulatory framework matures.

The 2024 Code des communications électroniques et postales introduces specific rules on digital surveillance. It defines the powers of state authorities for lawful interception and monitoring, while also requiring private actors to respect privacy and obtain authorisation for their own surveillance activities, including the use of CCTV. This represents a more concrete regulatory anchor for surveillance-related compliance compared to jurisdictions that rely solely on general data protection principles.

7. Outlook and Recommendations

7.1 Perceived Gaps and Pressures

Despite the establishment of a comprehensive legal framework, several practical challenges continue to shape the implementation of data protection law in Burundi.

- **Enforcement Uncertainty:** The most significant immediate challenge is the absence of an operational supervisory authority. Without the Agency in place, there is currently no body to interpret the law, issue guidance, or enforce compliance. This creates uncertainty for businesses trying to understand their obligations in practice.
- **Technical Depth:** The law establishes principles but leaves much of the operational detail to future implementing regulations. Until those regulations are published, organisations face compliance ambiguity on issues such as DPO requirements, DPIA processes, and transfer authorisation procedures.
- **Market Capacity:** Smaller businesses and public institutions frequently lack access to specialised expertise in data governance and regulatory compliance, creating uneven implementation across the economy.
- **External Pressures:** Rapid digitalisation, the expansion of mobile financial services, and increasing reliance on cross-border data flows are placing strain on existing compliance structures. Regional integration frameworks such as the AfCFTA are likely to intensify the need for harmonised data protection standards across African jurisdictions.
- **International Alignment:** Regulatory trends influenced by frameworks such as the GDPR are shaping expectations around accountability, transparency, and cross-border data governance. For Burundi, alignment with such standards is increasingly linked to participation in the global digital economy and prospects for EU adequacy recognition.

7.2 Future Trajectory

In the next 18 to 24 months, the primary focus is expected to be on building the foundational infrastructure of the new system. Once established, the Personal Data Protection Agency is expected to concentrate on:

- Building its own institutional capacity and staffing.
- Raising public awareness about the new law and individual rights.
- Auditing high-risk sectors — particularly finance and telecommunications — to prepare for active enforcement.
- Drafting secondary regulations to operationalise the 2026 law and provide practical guidance for businesses.

Most Impactful Reform by 2027

The single most impactful reform would be the operationalisation of the law through detailed, practical regulations and guidance. This would transform the framework from a foundational legal text into a usable, predictable compliance system. For businesses, clarity on obligations, processes, and enforcement priorities is essential to enable confident investment in digital services while maintaining a secure and legally compliant operating environment.

02 Kenya

1. The Legislative and Regulatory Landscape

1.1 Primary Legal Framework

The Kenya Data Protection Act 2019 (DPA) is the primary data protection law in Kenya. In the six years since its enactment, the framework has undergone several legislative updates and regulatory expansions that have progressively strengthened its reach and operational infrastructure.

In January 2026, the Office of the Data Protection Commissioner (ODPC) completed its public consultation on the draft Data Protection (Conduct of Compliance Audit) Regulations 2024. These proposed regulations provide a framework for conducting audits, reporting, and the accreditation of external auditors — a development that will materially expand the ODPC's supervisory toolkit.

The Finance Bill 2024 had proposed amendments that would have given the Kenya Revenue Authority (KRA) expanded access to personal data. Public opposition led to the withdrawal of this clause, demonstrating that civil society engagement remains an active check on legislative overreach in the data protection space.

The Data Privacy and Governance Society of Kenya (DPGSK) has developed the Draft Data Protection (Amendments) Bill 2025. The proposed amendments seek to expand the definition of sensitive data, enhance obligations for controllers and processors, establish a dedicated Data Protection Appeals Tribunal, and strengthen data subject rights. Additionally, the ODPC has published a suite of regulations and guidance notes — including the Enforcement and Penalty Regulations and the General Regulations of 2022 — that complement and operationalise the original 2019 Act.

CONTRIBUTOR

Ian Makambu Mong'are is a Data Privacy and Compliance professional with a dual background in law and financial services, currently serving as Head of Data Protection Services at Datavara Tech Solutions Limited. He specialises in data protection governance, DPIAs, DPO-as-a-Service, and AML/CFT risk frameworks across fintech, healthcare, and NGO sectors in East Africa. An LLB graduate of Kenyatta University and holder of a Postgraduate Diploma from the Kenya School of Law, Ian combines legal rigour with practical compliance expertise to help organisations navigate Kenya's evolving data protection landscape.

Constitutional Foundation

Article 31 of the Constitution of Kenya 2010 guarantees every person the right to privacy, including protection against unnecessary searches, disclosure of personal information, and interference with communications. This constitutional anchor provides a foundational basis for data protection claims before the courts.

Sectoral Laws and Their Interaction
Several sector-specific laws impose privacy and cybersecurity obligations that interact with the general data protection framework.

- **Telecommunications:** The Kenya Information and Communication Act (KICA) is among the earliest laws to address data privacy. The Consumer Protection Regulations 2010 specifically prohibit the interception of messages or disclosure of any such interception.
- **Health:** The Digital Health Act 2023 ensures the privacy, confidentiality, and security of health data and establishes a Digital Health Agency to oversee digital health services, secure health data transfers, and develop a national digital health information system. The HIV/AIDS Prevention and Control Act 2006, which predates the DPA, remains a pioneer sector-specific protection for sensitive health data.
- **Finance and Banking:** The Central Bank of Kenya has published the CBK Guidance Note on Cybersecurity (2017) and the Cybersecurity Guidelines for Payment Service Providers (2019), both oriented towards cybersecurity governance and risk management in alignment with the DPA's data security obligations.

1.2 The Supervisory Authority

The Office of the Data Protection Commissioner (ODPC) was established pursuant to the Data Protection Act 2019. The first Data Protection Commissioner was appointed on 16 November 2020, marking the transition from a legislative text to an active enforcement institution.

The ODPC is funded primarily through National Treasury appropriations by Parliament, supplemented by revenue from registration fees and statutory fines. It also collaborates with international partners including the European Union and Germany's GIZ to bridge resource gaps and strengthen institutional capacity.

While the ODPC is designed as an independent office, its status as a state office rather than a constitutional commission raises legitimate questions about the scope of its independence. Unlike constitutional commissions such as the Ethics and Anti-Corruption Commission (EACC), the ODPC cannot claim absolute freedom from direction or control. The Data Commissioner is a presidential appointee, and the office's close institutional ties with the Ministry of Information, Communication, and Technology have been cited as potential limitations on its independence. In practice, however, the Commission has discharged its mandate without visible political interference to date. Whether the ODPC will issue determinations against government agencies which are among the largest processors of personal data in Kenya remains an important test of its institutional resolve.

The ODPC's key mandated powers under section 9 of the Act include: investigating data protection issues on its own initiative or upon complaint; facilitating dispute resolution through conciliation, mediation, and negotiation; issuing summons to witnesses; requiring persons subject to the Act to provide information and assistance; imposing administrative fines; and undertaking any other activities necessary to fulfil its mandate.

2. Core Compliance Requirements & Definitions

2.1 Scope and Applicability

The DPA applies extraterritorially. Under section 4(b)(ii), it regulates the processing of personal data by any data controller or processor who is not established or ordinarily resident in Kenya but who processes the personal data of data subjects located in Kenya. For multinationals, this means Kenyan data protection obligations apply regardless of where the organisation is incorporated, provided its processing activities target or affect Kenyan residents.

The DPA applies extraterritorially. Under section 4(b)(ii), it regulates the processing of personal data by any data controller or processor who is not established or ordinarily resident in Kenya but who processes the personal data of data subjects located in Kenya. For multinationals, this means Kenyan data protection obligations apply regardless of where the organisation is incorporated, provided its processing activities target or affect Kenyan residents.

Lawful Bases for Processing

The Data Protection Act 2019 establishes that personal data may only be processed where a lawful basis exists, recognising six grounds: consent, contractual necessity, legal obligation, vital interests, public interest, and legitimate interests. Although these bases closely mirror those under the GDPR, their practical application in Kenya reveals a distinctive regulatory emphasis.

Consent has emerged as the most prominent lawful basis in practice. The Act imposes strict requirements that consent be freely given, specific, informed, and unambiguous, while also placing the burden of proof on the data controller and allowing withdrawal at any time. This prominence is reinforced by the requirement that personal data generally cannot be used for commercial purposes without express consent, which significantly affects digital platforms, fintech companies, and marketing-driven businesses. Enforcement patterns by the ODPC further demonstrate a consent-centred compliance culture, with numerous enforcement actions addressing unsolicited marketing and misuse of personal data without proper consent.

By contrast, the legitimate interests basis remains comparatively underdeveloped and is subject to a balancing test that allows data subjects to object unless the controller demonstrates overriding interests or legal necessity. Legal obligation and public interest are most frequently relied upon by government institutions and regulated sectors such as financial services, though courts and regulators have increasingly scrutinised such claims to ensure they do not undermine the constitutional right to privacy. Kenya's legal framework structurally aligns with international data protection standards, but its operational reality reflects a system in which consent dominates regulatory practice, legitimate interests are cautiously applied, and public interest processing continues to attract heightened oversight.

Sensitive Personal Data

The Data Protection Act 2019 establishes a notably expansive definition of sensitive personal data and subjects its processing to heightened regulatory safeguards. Sensitive data includes information revealing race, health status, ethnic origin, conscience, belief, genetic and biometric data, as well as property and family details — categories that extend beyond those recognised in the GDPR and reflect Kenya's socio-economic context. Proposed reforms under the Data Protection (Amendment) Bill 2025 aim to further expand this definition by including political opinions and trade union membership.

The Act imposes a stricter regulatory threshold for sensitive data processing by requiring explicit consent as an additional condition layered on top of an existing lawful basis, creating a higher compliance burden than comparable regimes. The ODPC has reinforced this framework through sector-specific guidance on biometric, health, and financial data, while the Worldcoin ruling confirmed that Data Protection Impact Assessments are mandatory preconditions for high-risk processing.

Beyond explicit consent, organisations handling sensitive data must comply with additional obligations including: mandatory DPIAs for high-risk activities; stricter cross-border transfer requirements; compulsory registration with the ODPC regardless of organisational size; potential data localisation requirements, including maintaining at least one copy of data in Kenya; and the appointment of a Data Protection Officer. Collectively, these layered safeguards illustrate Kenya's precautionary regulatory approach, signalling that the processing of sensitive personal data is treated not merely as a compliance issue but as an area requiring heightened accountability and institutional oversight.

2.2 Data Subject Rights

The DPA grants a comprehensive suite of data subject rights under section 26. These include the right to be informed, the right of access, the right to rectification and erasure, the right to restriction of processing, the right to data portability, the right to object to processing, and rights related to automated decision-making.

Practical Mechanisms for Exercising Rights

The Data Protection (General) Regulations 2021 prescribe standardised forms including Form DPG 3 and Form DPG 4 for requests relating to the rectification and erasure of personal data. These forms require detailed personal identification and specification of the requested remedy. The

information requirements are more extensive where requests are made on behalf of minors or incapacitated persons.

The ODPC has operationalised an online complaints desk and a help desk to improve accessibility for data subjects whose rights have been denied or ignored. Complaints are required to be resolved within 90 days of admission.

The ODPC has handled more than 9,000 complaints since its establishment. The predominant complaints have been lodged against digital credit providers, reflecting widespread concerns about data harvesting, contact list access, and debt collection harassment in the digital lending sector.

Limitations and Exemptions

The DPA recognises a range of exemptions to data subject rights. Section 51 provides broad carve-outs for purposes such as tax collection, national security, execution of judgments, law enforcement, and immigration control. Section 52 exempts processing for journalism, literature, and art where compliance would undermine those purposes, while requiring due regard to freedom of expression and the public interest. Section 53 provides a modified compliance regime for research, historical, and statistical purposes, prohibiting uses likely to cause harm. Together, these provisions seek to balance data protection rights against societal, state, and expression interests.

3. Governance, Accountability & Ongoing Compliance

3.1 Directors' Duties and Corporate Accountability

The DPA imposes direct legal obligations on data controllers and processors as entities, while also creating routes to personal liability for corporate officers. Under section 68, where an offence is committed by a body corporate and is proven to have been committed with the consent or connivance of, or attributable to the negligence of, a director, manager, secretary, or similar officer, that individual is also guilty of the offence and liable to the prescribed penalties.

In **Lee Mutunga v Milestone Games Limited T/A SportPesa (ODPC Complaint No. 1899 of 2024)**, the ODPC recommended the prosecution of SportPesa directors for obstructing investigations, a significant escalation of individual accountability that signals the direction of future enforcement. While this framework exists in statute, the mechanisms remain underutilised. As enforcement matures, greater board-level compliance engagement is expected.

Data Protection Officer (DPO) Mandate

DPO appointment is mandatory for: public bodies and government agencies; entities whose core activities involve regular and systematic monitoring of data subjects on a large scale; and entities that process sensitive personal data on a large scale. In practice, financial institutions, telecommunications companies, and healthcare providers are expected to appoint DPOs.

A significant number of organisations have not yet appointed DPOs, instead folding data protection responsibilities into existing compliance or legal functions an arrangement that can create conflicts of interest. The DPA does not prescribe specific academic qualifications for DPOs, but ODPC guidance emphasises the need for knowledge of data protection law, organisational policies, and information technology. In terms of reporting lines, practice varies, but reporting predominantly flows to the Board Risk Committee or Audit Committee.

Board Oversight Expectations

While the DPA does not prescribe specific board oversight duties, the accountability principle under section 25 requires controllers to demonstrate compliance. Read alongside the Companies Act 2015 and evolving corporate governance norms, this positions the board as responsible for ensuring that data protection compliance is embedded within enterprise risk management frameworks rather than treated as a purely operational matter.

3.2 Key Annual Compliance Cycle Requirements

Beyond initial registration, the DPA imposes ongoing compliance obligations across several dimensions:

- **Registration and Records:** Controllers and processors must notify the ODPC of any changes to registration details and renew certificates as required. They must maintain detailed records of all processing activities, including purposes, data categories, and security measures.

- **Privacy Notices:** Privacy notices must be kept current to reflect changes in how personal data is processed.
- **Staff Training:** Regular staff training on data protection is expected and will be examined during audits.
- **Vendor Management:** Controllers must vet third-party vendors and document data protection measures in processor agreements.
- **DPIA Reviews:** DPIAs should be reviewed periodically, particularly when processing activities or technology evolve.
- **Compliance Audits:** Once finalised, the 2024 Compliance Audit Regulations will subject controllers to mandatory audits by the ODPC or an accredited auditor.

Data Protection Impact Assessments (DPIAs)

Section 31 of the DPA requires a DPIA before undertaking high-risk processing activities, including large-scale processing of sensitive data, use of new technologies, profiling, CCTV surveillance, and cross-border transfers of sensitive data. The DPIA must be submitted to the ODPC at least 60 days before processing begins. Where residual high risk remains despite proposed mitigations, prior consultation with the ODPC is mandatory.

The Worldcoin case, decided by the High Court in May 2025, provides a stark illustration of the consequences of DPIA non-compliance. The court found that the collection of biometric data from over 350,000 Kenyans without a DPIA constituted a fundamental breach of the DPA, and ordered the permanent deletion of all unlawfully collected data within seven days under ODPC supervision.

Breach Notification Requirements

Controllers must notify the ODPC within 72 hours of becoming aware of a breach likely to affect data subjects' rights, with a reasoned explanation required for any delay. Processors must notify the relevant controller within 48 hours to allow the controller to meet its own reporting deadline. Where the breach poses a high risk to individuals, affected data subjects must also be notified without undue delay, with clear details on the breach, its likely consequences, and remedial steps taken.

Every breach notification must include: the nature of the breach; the categories and approximate number of affected individuals; the likely consequences; and the proposed mitigation measures. Controllers must also maintain internal records of all breaches, including those that fall below the formal notification threshold, as evidence of compliance.

For health data specifically, the Digital Health Act 2023 imposes a stricter regime: controllers must notify the Digital Health Agency within 48 hours and provide full details of corrective measures and resolution timelines within 72 hours. The overall breach framework operates in three sequential stages: processor to controller, controller to regulator, and controller to affected data subjects.

4. Enforcement and Practical Reality

4.1 Regulatory Activity

Kenya's ODPC has established one of the most active enforcement records on the African continent. As of May 2025, it had received 7,611 complaints, resolved 7,497, and issued 247 determinations, 112 enforcement notices, 19 penalty notices, 134 compensation orders, and 20 prosecution recommendations reflecting a steadily assertive enforcement posture.

Landmark Enforcement Decisions

- **Worldcoin (Republic v Tools for Humanity Corporation (US) & 9 others; Katiba Institute & 4 others (Ex parte Applicants) [2025]):** The High Court declared biometric data collection from over 350,000 Kenyans unlawful due to failure to conduct a DPIA, absence of informed consent, and improper registration. The court ordered permanent deletion of all collected data within seven days under ODPC supervision and cancelled Worldcoin's registration. This is the most consequential data protection ruling in Kenyan legal history.
- **SportPesa (Lee Mutunga v Milestone GamesLtd T/A Sportpesa [2025]):** The ODPC ordered KES 350,000 in compensation and recommended prosecution of the company's directors for obstructing the exercise of data erasure rights a notable escalation of individual accountability.
- **Regus Kenya (Regus Kenya Limited v Data Protection Commissioner & another [2025]):** In September 2025, the High Court upheld the

ODPC's penalty notice and affirmed its procedural powers and jurisdiction, providing important jurisprudence on the regulator's enforcement authority.

- **Whitepath Company and Regus Kenya:** Jointly fined the statutory maximum of KES 5 million for unlawfully accessing user data to send unsolicited messages.
- **Mulla Pride (Arnold Mwawura & Anor v Mulla Pride Limited [2023]):** Fined KES 2.975 million by the ODPC for using third-party personal data to send threatening messages — a practice common among digital lenders.
- **Oppo Kenya (December 2022):** The first organisation fined under the DPA; penalised KES 5 million for using a complainant's social media photo for marketing without consent.

Maximum Penalties and Enforcement Range

Administrative fines are capped at KES 5 million or 1% of annual turnover, whichever is lower, a notably modest ceiling compared to the GDPR's maximum of €20 million or 4% of global turnover. Criminal penalties, including fines and imprisonment, apply to serious offences such as unlawful processing of sensitive data, failure to register, and obstructing the ODPC. The KES 5 million maximum has already been applied in at least two cases — Oppo Kenya and Whitepath/Regus. The proposed 2025 Amendment Bill seeks to raise these thresholds materially, though the revised figures have not yet been publicly confirmed.

Advisory and Guidance Activity

The ODPC has published a broad range of guidance notes covering registration, DPIAs, consent, health data, digital credit providers, the public sector, and other industries. It has also produced an ADR Framework, a Personal Data Protection Handbook, and a Complaints Management Manual. In December 2024, it released two significant instruments for public consultation: the Data Protection (Conduct of Compliance Audit) Regulations 2024 and the Data Sharing Code.

Regionally, the ODPC actively participates in the Network for African Data Protection Authorities (NADPA) and has hosted its conference in Kenya. In 2025, the ODPC won Global Privacy Assembly awards for its dispute resolution and enforcement work, cementing its reputation as a leading data protection authority on the continent.

4.2 Private Litigation

Under section 63 of the DPA, any person who suffers damage from a data protection violation is entitled to compensation, covering both material harm such as financial loss and identity theft and non-material harm, including distress and reputational damage. Claims may be pursued before the courts, following an ODPC determination, or through the ADR process.

The 2025 Amendment Bill proposes expanding complaint-filing standing from data subjects to 'any person', including legal entities, potentially enabling NGOs, journalists, and businesses to file complaints on behalf of affected individuals. While class actions are not yet formally recognised under Kenyan law, civil society organisations such as the Katiba Institute have pursued public-interest litigation that operates as a quasi-class-action model a pattern demonstrated prominently in the Worldcoin proceedings and expected to continue as a key enforcement avenue.

Key Court Decisions

- **Worldcoin (May 2025):** The most consequential data protection case in Kenyan legal history. The High Court ordered permanent deletion of biometric data from over 350,000 Kenyans, cancelled Worldcoin's registration, and prohibited further collection without a valid DPIA and consent.
- **Thakrar v WPP PLC:** The High Court clarified that data privacy claims arising within employment disputes fall under the jurisdiction of the Employment and Labour Relations Court, not the Commercial Court an important jurisdictional delineation.
- **Gichuhi Case:** Provided early jurisprudence on the ODPC's procedural obligations, particularly around its 90-day complaint resolution timeline.
- Regus Kenya v Data Protection Commissioner (September 2025): The High Court upheld the ODPC's enforcement authority, affirming the Commissioner's procedural powers and penalty jurisdiction.
- **Erastus Ngura Odhiambo v Republic [2022] KEHC 702 (KLR)[March 2026):** The High Court confirmed that phone numbers are digital identifiers and therefore personal data, and that the reassignment of a phone number to a new user without notice to the previous owner, and

without technical safeguards to prevent the transfer of personal data associated with the number, constitutes a violation of the right to privacy.

Together, these cases are building a body of Kenyan data protection jurisprudence across constitutional, commercial, and employment law contexts.

5. Cross-Border Data Transfers

5.1 Transfer Mechanisms

Section 48 of the DPA and the 2021 General Regulations establish four mechanisms for transferring personal data outside Kenya:

- **Adequacy Decisions:** The ODPC may designate countries as providing sufficient protection, permitting free data flows to those jurisdictions. No formal whitelist has yet been published.
- **Appropriate Safeguards:** Controllers may rely on binding corporate rules, standard contractual clauses, or other legally binding instruments, all of which must be documented.
- **Necessity-Based Transfers:** Transfers without specific safeguards are permitted where required for contract performance, legal claims, vital interests, or compelling public interest.
- **Explicit Consent:** Consent may serve as a transfer basis but must meet the DPA's stringent standards and is generally unsuitable as a routine mechanism for large-scale commercial transfers.

Since no formal adequacy whitelist exists, controllers transferring data to EU-based entities typically rely on EU-style standard contractual clauses (SCCs) as an accepted safeguard, subject to documentation. In May 2024, Kenya and the EU launched the first adequacy dialogue on the African continent, a development that, if successful, would enable free data flows between the two jurisdictions without further safeguards. Data Commissioner Immaculate Kassait has highlighted that an adequacy decision would reduce compliance costs and facilitate digital trade. However, the EU adequacy process is lengthy, typically spanning several years, and past African attempts by Morocco and Mauritius were unsuccessful.

Data Localisation Requirements

The 2021 General Regulations impose data localisation requirements for data related to state strategic interests, including civil registration, elections, public finance, and primary healthcare, which must be processed on servers located in Kenya or with a local copy maintained. The Digital Health Act 2023 adds a potentially stricter localisation rule for health data, largely limiting cross-border transfers to health tourism circumstances, though the ODPC takes a broader view permitting transfers with consent or adequate safeguards. No general localisation obligation applies to commercial data outside these categories.

The December 2024 Cloud Policy further encourages localisation for sensitive government and critical infrastructure data, though it is a policy document rather than binding law. Together, these overlapping frameworks create a complex compliance landscape for multinationals managing cross-border data flows.

In practice, multinationals operating in Kenya manage transfers through SCCs, binding corporate rules, bilaterally negotiated transfer agreements, and hybrid approaches combining multiple mechanisms for cloud-based operations.

6. Sector-Specific & Emerging Challenges

6.1 Critical Sectors

- **Financial Services and Fintech:** Financial institutions and fintechs must register with the ODPC regardless of size and face additional cybersecurity and data handling obligations from the Central Bank of Kenya, the Capital Markets Authority, and the National Computer and Cybercrimes Coordination Committee (NC4), including 24-hour breach reporting under the 2024 critical infrastructure regulations. Digital credit providers have generated the highest volume of ODPC complaints, prompting a 2022 audit of 40 providers and sector-specific guidance in 2023, with common violations centring on unauthorised access to borrower contact lists for debt collection harassment.
- **Telecommunications:** Telecom operators are governed by both the DPA and sector-specific legislation under KICA and the Communications

Authority Act. The ODPC's Communications Sector Guidance Note covers subscriber, traffic, location, and financial data. Telecom operators are also designated as critical infrastructure, adding a further compliance layer.

- **Healthcare:** The Digital Health Act 2023 established the Digital Health Agency to oversee a national health information system, imposing a 48-hour breach notification requirement, a 20-year minimum data retention period, and mandatory security measures including encryption and access controls. Section 47 of the Act potentially restricts cross-border health data transfers to health tourism circumstances only — a provision whose precise legal scope remains contested but which, if strictly interpreted, would impose significant localisation requirements.

6.2 Technology Frontiers

Kenya has no AI-specific legislation as of March 2026, relying instead on the DPA, cybercrimes legislation, and consumer protection laws to govern AI-related data processing. The National AI Strategy 2025–2030 sets out a governance roadmap positioning Kenya as Africa's leading AI hub, and discussions of a dedicated AI law are underway, though no bill has been introduced.

The Worldcoin case has emerged as the most significant AI-adjacent precedent, establishing that biometric data collection requires a DPIA and valid consent, and that financial incentives such as cryptocurrency payments can invalidate consent. These principles carry broad implications for organisations deploying AI and biometric systems.

Kenya's digital surveillance framework is governed by the Computer Misuse and Cybercrimes Act 2018, KICA, and the DPA. NC4 holds powers for lawful interception, and the Communications Authority regulates subscriber data and telecommunications surveillance. CCTV operations by both private and public entities must comply with DPA principles, and a DPIA is required before deploying systematic monitoring of publicly accessible areas. There is no dedicated standalone CCTV regulation. The 2024 Cybercrimes Amendment expanded NC4's powers to restrict access to websites linked to illegal activity, raising free speech concerns, while the proposed 2025 Amendment Bill seeks to limit ODPC collaboration with national security organs though security agencies' own interception powers would remain intact.

7. Outlook and Recommendations

7.1 Perceived Gaps and Pressures

- **Penalty Cap:** The KES 5 million administrative fine cap remains a weak deterrent for large multinationals, effectively reducing compliance to a cost-benefit calculation rather than a binding obligation.
- **ODPC Capacity:** Resource constraints at the ODPC create backlogs in complaint resolution and audit activity, limiting the regulator's ability to maintain systematic oversight of a rapidly growing digital economy.
- **SME Compliance:** Compliance levels among small and medium-sized enterprises remain low due to limited awareness and capacity across Kenya's broader business landscape.
- **Cross-Border Complexity:** The absence of an adequacy whitelist and the overlapping localisation requirements under the DPA, the Digital Health Act, and critical infrastructure regulations create significant uncertainty for multinational operators.
- **Technology Gaps, among others:** The absence of AI-specific legislation leaves organisations without clear regulatory guidance on high-risk AI deployments. Concerns about ODPC independence from government influence and low public awareness of data protection rights compound the structural gaps that the 2025 Amendment Bill and ongoing reforms seek to address.

The May 2024 EU-Kenya adequacy dialogue is the most significant external driver of reform, creating strong commercial incentives for Kenya to align with GDPR standards on ODPC independence, penalty levels, and enforcement effectiveness. The AfCFTA digital trade protocols and the AU's Malabo Convention which Kenya has not yet ratified add regional pressure for a more robust and credible framework. Kenya's rapid digitalisation, with mobile penetration at 128.3% and the digital economy projected to contribute KES 662 billion to GDP by 2028, continuously outpaces the regulatory framework's capacity to manage emerging risks. The World Bank's USD 390 million Digital Economy Acceleration Project and

growing competition from Rwanda, Uganda, and Tanzania further underscore the urgency of sustained legal reform.

7.2 Future Trajectory

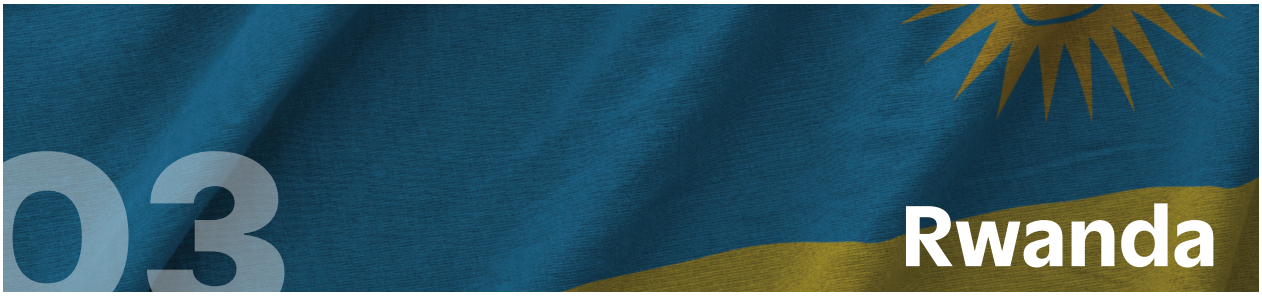
The Data Protection (Amendment) Bill 2025 is the most significant pending reform, proposing expanded sensitive data categories, stronger ODPC independence, mandatory accountability demonstrations, and formal codification of data portability and automated decision-making rights. It also proposes establishing a dedicated Data Protection Appeals Tribunal, expanding complaint-filing standing to any person including legal entities, and increasing financial penalty thresholds.

Several additional instruments are pending finalisation, including the Compliance Audit Regulations 2024, the Data Sharing Code 2024, the Kenya Robotics and AI Society Bill, and a Draft Critical Infrastructure Protection Bill. Together, these reforms represent a comprehensive legislative modernisation effort aimed at aligning Kenya's framework more closely with GDPR standards.

The ODPC's near-term priorities centre on finalising and implementing the Compliance Audit Regulations to enable systematic, risk-based auditing across high-risk sectors including digital lending, health, and telecommunications. Continued enforcement against digital credit providers, supervision of the Worldcoin data deletion, and advancing the EU adequacy dialogue are also key priorities. The ODPC is expected to issue guidance on AI and automated decision-making as the National AI Strategy 2025–2030 enters its implementation phase, alongside finalisation of the Data Sharing Code. Public awareness campaigns and expansion of county-level offices aim to improve accessibility for data subjects outside Nairobi.

Most Impactful Reform by 2027

The single most impactful reform would be enactment of the 2025 Amendment Bill with a materially higher penalty cap raising the maximum fine from KES 5 million to at least 2% of annual Kenyan turnover, and 4% for the most serious violations. Higher penalties would provide genuine deterrence for large multinationals, strengthen ODPC credibility in the EU adequacy dialogue, and operationalise board-level accountability through the codified accountability principle. The establishment of a Data Protection Appeals Tribunal would further provide an efficient and dedicated appellate mechanism, reducing reliance on overburdened general courts. Without penalty reform, all other improvements risk being undermined by an enforcement regime that large organisations can simply absorb as a routine cost of doing business.



03 Rwanda

1. The Legislative and Regulatory Landscape

1.1 Primary Legal Framework

Rwanda's primary data protection instrument is Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy (the DPP Law). The law was gazetted and came into force on 15 October 2021. No major amendments have been made to the DPP Law itself since its enactment. Supplementary implementation guidelines have been issued by the National Cyber Security Authority (NCSA), but these are administrative instruments and do not have the force of law.

From a business perspective, the DPP Law represents a comprehensive and relatively modern framework, closely modelled on the EU General Data Protection Regulation (GDPR). Organisations operating in Rwanda must treat personal data governance as a structured compliance discipline, with formal obligations around registration, DPO appointment, impact assessments, and breach notification.

Constitutional Foundation

Article 23 of the Constitution of Rwanda provides the foundational privacy protections underpinning the DPP Law. It guarantees privacy of person and family life from unlawful interference; inviolability of the home against unauthorised search or entry; confidentiality of correspondence and communications; and protection of a person's honour and dignity in all matters relating to private life. The DPP Law explicitly cites Article 23 as its primary constitutional authority, grounding data protection obligations in these fundamental rights.

Sectoral Laws and Their Interaction

Several sectoral laws impose parallel privacy and cybersecurity obligations that operate alongside and interact with the DPP Law:

- **ICT and Telecommunications:** Law No. 24/2016 of 18 June 2016 Governing Information and Communication Technologies (the ICT Law) regulates electronic communications, telecom operators, and network security. It establishes mandatory lawful interception obligations, sector-specific data localisation requirements, and liability rules for digital services. The ICT Law and the DPP Law must be read together by organisations in this sector.
- **Cybersecurity Framework:** The NCSA administers a cross-sector cybersecurity framework that includes regulations, directives, incident response obligations, and security standards applicable to data controllers and processors across industries.

CONTRIBUTOR

David Bahige is an Associate at Trust Law Chambers, Kigali, specializing in Rwanda's Data Protection Law and regional privacy compliance. With over six years' experience advising regulators and multinationals, David provides strategic, practical insights into data localization, cross-border transfers, and AI regulation. Qualified in both Rwanda and Uganda, he offers a unique dual-jurisdictional perspective on East Africa's digital trade landscape. A co-author for Chambers Global on TMT, David is dedicated to operationalizing trust, ensuring data protection serves as a "badge of quality" and driver for innovation in Africa's digital economy.

- **Financial Services:** The National Bank of Rwanda (BNR) issues sector-specific data protection and cybersecurity requirements for financial institutions under Law No. 44/2024 Governing Banks and Law No. 61/2021 Governing the Payment System. The BNR also holds authority over payment systems and fintech actors under Law No. 48/2017 Governing the National Bank of Rwanda.
- **Healthcare:** The health sector is governed by Ministry of Health frameworks and the Patients' Rights and Responsibilities Charter (2018), imposes confidentiality and informed consent requirements for the processing of medical data.

1.2 The Supervisory Authority

The Data Protection Office (DPO) under the National Cyber Security Authority (NCSA) is the designated supervisory authority for data protection in Rwanda. The NCSA was established by Law No. 26/2017 of 31 May 2017. The Data Protection function within the NCSA became operational in 2020.

The NCSA is funded through state budget allocations, income from its activities, government-approved loans, and donations, grants, and bequests. It has administrative and financial autonomy. However, in practice, the NCSA operates under the supervision of the Office of the President, which means its independence is generally considered limited to moderate rather than fully independent. This institutional placement, common among first-generation data protection authorities in the region is a structural consideration for businesses assessing regulatory risk.

The NCSA's key mandated powers encompass four broad categories. Investigative powers include investigating complaints, conducting technical inspections of operators, accessing personal data records to verify lawful processing, requiring production and copying of documents, and entering premises to search and seize equipment linked to violations. Corrective and enforcement powers include imposing administrative fines ranging from RWF 2,000,000 to RWF 5,000,000 or 1% of global turnover for organisations, suspending or revoking licences and registrations, and ordering cessation of unlawful activities. Authorisational powers cover issuing and renewing registration certificates, granting ICT-related licences, and authorising, restricting, or prohibiting international data transfers. Advisory and regulatory powers include providing opinions on data protection matters, setting standards and sector-specific rules, and establishing standard contractual forms and codes of conduct.

2. Core Compliance Requirements & Definitions

2.1 Scope and Applicability

The DPP Law applies extraterritorially. Under Article 2, the law extends to any data controller, data processor, or third party who is neither established nor resident in Rwanda, provided they are processing the personal data of data subjects located in Rwanda. For multinationals, this means Rwandan data protection obligations apply regardless of where the organisation is incorporated or based, provided its processing activities target or affect individuals in Rwanda.

Lawful Bases for Processing

Under Article 46 of the DPP Law, a data controller or processor may lawfully process personal data on any of the following eight grounds:

- Consent — the data subject has given freely given, specific, informed, and unambiguous consent for one or more specified purposes.
- Contractual Necessity — processing is required for the performance of a contract to which the data subject is a party, or to take steps at their request prior to entering a contract.
- Legal Obligation — processing is required for the controller to comply with a legal obligation.
- Vital Interests — processing is necessary to protect the life or death interests of the data subject or another person.
- Public Interest or Official Authority — processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Duties of a Public Entity — processing is carried out for the performance of the duties of a public entity.
- Legitimate Interests — processing is for legitimate interests pursued by the controller or a third party, provided these are not overridden by the rights, freedoms, or interests of the data subject.

- Research Purposes — processing is conducted for research purposes upon authorisation by the relevant institution.

While consent is a primary gateway for processing in consumer-facing contexts, it is not the dominant or exclusive basis. In practice, public bodies, regulated financial institutions, and healthcare providers frequently rely on legal obligation, public interest, and contractual necessity grounds. The availability of multiple lawful bases reflects the law's GDPR-aligned design.

Sensitive Personal Data

The DPP Law imposes heightened restrictions on sensitive categories of personal data. Under Article 10, sensitive data may only be processed on specific grounds including: explicit consent of the data subject; compliance with legal obligations or exercise of specific rights; vital interests where the subject cannot consent; public health purposes such as preventing serious cross-border health threats; and archiving, scientific, historical, or statistical research in the public interest.

When processing sensitive personal data is permitted, Articles 11 and 38 require the controller or processor to implement mandatory additional safeguards. These include: appointing a Data Protection Officer; applying technical measures such as encryption and pseudonymisation to protect the data; conducting a Data Protection Impact Assessment before processing commences; ensuring access is restricted to personnel bound by confidentiality obligations; maintaining records of all processing activities involving sensitive data; implementing procedures to detect, respond to, and notify any data breaches involving sensitive data within the prescribed timelines; storing sensitive data separately from general personal data; and ensuring ongoing staff capacity building so that those handling sensitive data are continuously trained on applicable obligations and safeguards.

2.2 Data Subject Rights

Law No. 58 of 2021 provides a comprehensive suite of data subject rights aligned with international standards:

- Right of Access — obtain a copy of personal data held and information on processing purposes, recipients, sources, and any transfers.
- Right to Rectification — correct inaccurate or incomplete data. The controller must respond within 30 days.
- Right to Erasure — request deletion where data is no longer needed for its original purpose, consent is withdrawn, processing is unlawful, or a valid objection is upheld.
- Right to Portability — receive personal data in a structured, machine-readable format and request transfer to another controller where technically feasible.
- Right to Object — object to processing that causes harm to the data subject. The right is absolute for direct marketing and related profiling.
- Right to Withdraw Consent — consent may be withdrawn at any time, and must be as easy to withdraw as it was to give.

Practical Mechanisms for Exercising Rights

For rights such as access, rectification, erasure, portability, and objection, the individual must submit a request in writing or electronically directly to the data controller or processor. Data subjects may be represented by parents, guardians, or authorised persons with written authorisation. If dissatisfied with the controller's response, the data subject may appeal to the NCSA within 30 days of receiving that response. If unsatisfied with the NCSA's determination, the individual has a statutory right to file a case with a competent court.

As of early 2026, the NCSA has not yet published data on complaint volumes or request trends. Since the end of the two-year transitional grace period in October 2023, the Authority has been in the process of preparing compliance and enforcement reports, none of which have been finalised at this stage. The absence of published data is itself instructive: it reflects that Rwanda's regime is actively transitioning from initial compliance registration towards systematic enforcement, and that observable trends are expected to emerge as the NCSA's reporting infrastructure matures.

Limitations and Exemptions

Data subject rights under the DPP Law are not absolute and may be limited in defined circumstances. Recognised grounds for restriction include: national security and law enforcement, data may be retained longer or accessed by authorities

for investigations; public interest, research, and public health, rights may be limited where processing serves public tasks or essential health purposes; legal claims and judicial proceedings, processing may continue where necessary to establish, exercise, or defend legal claims; freedom of expression and journalism, balanced against privacy, dignity, public order, and morality; and protection of others, rights may be restricted where exercising them would prejudice third-party rights, confidential references, exam materials, or ongoing negotiations.

3. Governance, Accountability & Ongoing Compliance

3.1 Directors' Duties and Corporate Accountability

The DPP Law creates a multi-layered accountability framework. Under the ICT Law, any entity offering goods or services through electronic transactions must disclose the names of its office bearers and registration number to consumers on its website. Data controllers or processors not established in Rwanda who process the data of Rwandan residents must designate a written representative in Rwanda to ensure compliance with the law. Organisations processing sensitive data on a large scale or performing systematic monitoring must designate a DPO whose contact details must be published and notified to the NCSA.

On liability, the law draws a clear line between corporate and personal exposure. Article 62 of the DPP Law establishes that a corporate body convicted of data protection offences such as unlawful sale or processing of sensitive data is liable to a fine of 5% of its annual turnover from the preceding financial year. Personal criminal liability flows from the constitutional principle that criminal liability is personal: since the criminal offences in Articles 56 to 61 of the DPP Law apply to any 'person' who commits the prohibited acts, a director or senior officer who personally carries out or directs such conduct may be held individually liable. Upon conviction, a natural person may face imprisonment ranging from one to ten years and significant fines depending on the severity of the offence.

Data Protection Officer (DPO) Mandate

Under Article 40 of the DPP Law, appointment of a DPO is mandatory for: any public or private corporate body or legal entity carrying out processing (with the exception of courts); organisations whose core activities involve regular and systematic monitoring of data subjects on a large scale; and organisations whose core activities involve large-scale processing of sensitive personal data.

A DPO must possess general professional competence, specialised knowledge of data protection laws and practices, and the practical capability to perform their statutory duties. In practice, the DPO acts as both an internal compliance monitor and an external liaison with the NCSA. Key duties include advising on data protection obligations and DPIAs, monitoring compliance programmes, conducting internal audits of data processing operations, and serving as the NCSA's contact point including for prior consultation on high-risk processing.

Board Oversight Expectations

Boards of Directors are expected to exercise active, structured oversight of data protection compliance. This encompasses: ensuring appointment of a DPO where required and, in certain sectors, designating technical leadership responsible for network security; overseeing regular audits, penetration testing, and vulnerability assessments with timely remediation; ensuring DPIAs are conducted and appropriate safeguards implemented; establishing systems for breach notification, regulatory reporting, and complaint handling; and maintaining awareness that directors may face personal criminal liability for unlawful acts involving personal data. The growing enforcement posture of the NCSA makes board-level engagement increasingly important.

3.1 Key Annual Compliance Cycle Requirements

Beyond initial registration, organisations face a structured set of ongoing compliance obligations under the DPP Law and the ICT Law.

Registration and Licence Renewal

- **Data Protection Certificate:** Controllers and processors must apply for renewal of their registration certificate within 45 working days before expiry.
- **ICT/Telecom Licences:** Licensed operators in the ICT sector must pay periodic licence fees

and apply for renewal at least three months before their existing licence expires. Electronic numbering resources and addresses attract annual subscription fees.

Annual Audits and Security Assessments

- **Annual Vulnerability Testing:** All licensed telecommunications operators must perform vulnerability assessment and penetration testing at least once a year across all "planes" of their network.
- **Biannual Internal Audits:** Telecom sector licensees must conduct technical and process audits at least twice a year, submitting results to the Regulatory Authority (RURA) within 30 calendar days of completion.
- **Regulatory Authority Audits:** RURA conducts its own compliance audit for every licensee at least once a year.
- **Security Verification:** All data controllers and processors must regularly verify the effectiveness of their personal data security safeguards.

Data Protection Impact Assessments (DPIAs)

Under Article 38, a DPIA is mandatory before processing that is likely to result in high risk to the rights and freedoms of individuals. The DPP Law specifies five scenarios where a DPIA is always required: automated processing and profiling where decisions produce significant effects on individuals; large-scale processing of sensitive personal data (health, genetic, biometric); systematic monitoring of publicly accessible areas on a large scale (such as extensive CCTV networks); any processing activity specifically identified by the NCSA as high-risk; and when applying for authorisation to store or transfer data outside Rwanda.

The designated DPO must advise on and monitor the DPIA. Prior consultation with the NCSA is required where residual high risk cannot be adequately mitigated. DPIAs and processing activity records must be maintained and submitted to the NCSA upon request. Telecom operators must submit their audit reports to RURA within 30 days of completion.

Breach Notification Requirements

Rwanda's breach notification framework operates in two sequential stages with specific timelines. The data controller must provide an initial notification to the NCSA within 48 hours of becoming aware of a breach, followed by a full detailed report within 72 hours of discovery. If a data processor discovers a breach, it must notify the relevant controller within 48 hours. Where the breach is likely to result in high risk to the rights and freedoms of individuals, the controller must also notify affected data subjects promptly after becoming aware of the breach.

The 72-hour report to the NCSA must describe the nature of the breach, include the DPO's contact details, set out the measures taken or proposed, and describe the consequences of the breach. Where subject notification is required or approved by the NCSA, the controller must communicate the breach directly to individuals in writing or electronically.

4. Enforcement and Practical Reality

4.1 Regulatory Activity

Rwanda's data protection enforcement regime is still in its early stages. No major enforcement actions — formal investigations, fines, or publicly documented sanctions have been disclosed by the Data Protection Office under the NCSA in the last 12 to 24 months. This reflects the relative newness of the regime: the DPP Law provided a two-year transitional period for organisations already in operation at the time of its enactment to achieve compliance, with the registration deadline falling in October 2023. The NCSA has since been transitioning from a registration-based compliance focus toward active inspections and enforcement.

The legal framework provides for significant administrative fines, criminal penalties, and licence-based sanctions, but publicly documented enforcement cases remain limited at this stage. For businesses, this should not be interpreted as regulatory passivity, the NCSA has signalled that active sector audits are a near-term priority, and the penalty regime is substantial.

Penalty Framework

Administrative fines under the DPP Law are set at RWF 2,000,000 to RWF 5,000,000 for individuals, and 1% of global turnover for corporate bodies. The ICT Law carries higher administrative sanctions: licence transfer violations attract fines up to RWF 50,000,000, and daily non-compliance penalties can

reach RWF 15,000,000 per day. Telecom security regulation violations attract fines between RWF 1,000,000 and RWF 5,000,000.

Criminal penalties are severe. Unlawful collection or processing of sensitive personal data carries seven to ten years' imprisonment and a fine of RWF 20,000,000 to RWF 25,000,000. Unlawful sale of personal data carries five to seven years' imprisonment and a fine of RWF 12,000,000 to RWF 15,000,000. Malicious destruction or alteration of data attracts three to five years' imprisonment. General unlawful access or sharing carries one to three years. A corporate body convicted of criminal offences is liable to a fine of 5% of its annual turnover from the preceding financial year.

Guidance and Advisory Activity

The NCSA has demonstrated a high level of activity in producing compliance tools and guidance. It has published registration guides, self-assessment tools, data inventory templates, DPIA guides, DPO designation guidance, complaint procedures, contractual clauses, and application forms for cross-border data transfer authorisations. The law permits the NCSA to develop formal codes of conduct for specific sectors and certification schemes to signal compliance. In practice, these mechanisms are still being developed and no official certification programme equivalent to GDPR-style certification has yet been launched. The NCSA does issue formal certificates of registration to data controllers and processors.

4.2 Private Litigation

Article 65 of the DPP Law explicitly establishes a statutory right for individuals to claim compensation in a competent court where they have suffered serious damage resulting from acts of a data controller or processor that violate the law. A data controller or processor can only avoid liability if they can demonstrate they were not responsible for the damage. This is a reverse burden that places the onus on the defendant.

Individuals may access the court system through two primary routes: a direct civil claim for damages resulting from a breach; or an appeal against a regulatory decision by the NCSA, where the court exercises review jurisdiction. The DPP Law uses the broader term 'serious damage' rather than explicitly categorising damages as material or non-material, though both categories would ordinarily fall within the concept of compensable harm under Rwandan civil law.

As of early 2026, no class-action lawsuits have been brought on data privacy grounds in Rwanda. The most significant data-related incident in recent months is the 2026 Equity Bank Rwanda cyber-fraud investigation, involving an alleged loss of RWF 4.7 billion and multiple arrests. While primarily a financial crime investigation, it raises significant data protection and cybersecurity questions that may shape future compliance expectations in the financial sector. The NCSA has prioritised health sector compliance, conducting nationwide enforcement and awareness efforts. Civil society organisations including Digital Rights Rwanda and the Internet Society Rwanda Chapter are actively promoting public awareness and legal support for individuals seeking data protection remedies.

5. Cross-Border Data Transfers

5.1 Transfer Mechanisms

Rwanda takes a 'local-first' approach to data governance. The DPP Law mandates as a default position that data controllers and processors must store personal data within Rwanda. Storing data outside the country is only permitted where the entity holds a valid registration certificate specifically authorising foreign storage, issued by the NCSA. This is a more prescriptive localisation requirement than exists in most comparable East African jurisdictions.

Under Article 48, a controller or processor may transfer personal data to a third party outside Rwanda under the following mechanisms: prior authorisation from the NCSA with proof of appropriate safeguards; informed consent of the data subject; contractual necessity — where the transfer is required to perform or prepare a contract between the subject and the controller, or a contract in the subject's interest with a third party; public interest and legal claims; vital interests of the data subject when they cannot consent; and compelling legitimate interests for non-repetitive, limited-subject transfers where circumstances have been assessed and suitable safeguards provided.

For all transfers to parties outside Rwanda, the law mandates a written contract with the foreign recipient setting out roles and responsibilities. The NCSA has published standard contractual clauses (SCCs) functional equivalents of EU SCCs in its guidelines, which should be incorporated into data processing agreements and international transfer addendums. While EU SCCs are not expressly named in the law, the NCSA guidance effectively adopts their structure.

Adequacy Decisions and Recognised Mechanisms
No formal whitelist of countries providing adequate data protection has been issued by the NCSA. Transfers are assessed case-by-case, typically requiring NCSA authorisation. This creates an operational burden for businesses with regular international data flows, and is identified by the contributor as the most significant practical constraint on cross-border business operations. The NCSA's SCC guidelines provide the clearest pathway for non-adequacy transfers.

Sector-Specific Localisation — Telecommunications
The telecommunications sector is subject to a stricter and absolute localisation mandate under Article 16(e) of the Regulations Governing Telecom Network Security (2016). Subscriber information — encompassing voice, SMS, data, and billing records — must not be transferred, stored, or processed outside the Republic of Rwanda. Unlike the general DPP Law framework, which permits offshore storage subject to NCSA authorisation, this prohibition admits no exception: telecom subscriber data must remain within Rwandan territory regardless of any authorisation held. This creates a materially more restrictive regime for telecom operators than applies to other sectors, and is a critical compliance consideration for operators and any third-party processors they engage.

Practice for Multinational Organisations
In practice, multinationals operating in Rwanda manage compliance through a combination of: NCSA registration as controllers or processors with specific approval for any data stored or transferred outside Rwanda; SCC-type contractual clauses in intra-group agreements; DPIAs for high-risk or large-scale processing involving sensitive data; local retention of sensitive data with authorised, limited transfers to regional hubs; and appointment of a local representative for foreign entities processing Rwandan data. Rwanda's alignment with EAC harmonisation efforts on data governance is expected to progressively simplify intra-regional data flows over time.

6. Sector-Specific & Emerging Challenges

6.1 Critical Sectors

While the DPP Law applies universally, three sectors operate under layered and notably stricter regimes.

- **Telecommunications (strictest regime):** Subscriber data must remain in Rwanda. Networks must be technically equipped to enable state interception. The Chief Technology Officer or Chief Information Officer of a licensed telecom must be Rwandan. Technical security protections must cover management, signalling, and data planes. Internal audits must be conducted biannually and a regulator audit conducted annually.
- **Healthcare:** Medical data is treated as highly sensitive and subject to enhanced security requirements. Clinical confidentiality measures must be in place. Informed consent requirements are stronger for both treatment and research involving patient data. The NCSA has identified health as a priority compliance sector.
- **Financial Services (Fintech):** Financial institutions and payment service providers are regulated by the National Bank of Rwanda, which imposes additional data protection requirements beyond the DPP Law. Consumer data rights are modified in the digital transaction context, for example, limits apply to cancellation rights in electronic transactions. The Equity Bank Rwanda cyber-fraud investigation signals that financial sector data security is under heightened scrutiny.

Data Localisation Requirements
Rwanda has one of the most prescriptive data localisation regimes in the region. The DPP Law's default rule requires all personal data relating to individuals in Rwanda to be stored within the country, regardless of whether the processing entity is established locally or abroad. Offshore storage

requires a specific authorisation in the registration certificate. The telecommunications sector is subject to an absolute localisation requirement for subscriber data. This 'local-first' posture is a defining feature of Rwanda's data protection framework and a material compliance consideration for cloud-based and multinational operations.

6.2 Technology Frontiers

Rwanda's DPP Law and ICT Law together provide a reasonably future-oriented framework for emerging technologies, though dedicated AI legislation has not yet been enacted.

- **Artificial Intelligence and Automated Decision-Making:** The DPP Law grants individuals the right not to be subject to decisions based solely on automated processing including profiling that produce legal or similarly significant effects, unless justified by consent, contract, or law. Controllers must disclose the logic and consequences of automated processing. DPIAs are mandatory for systematic, large-scale profiling. These provisions directly govern AI-driven decision-making in credit scoring, fraud detection, and similar applications.
- **Biometric Systems:** Biometric data is classified as sensitive personal data subject to the strictest safeguards, including encryption, pseudonymisation or tokenisation, secure storage, mandatory DPIAs for large-scale deployments, and licensing requirements for authentication services under the ICT Law.
- **Digital Identity and Electronic Transactions:** Electronic records and signatures have full legal validity under the ICT Law. Electronic signatures are admissible if they identify the signer and indicate consent. Certification providers must be licensed and comply with strict security standards. Foreign electronic certificates are accepted where equivalently reliable.
- **Regulatory Flexibility:** The ICT Law adopts a technology-neutral approach, applying rules without bias across technologies. The ICT Minister holds authority to issue regulations for emerging issues, and regulators are expected to adapt their standards as technology evolves.

Rwanda is actively developing AI governance frameworks including the AI Playbook for Small States positioning itself as a trusted AI partner regionally. The NCSA is expected to issue guidance on AI-adjacent data protection obligations as the National Cybersecurity Strategy 2024-2029 is implemented.

On surveillance, the ICT Law (Articles 123 and 124) mandates that all electronic communications network and service providers equip their systems with technical instruments facilitating lawful interception by authorised state entities. The Minister responsible for ICT may interrupt private communications deemed detrimental to national sovereignty, public order, or good morals. CCTV and large-scale public area monitoring are classified as high-risk processing under the DPP Law, requiring a mandatory DPIA, transparency notices to the public about the purpose and data retention period, and compliance with the principles of necessity and proportionality. Private actors engaging in digital surveillance without lawful basis face criminal liability.

7. Outlook and Recommendations

7.1 Perceived Gaps and Pressures

Despite having one of the most comprehensive data protection frameworks in the region, Rwanda's regime presents several practical challenges from a business perspective.

- **Limited Enforcement Track Record:** The absence of publicly documented fines, decisions, and enforcement precedents creates uncertainty about how rules are interpreted and applied in practice. Businesses cannot calibrate their compliance programmes against actual regulatory decisions.
- **Regulatory Guidance Gaps:** Many compliance areas including cross-border transfers, DPIA methodology, and sector-specific obligations rely on guidelines rather than detailed regulations, creating uncertainty particularly for first-time entrants to the Rwandan market.
- **Data Localisation Burden:** The default requirement to store all personal data within Rwanda, combined with the case-by-case transfer authorisation process, creates significant operational and cost burdens, particularly for multinational companies, cloud-based service providers, and fintechs whose business models depend on cross-border data flows.

- **Approval-Based Transfer Regime:** The absence of an adequacy whitelist means every international transfer requires individual NCSA authorisation, leading to delays and unpredictability in time-sensitive operational contexts such as emergency processing or short-term data access arrangements.
- **Institutional Maturity:** The NCSA's Data Protection Office has been operational since 2020 but remains relatively young. Enforcement capacity, sectoral expertise, and complaint-processing resources are still developing.
- **Compliance Cost and Complexity:** The cumulative obligations of registration, DPO appointment, DPIAs, breach notification, localisation requirements, and annual renewals create a high compliance burden, particularly for startups and smaller enterprises with limited compliance infrastructure.

External pressures driving reform include: the EU adequacy dialogue — Rwanda's DPP Law was deliberately aligned with the GDPR to position the country for an EU adequacy decision, which would materially reduce compliance costs and facilitate digital trade with European partners; the AfCFTA Digital Protocol — Rwanda is modernising its regulatory framework to align with continental digital trade obligations, adoption of the AU Data Policy Framework, and the Electronic Transactions and Digital Signatures frameworks; and rapid domestic digitalisation — the $200 million World Bank Digital Acceleration Project (2022-2026) and Rwanda's ambitions in AI governance and digital services are intensifying regulatory pressure to ensure the framework keeps pace with technological adoption.

7.1 Future Trajectory

Several legislative and regulatory developments are expected to reshape Rwanda's data protection and digital governance landscape before the end of 2026. In the financial and digital sector: a Virtual Assets Regulation approved by Cabinet introduces a licensing, supervision, and AML compliance framework for cryptocurrencies and digital assets; strengthened Foreign Exchange Regulations (2025/2026) include enhanced compliance requirements and whistleblower protections; and the Financial Sector Development Strategy 2025-2030 sets a policy framework for digital financial services and non-bank payment system oversight. In health: the ART Regulation (2025) establishes a legal framework for assisted reproductive technologies with updated healthcare provider liability rules; and NGOs must achieve full compliance with new registration requirements by July 2026.

The NCSA's near-term priorities, based on its 2024-2029 National Cybersecurity Strategy and public statements, include: transitioning to active sector audits following the October 2023 registration deadline, with priority focus on health, finance, telecommunications, and education; finalising sector-specific data protection guidelines and detailed rules on registration and compliance obligations; developing mechanisms to govern international data transfers, including adequacy considerations for cloud storage outside Rwanda; and encouraging organisations to reinforce contractual safeguards with third-party processors.

Most Impactful Reform by 2027

The single reform most likely to improve the effectiveness of data protection and the ease of doing business in Rwanda by 2027 is the formal adoption of a clear, published cross-border data transfer adequacy framework. The current requirement for case-by-case NCSA authorisation for every transfer or storage of data outside Rwanda is an operational burden and a competitive disadvantage relative to jurisdictions with streamlined transfer mechanisms. It is particularly acute for businesses that require short-term or emergency cross-border access to data.

A codified adequacy framework would provide predictability on which jurisdictions are deemed to offer sufficient protection, reduce administrative burden by limiting the need for repeated individual approvals, standardise the use of contractual safeguards including NCSA-issued SCCs with clear regulatory recognition, and signal Rwanda's credibility as a GDPR-aligned jurisdiction in the context of the EU adequacy dialogue. Taken together, this reform would reduce compliance costs, support digital trade, and position Rwanda more firmly as the regional benchmark for data protection governance.

04 Tanzania

1. The Legislative and Regulatory Landscape

1.1 Primary Legal Framework

Tanzania's data protection regime is anchored in **the Personal Data Protection Act (PDPA) of 2022**, which came into force on 1st May 2023. The law establishes a comprehensive compliance framework governing the collection, use, storage, and disclosure of personal data across both public and private sectors.

From a business perspective, the PDPA marks a structural shift from informal data handling practices to regulated data governance. Organisations are now required to treat personal data not merely as an operational asset, but as a regulated risk category requiring internal controls, documentation, and oversight.

The **Constitution of the United Republic of Tanzania** recognises the right to privacy under **Article 16**. The PDPA operationalises this right by translating it into enforceable corporate obligations. Privacy therefore functions both as a constitutional guarantee and as a compliance burden with direct financial and reputational consequences.

Sectoral Laws and Their Interaction

In addition to the PDPA, sector-specific laws in financial services, telecommunications, and healthcare impose parallel confidentiality and cybersecurity obligations. In practice, this creates a layered compliance environment where organisations must reconcile overlapping regulatory requirements. For regulated industries, compliance failures may therefore arise not from absence of policy, but from misalignment between sectoral obligations and general data protection principles.

CONTRIBUTOR

Abdul Said Naumanga is an Advocate of the High Court of Tanzania, a Partner and Head of Personal Data Protection at Robik Attorneys & Legal Consultants, specialising in Data Protection, Privacy Law, and complex civil litigation. He advises individuals and organisations on compliance with the Personal Data Protection Act and related regulatory frameworks governing the collection, processing, and transfer of personal data. Naumanga has been directly involved in regulatory proceedings before the Personal Data Protection Commission and engages in privacy governance discussions in Tanzania. He is a member of the Tanzania Personal Privacy Association (TPPA).

1.2 Primary Legal Framework

Tanzania's data protection framework is administered by the Personal Data Protection Commission (PDPC), established under section 6 of the Act and operationalised in April 2024. The establishment of the Commission marked the transition from a legislative framework to an active enforcement regime.

From a governance standpoint, the PDPC is structured as an independent corporate body with legal capacity to enforce compliance, impose sanctions, and award remedies. Its institutional design — combining a policy-level Board and an operational Director General — reflects a hybrid model of regulatory oversight and administrative enforcement.

The Commission's statutory mandate extends beyond registration and compliance monitoring to include investigation, enforcement action, and public awareness. Crucially, its powers to issue enforcement notices, impose administrative fines, and award compensation position it as a financially consequential regulator rather than a purely advisory body.

In practical terms, organisations must treat engagement with the PDPC in the same manner as engagement with other high-impact regulators. Regulatory interaction is no longer optional or reactive; it requires structured compliance systems, documented decision-making, and readiness for audit or investigation.

While the PDPC is established as an independent statutory body, its operational independence is still evolving in practice. The Commission is institutionally linked to the executive through appointment processes and reporting structures — a pattern common in emerging regulatory frameworks across the region. However, early enforcement decisions indicate a willingness to exercise regulatory powers without overt political influence. Among practitioners, the prevailing view is that while formal independence exists in law, practical independence will be tested and defined over time through enforcement consistency and institutional maturity.

As enforcement activity increases, the Commission is expected to play a central role in shaping the interpretation of data protection obligations through decisions, guidance, and regulatory practice. For businesses, this signals a shift from statutory interpretation to regulatory-driven compliance standards.

2. Core Compliance Requirements & Definitions

2.1 Scope and Applicability

Tanzania's data protection regime applies to the collection and processing of personal data carried out wholly or partly by automated or manual means. Under section 22 of the Personal Data Protection Act (Cap. 44), the law applies to processing activities conducted by data controllers established in Tanzania as well as those carried out within the territory. It may also apply to foreign controllers or processors where personal data is processed within Tanzania and the activity is not merely data transit through the country. For multinational organisations, this means regulatory exposure may arise even where the parent entity is incorporated abroad.

Lawful Bases for Processing

Processing of personal data must be grounded in lawful and legitimate purposes. The Act requires that personal data be processed lawfully, fairly, and for specific purposes consistent with the data protection principles set out under section 5. While consent is a commonly relied-upon legal basis, particularly in consumer-facing sectors, it is not the only lawful ground. Processing may also occur where it is necessary for lawful functions of the controller, compliance with legal obligations, or purposes directly related to the original collection of the data.

Handling Sensitive Personal Data

The law imposes stricter conditions on the processing of sensitive personal data. Section 30 of the Act generally prohibits processing of such data without the prior written consent of the data subject, subject to limited exceptions recognised by law. Sensitive personal data includes, among others, biometric information, financial data, health records, genetic data, data relating to offences, and personal data concerning children. Organisations handling such information must implement enhanced safeguards and carefully document the legal basis for processing.

Regulatory Framework and Compliance Obligations

Additional compliance obligations are set out in the **Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.** These Regulations require controllers and processors to adopt organisational and technical safeguards, including privacy-by-design practices and proper security controls. They also require the appointment of a Data Protection Officer and the conduct of Data Protection Impact Assessments for processing activities that present higher risks to individuals' rights. Together, these requirements signal a shift toward structured internal data governance rather than informal handling of personal data.

2.2 Data Subject Rights

The PDPA grants individuals several enforceable rights over their personal data. These include:

- The right to access personal data held by a data controller.
- The right to prevent certain forms of processing likely to affect the data subject.
- The right to object to the use of data for direct marketing.
- The right to challenge decisions made solely through automated processing.
- The right to request rectification, erasure, blocking, or destruction of personal data in appropriate circumstances.

Practical Mechanisms for Exercising Rights

The practical exercise of these rights is primarily governed by the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023, particularly Part III, which establishes structured procedures for enforcing data subject rights. These procedures include prescribed application forms, defined timelines, and mandatory obligations on data controllers. For example, requests to prevent processing may trigger immediate suspension obligations within seventy-two (72) hours, followed by a formal determination within seven (7) days. Similarly, applications for rectification or erasure must generally be determined within fourteen (14) days from the date of receipt.

In practice, this framework creates a tiered enforcement model. Data subjects may initially invoke their rights directly against the data controller or processor using prescribed procedures. Where requests are rejected, ignored, or inadequately addressed, the matter may be escalated to the Personal Data Protection Commission through formal complaint mechanisms. This dual structure allows for both immediate intervention and regulatory enforcement.

From a practical perspective, certain rights are increasingly used strategically. The right of access is often invoked to obtain information necessary to assess compliance or establish potential breaches. The right to prevent processing likely to cause harm functions as an urgent protective mechanism, enabling individuals to halt ongoing or imminent processing. Rights relating to rectification and erasure are frequently used in cases involving inaccurate records, reputational harm, or continued use of personal data without lawful basis.

Limitations and Exemptions

The exercise of data subject rights is not absolute and may be limited in certain circumstances. The Act recognises exceptions where processing is necessary for national security, law enforcement, compliance with other written laws, or the protection of public interest. Limitations may also arise where exercising the right would prejudice ongoing investigations or legal proceedings. These safeguards seek to balance individual privacy rights with broader state and public interest considerations.

3. Governance, Accountability & Ongoing Compliance

3.1 Directors' Duties and Corporate Accountability

The PDPA places primary compliance responsibility on data controllers and data processors that collect or process personal data. While the Act does not create a detailed fiduciary framework specifically for company directors, it recognises corporate accountability where organisations violate data protection obligations.

Under Section 62 of the Act, offences committed by a company may extend liability to directors, managers, or officers who authorised, permitted, or failed to prevent the violation. This creates potential personal exposure for senior management in cases of serious compliance failures.

In practice, this provision encourages organisations to treat data protection as a governance issue rather than a purely technical or operational matter. Boards and senior executives are expected to ensure that internal systems for data protection compliance are in place and effectively monitored. Failure to implement appropriate safeguards may expose the organisation to administrative fines, enforcement notices, or compensation claims.

Data Protection Officer (DPO) Mandate

The appointment of a Data Protection Officer is a mandatory element of the governance framework. Section 27 of the Act requires data controllers and processors to designate a DPO responsible for

ensuring that security and compliance measures are implemented. Regulation 32 of the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 further provides that the DPO is responsible for overseeing compliance programmes, monitoring processing activities, and advising the organisation on data protection obligations.

The Act and its Regulations do not prescribe specific academic or professional qualifications for a DPO. The role is defined functionally, focusing on the DPO's responsibility to oversee compliance, monitor processing activities, and advise the organisation. In practice, organisations typically appoint individuals with legal, compliance, or information security backgrounds. The law does not require the DPO to be institutionally independent, and the role may be performed alongside other managerial responsibilities, provided there is no conflict of interest and the DPO can effectively discharge their duties.

Board Oversight Expectations

For boards of directors, oversight of data protection compliance increasingly forms part of broader corporate risk management. This includes ensuring that organisations maintain clear internal policies on data processing, security safeguards, incident response procedures, and regulatory engagement. As enforcement activity develops, boards are expected to demonstrate that they actively supervise organisational compliance programmes rather than delegating responsibility entirely to technical teams.

3.2 Key Annual Compliance Cycle Requirements

Beyond initial registration, the PDPA establishes ongoing compliance obligations for organisations that collect or process personal data.

- **Registration:** Under section 14 of the Act, controllers and processors must register with the Commission before commencing processing activities. Registration remains valid for five years as provided under section 16.
- **Quarterly Reporting:** Regulation 32(c) of the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 requires the DPO to prepare and submit a quarterly compliance report to the PDPC. For businesses, this means compliance is not a one-time exercise but an ongoing regulatory obligation.
- **Internal Governance:** Organisations must maintain internal compliance systems ensuring personal data is processed in accordance with the core principles under section 5 of the Act. This typically requires internal data governance frameworks, documented policies, and periodic internal compliance reviews.

While the Regulations require quarterly reporting, they do not prescribe a standardised template or detailed format. In practice, reporting expectations are still developing. Reports typically include summaries of data processing activities, compliance measures implemented, data subject requests received, and any identified incidents or risks. As regulatory practice evolves, more structured reporting guidance is expected to emerge from the Commission.

Data Protection Impact Assessments (DPIAs)

DPIAs are required where processing activities may present a significant risk to the rights and interests of data subjects. The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 require organisations to conduct DPIAs before undertaking high-risk processing activities and to submit the assessment results to the Commission where necessary. The Commission may issue directions or require mitigation measures where identified risks are not adequately addressed. For organisations deploying new digital systems or large-scale data analytics, DPIAs are therefore becoming an important compliance tool.

Breach Notification Requirements

The Act imposes obligations relating to personal data security breaches. Under section 27(5) of the Act, a data controller must notify the Commission without undue delay where a breach affecting personal data occurs. The Act does not prescribe a fixed statutory timeframe — such as 72 or 48 hours — and the Regulations currently do not specify a statutory deadline either. This creates interpretive flexibility but also regulatory uncertainty for organisations. To mitigate risk, many organisations adopt international best practices by reporting within a short and reasonable timeframe internally defined as 48 to 72 hours. As enforcement practice develops, the Commission is expected to clarify

expectations regarding notification timelines and whether distinct obligations apply to notifying affected data subjects as distinct from the Commission.

Practical Implementation Challenges

In practice, many organisations are still developing the operational capacity required to meet these ongoing obligations. Businesses that rely heavily on digital platforms, financial transactions, or large customer databases face higher compliance expectations. As enforcement activity increases, regulators are expected to scrutinise whether organisations have implemented structured compliance programmes rather than relying on reactive responses to complaints.

4. Enforcement and Practical Reality

4.1 Regulatory Activity

Although Tanzania's data protection regime is relatively recent, enforcement activity has already moved beyond a purely formative stage into substantive regulatory intervention. The Personal Data Protection Commission has demonstrated a willingness to investigate complaints, conduct quasi-judicial proceedings, and issue binding decisions with financial consequences.

In practice, enforcement proceedings before the Commission resemble structured adjudicatory processes involving investigation, hearing, and determination. Where violations are established, the Commission has exercised its powers to issue compliance orders, mandate deletion of unlawfully processed data, impose administrative penalties, and award compensation.

Enforcement Decisions

A significant illustration of this enforcement posture is seen in **Abdul Said Naumanga v. Mi Casa Company Limited (Complaint No. PDPC/CMP/014/2024)**, where the Commission found that the unauthorised use of personal images and video content constituted unlawful processing. The Commission ordered immediate removal of the content and awarded compensation of TZS 20,000,000. This decision is particularly instructive for two reasons: it confirms that informal digital conduct such as social media content creation falls squarely within the scope of regulated data processing, and it demonstrates that the Commission is prepared to attach direct financial consequences to privacy violations, even outside traditional corporate environments.

Similarly, in **Nyangoma Mwesigwa v. Cecilia Maliganya (Complaint No. PDPC/CMP/002/2025)**, the Commission addressed the unauthorised commercial use of a child's image. The decision reinforced the heightened protection afforded to sensitive personal data and confirmed that the absence of parental written consent constitutes a serious compliance failure.

Emerging Enforcement Patterns

Taken together, these decisions indicate an emerging enforcement pattern: the Commission is prioritising consent violations, misuse of sensitive data, and publicly visible forms of non-compliance. For organisations, this creates a clear risk profile — activities involving marketing, digital platforms, and biometric or visual data carry elevated regulatory exposure. While the current approach is calibrated, this should not be interpreted as regulatory leniency. As institutional capacity develops, there is a strong likelihood of progressive escalation in both the scale and frequency of penalties.

Advisory and Awareness Role

In addition to enforcement, the Commission plays an important advisory and awareness-building role. It engages with stakeholders through registration processes, complaint-handling procedures, and public awareness initiatives aimed at promoting compliance with the Act. While formal codes of conduct and certification mechanisms are still developing, the Commission's ongoing engagement with organisations and the public is gradually shaping practical understanding of data protection obligations. This dual role of enforcement and guidance reflects an evolving regulatory approach focused on both accountability and compliance support.

4.2 Private Litigation

The Personal Data Protection Act recognises the right of individuals to seek compensation for harm arising from unlawful processing of personal data. Section 37 provides a statutory basis for claims relating to both material and non-material damage,

establishing a direct link between regulatory non-compliance and potential civil liability exposure for organisations.

However, in practice, enforcement of data protection rights in Tanzania remains predominantly regulator-driven rather than court-driven. Most disputes are initiated through complaints before the Personal Data Protection Commission rather than through standalone court proceedings.

Key Interpretive Developments
Recent enforcement decisions indicate an important interpretive development in Tanzania's data protection framework. The Commission has recognised that the continued availability of personal data online without consent may constitute an ongoing violation rather than a single completed act. This approach reflects the reality of digital environments, where harm persists for as long as personal data remains accessible.

In at least one concluded case, the Commission asserted jurisdiction over a violation that originated prior to the commencement of the Act but continued through ongoing publication of personal data. This interpretation has significant implications for how limitation periods and historical regulatory exposure may be understood in practice, particularly for organisations that have been processing data for several years.

5. Cross-Border Data Transfers

5.1 Transfer Mechanisms

The transfer of personal data outside Tanzania is regulated under Part V of the Personal Data Protection Act (Cap. 44). Section 31 permits transfers to jurisdictions that provide an adequate level of protection for personal data, ensuring that equivalent safeguards continue to apply after the data leaves Tanzania.

Where the receiving country does not provide adequate protection, section 32 allows transfers only where appropriate safeguards are in place. These may include contractual arrangements or other legally recognised mechanisms. In such cases, the data controller must demonstrate that the rights of the data subject will not be undermined.

Approval Process for Transfers
The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 introduce a formal approval process for cross-border data transfers. Under Regulation 20, controllers and processors must apply to the Commission for a transfer permit using a standard form (Form No. 7), accompanied by supporting documentation demonstrating the adequacy of protection in the receiving jurisdiction, including contractual arrangements, international agreements, or other recognised safeguards.

The Commission is required to consider and determine a transfer application within 14 days from the date of receipt. In practice, the effectiveness of this timeline depends on the completeness of the application and the complexity of the transfer arrangement. Applications supported by clear documentation and well-defined safeguards are more likely to be processed within the statutory period, while incomplete or high-risk transfers may require further engagement with the Commission before approval is granted.

Adequacy Decisions and Recognised Mechanisms
At present, the Commission has not issued a formal whitelist of jurisdictions deemed to provide adequate protection. Similarly, the law does not expressly recognise specific international transfer mechanisms such as the European Union's Standard Contractual Clauses (SCCs). As a result, transfer approvals are assessed on a case-by-case basis, with emphasis placed on the existence of adequate safeguards and regulatory oversight in the receiving jurisdiction.

Practice for Multinational Organisations
In practice, multinational organisations operating in Tanzania manage cross-border data transfers through a combination of internal compliance frameworks, contractual safeguards, and prior engagement with the Commission. Many organisations adopt group-wide data protection policies and standard contractual arrangements to support transfer applications. Where cloud services or foreign data infrastructure are involved, regulatory approval and documentation of safeguards have become essential components of compliance strategy.

6. Sector-Specific & Emerging Challenges

6.1 Critical Sectors

Although the Personal Data Protection Act establishes a general framework applicable across sectors, several industries process personal data at a scale that attracts heightened regulatory attention. These include financial services, telecommunications, digital platforms, healthcare institutions, and public sector databases. In such sectors, compliance with the PDPA must operate alongside existing regulatory regimes governing confidentiality, cybersecurity, and consumer protection.

Tanzania does not yet have fully developed, standalone data protection regimes for individual sectors. Instead, sectoral obligations operate alongside the PDPA, creating a layered compliance framework. Organisations in regulated industries must therefore comply simultaneously with sector-specific requirements and the general data protection principles established under the Act.

- **Financial Services:** Banks and fintech companies handle large volumes of sensitive financial data relating to transactions, identification records, and payment systems. These institutions must combine financial confidentiality obligations with the data protection principles under section 5 of the Act. The growing use of digital financial services and mobile payments has significantly increased the volume of personal data processed within the sector.
- **Telecommunications:** Telecom operators process extensive subscriber information, including identification records, communication data, and digital service usage information. Because of their role as infrastructure providers, telecom operators are often among the largest holders of personal data within the economy and must align their practices with both telecommunications regulation and the PDPA.
- **Healthcare:** Healthcare institutions handle sensitive personal data as defined under the Act, including medical histories and biometric identification. Processing such information requires stricter safeguards and careful control of access within hospitals, clinics, and digital health platforms.

Data Localisation Requirements

At present, the PDPA does not impose a general data localisation requirement. However, cross-border data transfers are subject to regulatory approval and oversight under Part V of the Act and the applicable Regulations. In practice, this creates a controlled transfer regime rather than unrestricted data mobility.

6.2 Technology Frontiers

Rapid digital transformation is introducing new regulatory challenges for data protection in Tanzania. Emerging technologies such as artificial intelligence, machine learning systems, biometric identification tools, and digital identity platforms rely heavily on personal data. While the current legal framework provides general data protection principles, there are no technology-specific regulations or detailed guidelines addressing these emerging areas. As a result, organisations must interpret and apply general principles of the Act to increasingly complex technological environments.

- Biometric Identification: Biometric systems are increasingly used in financial services, telecommunications registration processes, and digital identity verification. Because biometric data falls within the definition of sensitive personal data under the Act, organisations deploying such technologies must obtain explicit consent and implement enhanced safeguards. Failure to protect biometric information carries significant regulatory risk.
- Digital Surveillance: Digital surveillance technologies, including CCTV monitoring and communication interception systems, raise privacy considerations even where used for security purposes. Their deployment must respect the data protection principles established by the Act, and organisations are expected to ensure that data collection is proportionate, limited to legitimate purposes, and protected against misuse

As digital technologies continue to expand across the economy, regulators are expected to focus more closely on high-risk data processing activities. Organisations deploying advanced data analytics, biometric verification tools, or automated decision-making systems should integrate data protection considerations at the design stage of

their digital infrastructure, consistent with the principle of privacy-by-design reflected in the regulatory framework.

There is currently no comprehensive standalone legal framework specifically governing digital surveillance or CCTV use from a data protection perspective. Such activities are regulated through a combination of general data protection principles and sector-specific laws, including telecommunications and criminal procedure frameworks. This fragmented regulatory approach creates compliance uncertainty, particularly for private sector actors deploying surveillance and digital monitoring systems.

While the Commission has not yet issued detailed sector-specific guidance on emerging technologies, there is a growing expectation within the regulatory and professional community that such guidance will be developed in the near term. Given the increasing use of biometric systems, artificial intelligence, and digital identity platforms, these areas are likely to form part of the Commission's future regulatory agenda. Stakeholder engagement and gradual development of secondary guidance are expected to play a key role in shaping compliance expectations in these high-risk areas.

7. Outlook and Recommendations

7.1 Perceived Gaps and Pressures

Despite the establishment of a comprehensive legal framework, several practical challenges continue to shape the implementation of data protection law in Tanzania.

- Organisational Capacity: A primary challenge lies in the gap between formal compliance requirements and organisational capacity. Many institutions — particularly those operating legacy systems — lack the technical infrastructure and internal governance frameworks required to operationalise data protection obligations. As a result, compliance is often reactive rather than embedded within organisational processes.
- Market Capacity Gap: There is a significant capability gap in the market. Smaller businesses and public institutions frequently lack access to specialised expertise in data governance, cybersecurity, and regulatory compliance. This creates uneven implementation across sectors, with larger organisations advancing more rapidly while smaller entities lag behind.
- External Pressures: Rapid digitalisation, expansion of mobile financial services, and increasing reliance on cross-border data flows are placing strain on existing compliance structures. Regional integration frameworks such as the AfCFTA are likely to intensify the need for harmonised data protection standards across African jurisdictions.
- International Alignment: International regulatory trends, particularly those influenced by frameworks such as the GDPR, are shaping expectations around accountability, transparency, and cross-border data governance. For Tanzania, alignment with such standards is increasingly linked to participation in the global digital economy.

7.2 Future Trajectory

Although the current legal framework is relatively new, there are no widely publicized major legislative amendments currently pending that would significantly alter the structure of the data protection regime before the end of 2026. Instead, the immediate evolution of the framework is expected to occur through regulatory practice, guidance, and enforcement activity.

As awareness of privacy rights increases, the number of complaints submitted to the Commission is likely to grow, leading to a gradual increase in investigations, enforcement notices, and administrative sanctions against non-compliant organisations. The Commission is also expected to place greater emphasis on public awareness, stakeholder engagement, and the development of practical compliance guidance.

High-risk sectors such as telecommunications, financial services, and digital platforms are likely to receive increased regulatory attention. Over time, enforcement decisions and regulatory engagement are expected to clarify how core principles of the Act apply in practice, particularly in relation to consent, sensitive data, and cross-border transfers.

Recommendations for Reform

Looking ahead, one practical reform that could significantly strengthen the effectiveness of Tanzania's data protection regime would be the development of detailed regulatory guidelines for high-risk technologies and digital services. Clear and sector-specific guidance on artificial intelligence, biometric identification systems, and cross-border data transfers would provide greater certainty for organisations operating in the digital economy. Such measures would also support consistent enforcement and reduce compliance uncertainty across sectors.

05 Uganda

CONTRIBUTOR

Daisy Bigabwa is a lawyer with expertise in financial services and AI powered solutions. She focuses on data governance, risk management, and regulatory compliance. With a strong passion for data governance frameworks, she enables innovative companies to build secure, trustworthy, and compliant solutions. Her work bridges law and technology, ensuring that emerging products align with evolving global standards while mitigating risk. She is driven by the challenge of enabling responsible innovation in fast-paced digital environments.

CONTRIBUTOR

Kityo Martin is a tech lawyer with expertise in data privacy and emerging technology governance. He acts as legal counsel for corporate entities, startups and individuals offering them advisory, consultancy and compliance services to ensure that they conduct sustainable business operations. Martin is a privacy consultant with DPO Privacy Centre East Africa and currently heads its Data Protection, Privacy and Cybersecurity Desk.

1. The Legislative and Regulatory Landscape

1.1 Primary Legal Framework

Uganda's data protection regime is anchored in the Data Protection and Privacy Act, Cap. 97 (the DPPA), which was enacted and came into force on 3rd May 2019. The law establishes the legal framework governing the protection of personal data and the privacy of individuals across both public and private sectors.

To operationalise its provisions, the Data Protection and Privacy Regulations (DPPR) were issued in 2021. Together, the DPPA and the DPPR constitute the primary compliance framework for data controllers, processors, and collectors operating in Uganda.

From a business standpoint, the DPPA represents a structural shift from informal data handling practices to a regulated governance model. Organisations are now required to treat personal data as a regulated risk category rather than a routine operational resource, with formal obligations around registration, security, and accountability.

Constitutional Foundation

Article 27 of the Constitution of the Republic of Uganda, 1995 (as amended) recognises the right to privacy. This includes protection from unlawful interference with a person, their home, communications, and premises. The DPPA operationalises this constitutional guarantee by translating it into enforceable data protection obligations.

Sectoral Laws and Their Interaction

In addition to the DPPA, several sectoral laws impose parallel privacy and cybersecurity obligations that interact with the general data protection regime. Key instruments include:

- The National Payment Systems Act, Cap. 59, governing the processing of financial transaction data and imposing security and confidentiality obligations on payment service providers.
- The Regulation of Interception of Communications Act, Cap. 101, governing lawful interception of electronic communications and setting conditions under which state agencies may access private communications data.
- The Access to Information Act, Cap. 95, which, while primarily enabling access to government-held information, also recognises limits on disclosure where privacy interests are at stake.
- The Tax Procedures Code Act, Cap. 343, which imposes a duty on the Uganda Revenue Authority (URA) to keep taxpayer information confidential under Section 55, while permitting collection of personal data necessary for the performance of public duties under Section 7.

The interaction of these instruments with the DPPA was directly examined by the High Court in Bitungwa Johnson v Uganda Revenue Authority (Civil Suit 23 of 2021) [Decided in November 2025]. The court confirmed that the DPPA applies to public bodies such as the URA in their capacity as data controllers, and that a data subject whose personal data has been inaccurately held or disclosed by a public body has a right to seek correction under Section 16 of the DPPA. The court also clarified that where a specific law, such as the DPPA provides a specific remedy, that statutory route must be engaged first before resorting to general civil proceedings. The administrative complaint mechanism available through the National Information Technology Authority (NITA-U) is therefore the preferred first avenue for data protection disputes with public bodies.

1.2 The Supervisory Authority

The Personal Data Protection Office (PDPO) is the national regulator charged with overseeing the implementation of the DPPA and the DPPR. The PDPO was established as an independent office under the National Information Technology Authority of Uganda (NITA-U) and began operations in 2021.

The PDPO is funded through the government budget. Its head the National Personal Data Protection Director reports to the Board governing NITA-U. However, the DPPA explicitly provides that in the exercise of its functions, the PDPO operates independently and is not subject to the direction or control of any person or authority. This statutory safeguard is intended to ensure a degree of operational independence from government influence.

A notable structural limitation is that the PDPO does not have corporate status it is an office within NITA-U rather than an independent body with its own legal personality. This affects its institutional autonomy and, in practice, may constrain its capacity to act independently of NITA-U's governance structures. Additionally, appeals from the PDPO's decisions are directed to the Minister responsible for ICT, a proximity that raises legitimate concerns about the independence of the appellate process.

The PDPO has five broad categories of statutory powers: investigative powers to examine suspected violations; corrective powers to issue compliance orders and remedial directions; advisory powers to provide guidance to organisations and data subjects; supervisory powers to monitor compliance with the Act and Regulations; and authorisational powers in relation to cross-border data transfers and specific processing activities.

2. Core Compliance Requirements & Definitions

2.1 Scope and Applicability

Uganda's data protection framework has an extraterritorial reach. Under Section 2 of the DPPA, the law applies to every person, institution, or public body whether private or public that collects, processes, or stores personal data relating to Ugandan citizens, regardless of whether that entity is based within or outside Uganda. This position was affirmed by the PDPO in its decision in Frank Ssekamwa & Others v Google LLC, which confirmed the Act's application to foreign based technology companies processing data belonging to Ugandan users.

Lawful Bases for Processing

Consent is the primary basis for processing personal data in Uganda. However, the DPPA recognises several other lawful grounds, including: national security; performance of a public duty; legitimate interests of the controller that do not override the rights of the data subject; law enforcement purposes; contractual necessity; research or statistical purposes; medical purposes; and compliance with a legal obligation to which the data controller is subject.

In practice, public bodies such as the URA rely on the public duty ground confirmed in the Bitungwa judgment while financial institutions and telecoms commonly invoke contractual necessity and legal obligation. Consent remains dominant in consumer-facing digital services.

Sensitive Personal Data

The DPPA imposes heightened obligations where an entity processes special categories of personal data sometimes referred to as sensitive personal data. Two specific requirements apply. First, where an organisation's core activities involve processing such data, it is required to appoint a Data Protection Officer (DPO) to oversee compliance. Second, where the intended processing of sensitive data is likely to result in a high risk to the rights and freedoms of individuals, the organisation must conduct a Data Protection Impact Assessment (DPIA) before commencing processing.

Sensitive data categories include health and medical information, biometric identifiers, financial data, and data relating to children. The Anguzu Bruce DNA ruling (Civil Application No. 059 of 2025, December 2025) is instructive on the treatment of genetic data as a form of sensitive personal data. The court held that collecting DNA samples which constitute personal genetic data from individuals requires their explicit written consent. In data protection terms, the court reasoned that the Data Protection and Privacy Act governs the collection of such information as personal data: adults retain full rights to decline collection, and where children are involved, prior consent of a parent or guardian is required under Section 8 of the DPPA. The absence of written consent from the adult individuals whose DNA was sought was a primary ground for dismissing the application.

2.2 Data Subject Rights

The DPPA grants individuals a suite of enforceable rights over their personal data:

- Right of access, to obtain confirmation of and access to personal data held by a data controller.
- Right to object or prevent processing, to refuse certain forms of processing that affect the data subject.
- Right to rectification, to request correction of inaccurate or incomplete personal data.
- Right to erasure, to request deletion of personal data in appropriate circumstances.
- Right to lodge a complaint, to report violations of the DPPA to the PDPO.

Notably, unlike data protection laws in comparable jurisdictions, the DPPA does not provide for a right to data portability. This has been confirmed by the PDPO in its decision in Ssimbwa Phillip v Chipper Technologies.

Practical Mechanisms for Exercising Rights

Individuals are first required to submit complaints directly to the organisation responsible for processing their personal data. If the organisation fails to resolve the matter satisfactorily, the individual may escalate the complaint to the PDPO, either electronically through the PDPO's online portal (https://pdpo.go.ug/file-complaint) or in person at the PDPO's offices at the 7th Floor, Padre Pio House, Plot 32, Lumumba Avenue, Kampala.

The primary form for lodging complaints with the PDPO is Form 11 (Complaints Concerning Infringement or Violation of the Act). Specialised complaints may be submitted using Form 6 (processing without appropriate security measures) or Form 9 (inaccurate personal data held by a data controller). The Bitungwa case further illustrates the statutory mechanism: where a data subject requests correction of their data under Section 16 of the DPPA, the data controller is obliged to comply and to notify the data subject of the correction made. If the controller fails to act, the data subject's recourse is to file a complaint with NITA-U (specifically PDPO) as the designated authority under Section 31 of the Act.

Limitations and Exemptions

Data subject rights under the DPPA are not absolute. Controllers and processors are not required to act on every request, but any refusal must be communicated to the data subject in writing with the reason stated. Grounds for declining to act on a request include national security, law enforcement, performance of public duties, medical purposes, and research or statistical purposes. The right to privacy itself is subject to permissible derogation as the Bitungwa court confirmed by reference to Article 44 of the Constitution, which does not list privacy among the non-derogable rights.

3. Governance, Accountability & Ongoing Compliance

3.1 Directors' Duties and Corporate Accountability

Directors and senior officers of organisations are responsible for ensuring compliance with the DPPA and its Regulations, including obligations relating to registration and the lawful collection and processing of personal data. The DPPA creates routes to personal liability for corporate officers: where a violation occurs, any officer who knowingly and wilfully authorised or permitted the acts leading to that violation may be held personally liable and prosecuted alongside the organisation.

The significance of personal liability was demonstrated in Uganda v Mugulusi Ronald, Uganda's first criminal conviction under the DPPA, in which a director of a digital money lending company was prosecuted for unlawfully obtaining and disclosing personal data. This decision confirms that individuals at the executive level face real exposure for compliance failures, not only the companies they direct.

Data Protection Officer (DPO) Mandate

Appointment of a DPO is mandatory under Regulation 47 of the DPPR for organisations whose activities involve regular and systematic monitoring of data subjects on a large scale, or whose core activities involve the processing of special (sensitive) personal data. Entities that do not meet these thresholds are not automatically required to appoint a DPO, though doing so is considered good practice. Practically, any entity going through the PDPO registration process is required to designate someone in the DPO role.

A DPO may be appointed from within the organisation or engaged externally. The DPPA and DPPR do not prescribe minimum academic qualifications, but the appointee should have knowledge of data protection law, organisational policies, and information technology sufficient to influence compliance within the organisation. The DPO must be appointed by the head of the company or institution.

Board Oversight Expectations

Boards of Directors are expected to exercise active but non-interfering oversight of the organisation's data protection compliance programme. In practice, this means providing strategic direction and governance without micromanaging operational compliance activities; ensuring that the DPO operates with sufficient independence and is free from undue influence; and giving timely consideration to DPO recommendations. As enforcement activity develops, boards will increasingly be expected to demonstrate that data protection is embedded in enterprise risk management rather than treated as a technical afterthought.

3.2 Key Annual Compliance Cycle Requirements

Beyond initial registration, the DPPA and its Regulations impose several ongoing compliance obligations:

- **Registration Renewal:** Organisations must renew their registration certificate with the PDPO annually, at least three months before expiry.
- **Annual Compliance Reports:** Organisations must prepare and submit a compliance report to the PDPO within 90 days of the end of each financial year (i.e. by the end of September). The report must cover data protection activities, compliance status, leadership changes, breaches suffered, and data protection training undertaken.
- **Breach Notification:** Upon discovering any data breach, organisations must immediately notify the PDPO using Form 7, providing details of the breach, the personal data at risk, and remedial actions taken. While no specific number of hours is prescribed, the use of the term 'immediately' indicates that notification must occur without undue delay.

- **Staff Training:** Organisations must conduct routine data protection training for staff as part of their ongoing compliance obligations.

Data Protection Impact Assessments (DPIAs)
A DPIA is mandatory prior to commencing any collection or processing of personal data that is likely to pose a high risk to the rights and freedoms of natural persons. Under Regulation 12 of the DPPR, a DPIA must include a systematic description of the envisaged processing operations and their purposes; an assessment of the risks to personal data; the measures proposed to address and mitigate those risks; and any additional information specified by the PDPO.

The PDPO is mandated to publish a list of processing operations that automatically require a DPIA, though this list has not yet been published. The law does not require routine prior submission or approval of DPIAs by the PDPO. However, the PDPO may require disclosure of a DPIA during oversight activities, and organisations should maintain DPIAs as core accountability documentation.

Notification to Data Subjects Following a Breach
Organisations are not automatically required to notify affected data subjects following a breach. Instead, the PDPO assesses the breach upon receiving the organisation's notification and determines whether direct notification to individuals is necessary. Where required, the PDPO directs the organisation on whether and how to notify. Methods of notification to data subjects include registered mail, electronic mail, a prominent notice on the organisation's website, or publication in mass media. The notification must include sufficient information about the breach to enable data subjects to take protective measures.

4. Enforcement and Practical Reality

4.1 Regulatory Activity

The PDPO has demonstrated an increasingly assertive enforcement posture, extending its reach to major multinational technology companies and establishing important precedents in the first years of its operation.

Landmark Enforcement Decisions

- Frank Ssekamwa & Others v Google LLC (2025): The PDPO found Google LLC in breach of its statutory obligations for failing to register as a data controller and for conducting unlawful cross-border data transfers. The decision affirmed the DPPA's extraterritorial applicability to foreign technology companies processing data of Ugandan users.
- AdLegal v WhatsApp & Meta (2026): Both companies were found to have failed to obtain proper consent from Ugandan users and to have offered those users weaker data protections than were provided to users in other jurisdictions. The PDPO ordered compliance with registration requirements and cross-border data transfer obligations, and recognised that non-material harm is actionable within Uganda's legal framework.
- Uganda v Mugulusi Ronald (2025): Uganda's first criminal conviction under the DPPA — a company director of a digital lending platform was prosecuted for unlawfully obtaining and disclosing personal data, confirming that individuals face personal criminal liability for DPPA violations.
- Uganda Securities Exchange investigation: Following a report from civil society organisation Unwanted Witness, the PDPO investigated and confirmed a data breach on a server hosted in Germany, illustrating the regulator's engagement with cross-border data security issues.
- Safeboda Uganda (pre-PDPO): NITA-U investigated suspected sharing of client data with foreign platforms without consent, following a complaint from Unwanted Witness. Safeboda was ordered to make specific modifications to its privacy policy, an early precedent for platform accountability.

Penalties and Enforcement Range
Under the DPPA, a corporation convicted of an offence may be fined up to 2% of its annual gross turnover. Individuals face a maximum fine of 240 currency points (approximately UGX 4,900,000 or USD 130) or imprisonment for up to 10 years, or both. To date, the PDPO has not applied the maximum penalties, focusing instead on remedial orders and compliance directions. As institutional capacity develops, escalation in the scale of

sanctions is expected.

Guidance and Advisory Activity

The PDPO publishes guidance notes and advisory materials to support compliance, though these remain limited in scope and do not yet comprehensively cover all sectors. The PDPO engages with stakeholders through consultations, workshops, and public awareness initiatives, though the depth and frequency of engagement is not yet consistent. Sector-specific guidelines have not been published; the PDPO has indicated these are anticipated.

4.2 Private Litigation

The DPPA provides individuals with enforceable rights when their personal data is misused or processed unlawfully. Where harm is suffered including financial loss, reputational damage, identity theft, discrimination, or emotional distress individuals may pursue remedies through two main avenues: a complaint to the PDPO (which can issue compliance directives and corrective orders) or a civil claim before the courts (which may award monetary compensation and other relief such as injunctions, data deletion orders, or directives to improve data security).

Importantly, the PDPO itself does not have the power to award compensatory damages as that power is reserved for the courts. This means that data subjects seeking financial redress must pursue separate court proceedings after exhausting the PDPO process, which adds complexity and cost to enforcement.

Key Cases Building Uganda's Data Protection Jurisprudence

- **ABC Capital Bank Ltd & 30 Others v Attorney General (Constitutional Court, March 2023):** The Constitutional Court clarified the balance between the right to privacy under Article 27 of the Constitution and the State's legitimate interest in tax collection, holding that state access to financial data must be justified by reasonable suspicion of tax fraud. This reasoning has influenced interpretation of the DPPA.
- **Nalubega Shadia v Stabex International Ltd (June 2023):** An employer used an employee's photograph for marketing purposes without her consent. The court confirmed that consent to process personal data must be clear, unequivocal, and provided by the data subject personally. Employer-assumed consent is not sufficient.
- **Bitungwa Johnson v Uganda Revenue Authority (November 2025):** The High Court at Kabale examined the erroneous disclosure of a taxpayer's identification number (TIN) by the URA, which led to motor vehicles being registered in his name without his knowledge and a tax demand being issued against him. The court found that the URA, as a public body and data controller under the DPPA, had an obligation to correct inaccurate personal data under Section 16 of the Act. No award of general damages was made as the URA had taken steps to correct the error, but the court issued an important structural ruling: where the DPPA provides a specific remedy, that statutory route must be invoked first. The preferred mechanism for data protection complaints against public bodies is the administrative complaint process to the PDPO under Section 31 of the Act, not direct civil litigation. The case underscores the importance of robust internal data governance by public institutions and the risks of holding inaccurate personal data.
- **In the Matter of the Estate of the Late Anguzu Bruce Exhumation Appln (December 2025):** The High Court at Kabale ruled on an application to exhume a deceased person's body to conduct DNA testing to determine the paternity of six alleged children for succession purposes. The court dismissed the application on several grounds, including a critical data protection basis: the six adult individuals whose DNA was sought had not given written consent to the collection of their genetic data, and no evidence was placed before the court that their consent had even been sought. Applying Section 8 of the DPPA, the court held that where DNA testing involves children, prior consent of a parent or guardian is required; where it involves adults, those individuals retain the right to decline collection of their biological data. The court further held that DNA data, as genetic information constitutes personal data protected under the DPPA, and that its collection requires explicit consent unless a court order mandates otherwise for compelling legal reasons. The

ruling establishes that the DPPA applies to biological and genetic data collection in the succession and family law context, and that consent is a foundational prerequisite. It also signals that courts will scrutinise data collection applications involving sensitive personal data with heightened care.

5. Cross-Border Data Transfers

5.1 Transfer Mechanisms

The DPPA establishes that personal data may only be transferred outside Uganda if the receiving country or organisation ensures an adequate level of protection for the personal data concerned. Adequacy is assessed by examining whether the legal framework, technical safeguards, and institutional protections available in the destination jurisdiction provide protections comparable to those required under Ugandan law. An adequacy assessment must be submitted to the PDPO.

Where adequacy cannot be established, transfers may still be permitted through the following alternative mechanisms: contractual protections detailed contractual clauses requiring the recipient to maintain confidentiality, implement appropriate security measures, and respect data subject rights; consent of the data subject where individuals have been clearly informed of the purpose and implications of the transfer, and consent is freely given, informed, and specific; and necessity-based transfers where the transfer is required for contract performance, establishment or defence of legal claims, or recognised public interest reasons such as international payment processing.

Adequacy List and Recognised Mechanisms

The PDPO has not issued a formal whitelist of countries recognised as providing adequate protection. Adequacy is therefore evaluated on a case-by-case basis. While the DPPA does not expressly reference EU Standard Contractual Clauses (SCCs), the PDPO generally regards internationally recognised contractual frameworks as evidence that an organisation has taken reasonable steps to ensure adequate protection. Many multinational companies operating in Uganda adopt contractual arrangements modelled on EU SCCs, or implement internal Binding Corporate Rules-equivalent frameworks applicable across all group entities.

Practice for Multinational Organisations

In practice, multinationals manage cross-border data flows through comprehensive data governance frameworks aligned with international standards including ISO 27001 for information security combined with transfer impact assessments that evaluate the legal protections and security measures in destination jurisdictions. Regulated sectors such as banking require financial data to be stored within Uganda or within a regional cloud; government entities must use the NITA-U-controlled public cloud. For other operational data, hybrid infrastructure models are common, with sensitive datasets stored locally and less sensitive data processed internationally.

6. Sector-Specific & Emerging Challenges

6.1 Critical Sectors

While the DPPA establishes a general framework applicable to all sectors, several industries attract heightened compliance attention due to the sensitivity and scale of personal data they handle.

- **Financial Services:** Banks, payment service providers, and fintech companies are supervised by the Bank of Uganda and face strict cybersecurity and data protection obligations as part of their licensing requirements. Customer financial data, transaction records, and account information must be protected against unauthorised access and fraud. Financial data is required to be stored within Uganda or within regional servers regulators do not permit offshore storage of financial data outside the region.
- **Telecommunications:** The Uganda Communications Commission regulates telecoms, which process large volumes of subscriber identity data, communications metadata, and mobile money transaction data. SIM card registration and subscriber verification requirements mean telecoms collect detailed identification data, making strict confidentiality safeguards essential.
- **Healthcare:** Healthcare providers handle highly sensitive patient records, laboratory results, and insurance data. Professional confidentiality

obligations apply alongside the DPPA, and access must be strictly limited to authorised personnel. The health sector is also subject to forthcoming changes under the National Health Compact (2025-2030), which aims to standardise medical record retention and introduce new rules for digital health data governance.

The PDPO has not yet published sector-specific guidelines to supplement the DPPA and DPPR, though these are anticipated in the near term.

Data Localisation Requirements

Uganda does not impose broad mandatory data localisation requirements across all sectors. However, sector-specific expectations apply. Financial institutions are expected to maintain records accessible to supervisory authorities and to store financial data within Uganda or regional servers. Government information systems processing citizen data are typically required to use infrastructure located in Uganda or under NITA-U-approved service providers. Outside these categories, no general localisation obligation applies to commercial data, though organisations are encouraged to adopt hybrid infrastructure strategies that maintain local copies of sensitive datasets.

6.2 Technology Frontiers

Uganda has not yet enacted AI-specific legislation. The general principles of the DPPA including consent, purpose limitation, data minimisation, and accuracy apply to AI-driven data processing, though their application to automated decision-making is not explicitly codified. The Ministry of ICT and National Guidance is developing a National AI Strategy and has recently invited public consultation, aiming to create a framework for ethical AI use and data protection in automated systems.

Biometric technologies are widely used in Uganda for identity verification, access control, and financial authentication. Because biometric data is sensitive and cannot easily be changed if compromised, the DPPA requires heightened safeguards. The Anguzu Bruce DNA ruling reinforces this: genetic and biometric data collection requires explicit consent, and courts will scrutinise applications involving biological data with heightened care.

Digital surveillance and communications interception are governed by the Regulation of Interception of Communications Act, Cap. 101 and the Uganda Communications Act, Cap. 103. Interception is generally permitted only under specific legal conditions and requires authorisation from designated authorities. Telecoms are required to maintain lawful interception capabilities. CCTV operators both public and private must ensure that surveillance is notified to individuals where feasible, that footage is used only for legitimate and proportionate purposes, and that recorded data is protected in accordance with the DPPA.

7. Outlook and Recommendations

7.1 Perceived Gaps and Pressures

Despite meaningful progress since the DPPA came into force, several structural gaps continue to shape the enforcement and compliance landscape in Uganda.

- **Guidance Deficit:** Many organisations require practical guidance on breach notification procedures, acceptable security standards, and cross-border transfer mechanisms. The PDPO's guidance outputs remain limited and do not comprehensively cover the range of sectors and scenarios that arise in practice.
- **SME Awareness:** Smaller businesses collect and process personal data as part of everyday operations but frequently lack awareness of their legal obligations or the capacity to implement structured compliance programmes.
- **PDPO Institutional Constraints:** The PDPO operates as an office within NITA-U rather than as an independent corporate body. This limits its institutional autonomy. Additionally, the PDPO lacks the power to award compensatory damages a reserve for the courts — which means data subjects seeking financial redress must initiate separate judicial proceedings, adding cost and complexity to enforcement.
- **Appeals Structure:** Appeals from PDPO decisions are directed to the Minister responsible for ICT. The law is silent on whether the Minister's decision is final or what further appellate routes exist. This proximity between the decision-maker and the appellate authority raises concerns about independence, and the absence of any tested appeals leaves significant

uncertainty about the practical scope of appellate review.

- **Rapid Digitalisation:** The growth of Uganda's digital economy including mobile money services, e-government platforms, and fintech innovation continues to outpace regulatory capacity. Cross-border data flows are increasing and the regulatory framework has not yet developed sufficient tools to manage the associated risks.

External pressures are also shaping Uganda's reform agenda. Regional integration initiatives under the AfCFTA emphasise harmonised digital governance standards. The influence of the EU GDPR continues to shape expectations around accountability and cross-border transfers among international partners engaging with Ugandan organisations. Uganda's aspirations as a regional technology and fintech hub further underscore the importance of a credible, functional data protection regime.

7.2 Future Trajectory

Uganda's health sector is set for regulatory changes ahead of 2026, driven by the National Health Compact (2025-2030), which aims to standardise medical record retention periods, strengthen accountability and transparency, and introduce new rules for digital health data governance. More broadly, regulators and policymakers have expressed interest in strengthening cybersecurity frameworks, improving online consumer protection, and promoting responsible data governance.

Over the next 18 to 24 months, the PDPO is expected to prioritise: public education and awareness campaigns to improve understanding of rights and obligations; increased compliance monitoring, particularly in high-risk sectors such as telecommunications, banking, fintech, and digital platforms; development of sector-specific guidance and practical compliance resources for businesses; and strengthened collaboration with regional and international partners to share best practices and develop harmonised regulatory standards.

Most Impactful Reform by 2027

Two reforms stand out as most likely to materially improve the effectiveness of Uganda's data protection regime. The first is the development of detailed operational guidance and certification frameworks — including model contractual clauses for cross-border transfers, standard breach response procedures, and baseline cybersecurity requirements which would allow organisations to translate legal principles into structured operational practices and build trust with consumers, regulators, and international partners.

The second, and arguably more fundamental, is an amendment of the DPPA to grant the PDPO the power to award compensatory damages in data protection complaints. The current requirement for data subjects to pursue separate court proceedings to obtain financial redress significantly undermines the accessibility and effectiveness of enforcement. Granting the PDPO compensatory powers, combined with establishing it as an independent corporate body would strengthen both its institutional autonomy and its ability to provide full redress to victims of data protection violations.

DPO
PRIVACY CENTRE
EAST AFRICA

Interested in receiving similar publications direct to your inbox?
Subscribe to our Substack

substack.com/@privacycentreea

Want to contribute an article or have an idea for collaboration?

privacycentreeastafrica@gmail.com