



SEMESTRIAL REPORT - JANUARY 2026

# AFRICA DATA PROTECTION

## REPORT

*Protecting data, empowering Africa*

### UGANDA

Formal notice from the PDPO:  
Google ordered to comply

### NIGERIA

Meta and the nigerian  
commission reach an  
agreement to end their data  
protection dispute

### ANGOLA

Public consultation on the  
draft law on the regulation  
of artificial intelligence



# CONTENTS

## 3 Editorial

### 5 Algeria

Data protection law strengthened by new measures

### 6 Nigeria

Data protection authority launches investigation into nearly 1,300 non-compliant organizations

### 7 Morocco

Dark web: the CNDP deploys a new surveillance system

### 8 Mali

Obstruction of the inspection mission: financial penalty of 5 million CFA Francs

### 9 Egypt

First application of the data protection law: a telecom operator sentenced by a court

### 10 Angola

Security breaches: sanctions imposed on public institutions

### 12 Nigeria

Meta and the Nigerian Commission reach an agreement to end their data protection dispute

### 13 Tanzania

Privacy: the PDPC sanctions the persistence of a data breach

### 14 South Africa

Launch of a platform for reporting data breaches

### 15 Senegal

Deepfakes: the CDP alerts on the dangers of AI and calls for responsible use

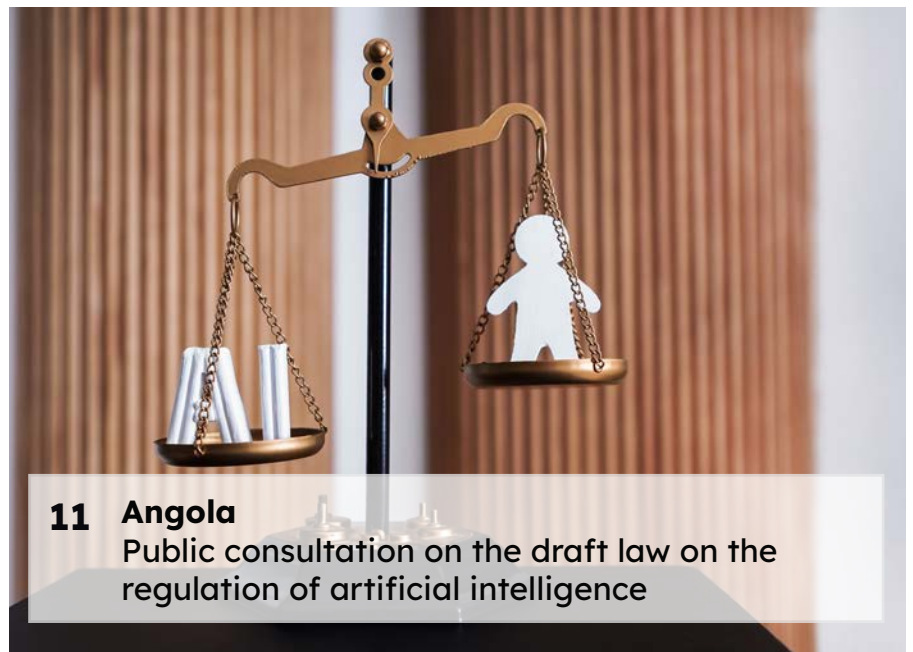
### 16 Kenya

High Court rules on the constitutionality of the data protection authority's powers



### 4 Uganda

Formal notice from the PDPO: Google ordered to comply



### 11 Angola

Public consultation on the draft law on the regulation of artificial intelligence

# EDITORIAL

For Africa, the year 2025 marked a notable acceleration in the momentum surrounding personal data protection and artificial intelligence regulation. With Djibouti and Gambia joining the group of countries with dedicated data protection legislation, more than forty African states now have a legal framework in this area.

This development reflects a growing maturity in addressing the challenges of digital sovereignty, individual freedoms, and citizen security in an interconnected world.

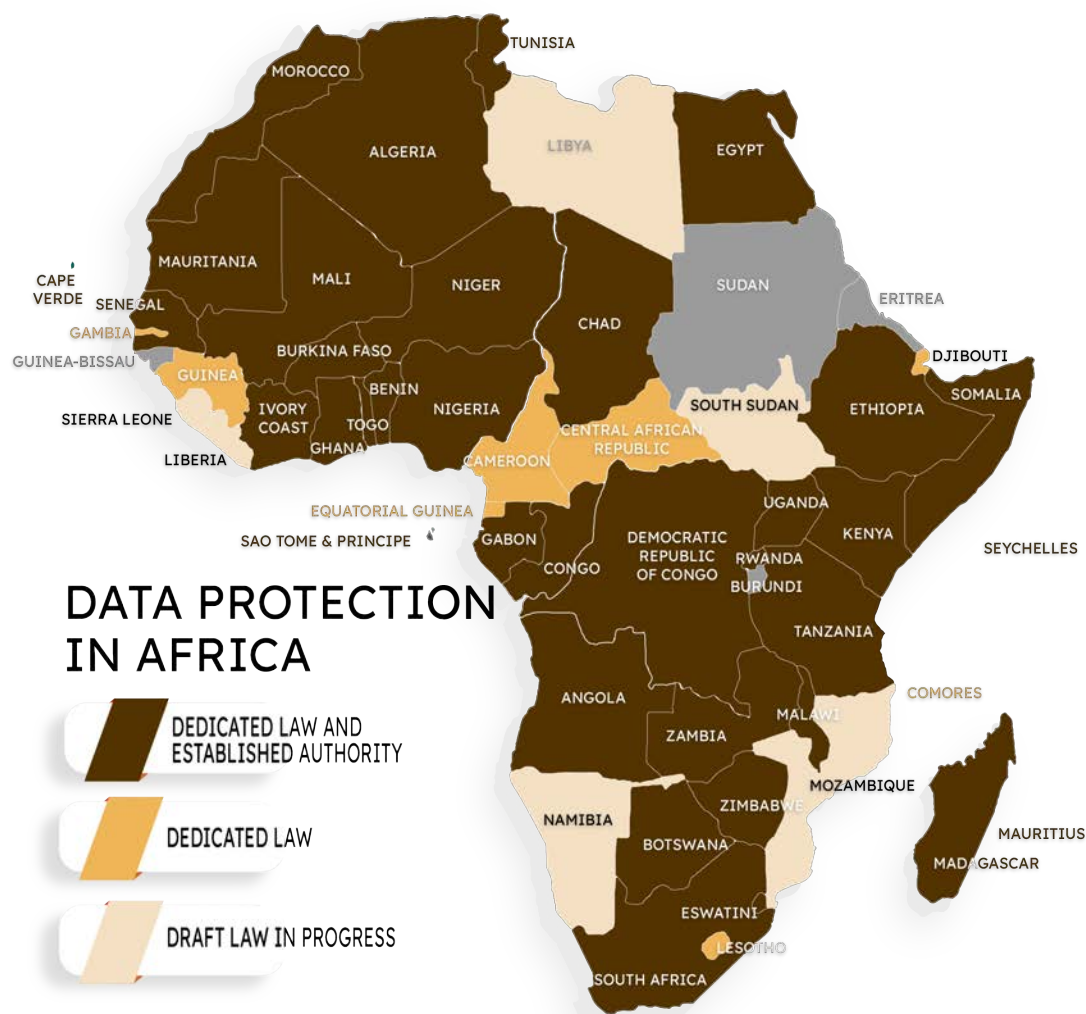
Concerning AI, the year of 2025 saw the continent shift from being a mere spectator to becoming a fully engaged actor. Initiatives such as the Angolan AI bill illustrate the ambition of African states to harness the benefits of this major technological innovation while preventing inherent risks—especially the imposition of extraterritorial standards. Although still limited in number, these initiatives outline the contours of a uniquely African regulatory model that balances socio-economic development goals with the protection of African

values as well as citizens' fundamental freedoms and rights.

Nonetheless, major challenges remain. Ensuring effective enforcement, harmonizing legislation, strengthening local capacities through training, and providing equitable access to technology remain priority areas. In 2025, the continent demonstrated that it can innovate in data and AI governance; the post-2025 challenge will be to translate these advances into tangible opportunities for its populations.



**Jules Hervé YIMEUMI**  
President of  
Africa Data Protection



## UGANDA

## FORMAL NOTICE FROM THE PDPO: GOOGLE ORDERED TO COMPLY

By the editorial team



© ENVATO

The Ugandan data protection authority issued on July 18th 2025 a decision sanctioning GOOGLE LLC for violating the country's Data Protection and Privacy Act . This decision follows a collective complaint filed by four Ugandan citizen who accused the tech giant of failling to comply with local legal obligations. It is based on the Data Protection and Privacy Act, Cap 97, and the Data Protection and Privacy Regulations, which govern the collection, processing and transfer of personal data.

The complainants specifically denounced Google's failure to register with the PDPO, the transfer of their personal data to data providers abroad without prior authorization. They also denounced the inability to contact a local Google representative, leaving them without recourse to address their concerns. In its defense, Google argued that its activi-

ties in Uganda did not fall under local legal obligations due to the absence of a physical presence in the country.

However, the PDPO rejected this argument, noting that Google is a registered taxpayer in Uganda and have substantial revenue from local users. The PDPO considered that economic presence alone was enough to establish the applicability of Ugandan law, even without the company does not have a physical establishment in the country.

The PDPO ordered Google to register within 30 days, to appoint a data controller for Uganda, and to provide evidence of compliance for its cross-border data transfers. Although the PDPO did not impose to know where data is stored, it reminded that any cross-border transfer must strictly comply with the provisions of Ugandan data privacy law.

## ALGERIA

# DATA PROTECTION LAW STRENGTHENED BY NEW MEASURES

By the editorial team

**A**lgeria has adopted a new law amending and supplementing its legal framework for the protection of personal data, following the publication in the Journal Officiel of Law No. 25-11 of July 24th 2025. This text, which updates Law No. 18-07 of 2018, introduces major provisions designed to address new digital and security challenges while strengthening citizens' rights and the obligations of public and private actors.

### Modernized definitions to better regulate emerging technologies

The reform brings essential clarifications to key definitions, now incorporating biometric data, profiling, pseudonymization, and data breaches. These additions reflect the legislator's intention to adapt to evolving technologies and their associated risks, particularly those linked to the growing use of facial recognition or behavioral analysis.

### Institutional strengthening of the national authority

To ensure more effective oversight, the Algerian Data Protection Authority (Autorité nationale de protection des données à caractère personnel - ANPDP) is granted new regional branches responsible for conducting audits and inspections of public and private organizations processing personal data. This decentralization aims to bring the Authority's action closer to the field, improve territorial coverage, and enhance responsiveness in the event of security incidents.

### Increased obligations for data controllers

The law now makes it mandatory for all data controllers and competent authorities to appoint a Data Protection Officer (DPO). The DPO's mission is to inform, advise, and train teams, while also serving as the point of contact with the ANPDP. Courts are exempt from

this requirement when acting in their judicial capacity.

### Mandatory record-keeping and impact assessments

Data controllers must now maintain a detailed register of their processing activities, including the purposes pursued, the categories of data collected, the recipients of the information, and the security measures implemented. An automated log of all operations performed on the data (collection, modification, deletion, etc.) is also required. Furthermore, when a processing operation is likely to present high risks to the rights and freedoms of individuals, the controller must carry out a data protection impact assessment.

These documents must be made available at any time to the ANPDP, thereby strengthening transparency and accountability.

### Regulation of international data transfers

The transfer of data to a third country or an international organization will now be subject to a prior assessment of the level of protection offered by the recipient. In the absence of sufficient safeguards, the transfer may only take place in exceptional circumstances, notably for the protection of vital interests or the prevention of a serious threat to public security. With this reform, Algeria has equipped itself with a more robust legal framework that strengthens citizens' rights and progressively aligns the country with international standards.



## NIGERIA

# DATA PROTECTION AUTHORITY LAUNCHES INVESTIGATION INTO NEARLY 1,300 NON-COMPLIANT ORGANIZATIONS

By the editorial team



© ENVATO

**T**he Nigerian Data Protection Authority (Nigeria Data Protection Commission – NDPC) published, on August 25th 2025, the list of nearly 1,300 organizations targeted by an investigation for non-compliance with data protection regulations. This initiative forms part of the implementation of the Nigeria Data Protection Act (NDPA), adopted in June 2023, which strengthened the NDPC’s investigative and enforcement powers.

These investigations aim to verify that the concerned entities can provide proof of submitting their 2024 compliance audit report, that they have appointed a Data Protection Officer (DPO) whose contact details have been communicated to the NDPC, and that they can present a summary of the technical

and organizational measures implemented to protect personal data. They also seek to ensure that these organizations are duly registered as data controllers or processors of major importance—that is, those whose data volume or sensitivity presents a high risk to the rights of data subjects.

Identified organizations have a period of 21 days to submit all required information. Failing this, they may face sanctions including administrative fines, compliance orders, or, in some cases, criminal prosecution. This large-scale compliance operation reflects the NDPC’s commitment to fostering a culture of compliance and strengthening digital trust in Nigeria.

## MOROCCO

## DARK WEB: THE CNDP DEPLOYS A NEW SURVEILLANCE SYSTEM

By the editorial team



© ENVATO

**T**he Moroccan data protection authority (Commission Nationale de contrôle de la protection des Données à caractère Personnel - CNDP) announced a major step in its efforts against the illicit dissemination of personal data on the dark web. Thanks to a tool developed by a specialized cybersecurity company, the CNDP can now more effectively monitor unauthorized disclosures of sensitive data and take appropriate action.

This tool will enable rapid identification of the concerned data controllers and allow the CNDP to apply the legal provisions, particularly in cases where data processing activities

have not been notified beforehand, as required under Law No. 09-08. Personal data processing operations must be subject to a prior declaration or authorization request to the CNDP, and no processing may be carried out without receipt of an acknowledgment.

The CNDP also plans to strengthen its technological resources with additional tools in the coming months. This evolution reflects its commitment to adapting to growing cybersecurity challenges and ensuring optimal protection of personal data.

## MALI

## OBSTRUCTION OF THE INSPECTION MISSION: FINANCIAL PENALTY OF 5 MILLION CFA FRANCS

By the editorial team

The Malian Data Protection Authority (Autorité de Protection des Données à Caractère Personnel – APDP) has imposed an administrative fine of 5 million CFA francs (approximately 7,500 euros) on a private clinic. The sanction follows the clinic’s obstruction of an inspection mission carried out by the APDP regarding a video surveillance system that had been installed illegally, without prior authorization. The decision is based on Law 2013-015 of May 21st 2013 on the protection of personal data.

### Obstructed inspection, resulting sanction

According to information provided by the APDP, the clinic hindered the authority’s agents by refusing to cooperate during an on-site inspection. Article 65 of Law No. 2013-015 of May 21st 2013, as amended, provides for sanctions ranging from 5 to 20 million CFA francs (approximately 7,500 to 30,000 euros) for any obstruction to the APDP’s activities, including refusal to provide information or documents relevant to the mission, concealment of evidence, or interference with an inspection.

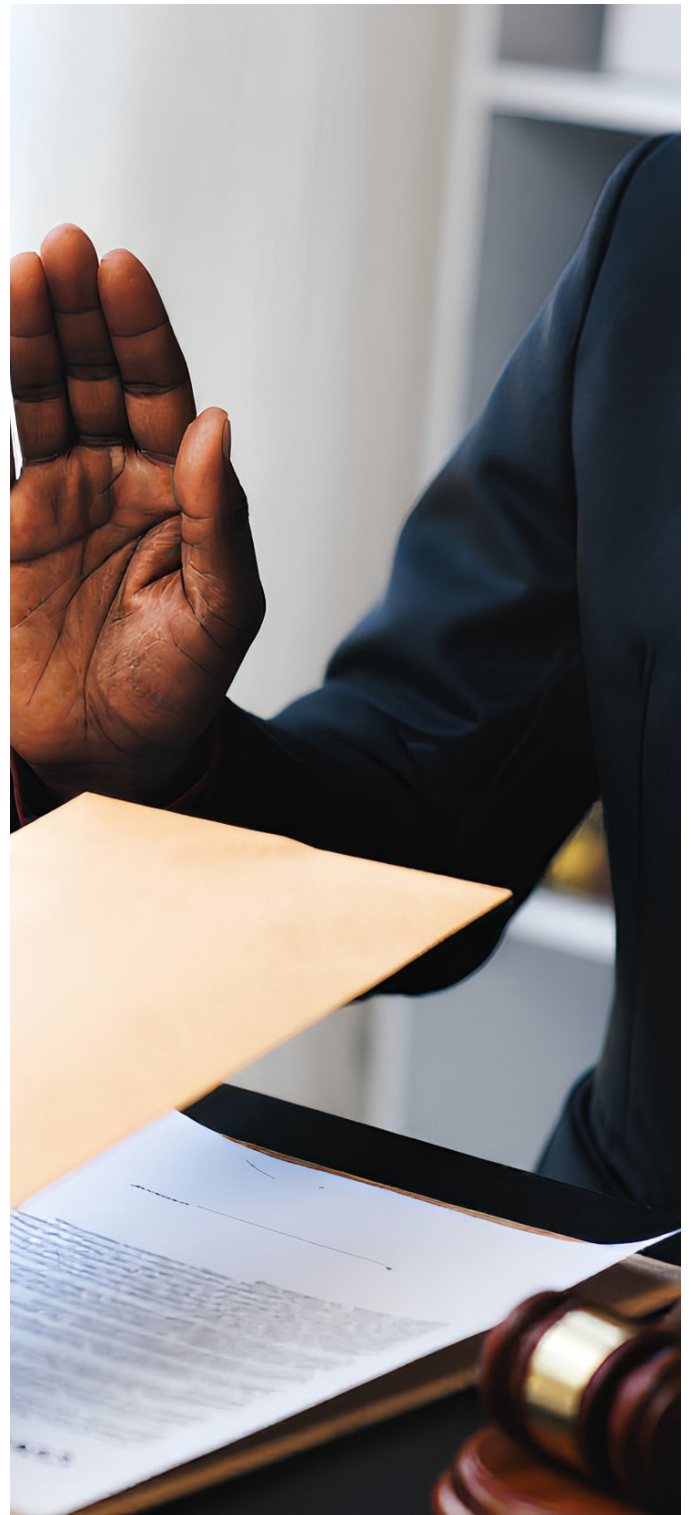
In this case, the clinic was sanctioned for preventing access to a video surveillance system deemed non-compliant with current regulations. The APDP reminds that any installation of surveillance devices in a public or semi-public space must, under penalty of sanctions, be declared and authorized in accordance with personal data protection legislation.

### A warning to public and private institutions

This decision reflects the APDP’s intention to assert its authority and strengthen compliance with personal data protection rules in Mali, particularly in the health sector, where sensitive data processing is common. Institutions, whether public or private, are required to comply with legal obligations governing the

the collection, processing, and retention of data.

The APDP emphasizes that this fine aims to remind all relevant actors of the importance of transparency and cooperation with competent authorities.



## EGYPT

# FIRST APPLICATION OF THE DATA PROTECTION LAW: A TELECOM OPERATOR SENTENCED BY A COURT

By the editorial team

**F**or the first time since the adoption of its 2020 data protection law, an Egyptian court has ordered a telecom operator to pay record compensation for a privacy violation. On 27 May 2025, the Alexandria Court ordered the operator to pay approximately €280,000 to a woman whose personal data was compromised following the fraudulent replacement of her SIM card.

### A landmark ruling

The case dates back to November 2022, when the plaintiff—who was abroad at the time—had her SIM card replaced without her consent. The perpetrators gained access to her WhatsApp account and blackmailed her into dropping a lawsuit she had filed abroad against a real estate company. Despite her requests, the telecom operator refused to provide a copy of her contract, prompting her to take legal action.

The court found the operator liable for failing to meet its legal data protection obligations. The decision relies on several pieces of legislation, including the Personal Data Protection Law (No. 151/2020), the Cybercrime Law (No. 175/2018), and the Consumer Protection Law (No. 181/2018). The court ruled that the operator had failed to secure its customer's data, thereby violating her constitutional right to privacy, guaranteed under Article 57 of the Egyptian Constitution.

### Legal obligations ignored

The court highlighted that the Cybercrime Law requires operators to retain user data for 180 days and protect it from unauthorized access. In this case, the operator failed both to prevent the fraudulent SIM replacement and to provide the necessary evidence to clear itself of responsibility.

As Egypt prepares to finalize the implementing decrees of its data protection law, this ruling marks the beginning of a new era of accountability for digital-sector actors.



## ANGOLA

# SECURITY BREACHES: SANCTIONS IMPOSED ON PUBLIC INSTITUTIONS

By the editorial team

The Angolan Data Protection Authority (Agência de Protecção de Dados – APD) published, on September 22th 2025, two major decisions condemning an airline and a bank to fines for serious breaches of personal data protection legislation. These sanctions, issued under Law No. 22/11 of June 17th, 2011 on the protection of personal data, mark a turning point in the fight against cybersecurity violations and breaches of confidentiality involving sensitive information in Angola.

### The airline: double penalty for negligence

In its decisions No. 001 and No. 002 from September 10th, 2025, the APD imposed two separate fines on the airline. The first, amounting to USD 100,000 (one hundred thousand US dollars), sanctions the failure to implement appropriate technical and organizational measures to protect the personal data of a passenger and their relatives. The company was also fined for processing customer and employee data without prior notification or authorization from the APD, in violation of the obligations set out in Law No. 22/11. The second fine, totaling USD 75,000 (seventy-five thousand US dollars), penalizes the airline's negligence in responding to a ransomware cyberattack that occurred on 15 September 2024, which resulted in the temporary loss, unauthorized access, and unlawful disclosure of sensitive information. The APD recalled that data controllers are required to ensure the security of personal data against any risk of breach or unauthorized access.

### A bank also under scrutiny

During an extraordinary meeting held on 30 April 2025, the APD had already fined a bank USD 75,000 for similar failures. The financial institution was accused of not having deployed the necessary security measures to protect employee data during a ransomware attack that occurred on 10 February 2023.

### Mitigated penalties due to cooperation

Despite the severity of the sanctions, the APD emphasized that the amounts of the fines had been reduced due to the exemplary cooperation of both entities. They actively collaborated with the authority to establish the facts and demonstrated a serious commitment to improving their internal security and compliance processes. Moreover, the absence of prior data protection violations also served as a mitigating factor.

### A strong signal for data protection in Angola

These decisions come in a context of increasing cyberattacks and highlight the urgent need for Angolan businesses and institutions to strengthen their security and compliance systems. They also demonstrate the APD's determination to assert its authority and enforce the law, including against major economic actors.



## ANGOLA

## PUBLIC CONSULTATION ON THE DRAFT LAW ON THE REGULATION OF ARTIFICIAL INTELLIGENCE

By the editorial team



© ENVATO

**I**n September 2025, Angola’s Ministry of Telecommunications, Information Technologies, and Social Communication presented a draft law on artificial intelligence (AI). Developed in a context of rapid digital transformation, the bill aims to establish a comprehensive legal framework regulating the development, use, and oversight of AI in Angola. The goal is twofold: to foster technological innovation while protecting citizens’ fundamental rights in line with the country’s constitutional values.

The proposal is based on Articles 40, 54, 55, and 210 of the Angolan Constitution, guaranteeing freedom of expression, personal data protection, and human dignity. It also aligns

with the African Declaration on AI, signed in Kigali in April 2025, promoting ethical and inclusive AI that supports sustainable development objectives.

The draft contains nine chapters and 86 articles covering general provisions, AI development and promotion, user rights, obligations of developers and providers, and AI governance and oversight.

Across Africa, countries such as Egypt, Kenya, Senegal, and Rwanda have already adopted national AI strategies, but Angola stands out by proposing a bill integrating civil, criminal, and administrative liability mechanisms.

## NIGERIA

# META AND THE NIGERIAN COMMISSION REACH AN AGREEMENT TO END THEIR DATA PROTECTION DISPUTE

By the editorial team

**O**n October 30th, a settlement agreement was reached between META (the parent company of Facebook, Instagram, and WhatsApp) and the Nigerian Data Protection Commission (NDPC), bringing to an end a legal dispute that had opposed the two parties for nearly two years. The agreement was approved on November 3rd, 2025, by the Federal High Court of Nigeria in Abuja.

### A dispute separate from other sanctions

It is important to emphasize that this agreement relates solely to the dispute between Meta and the NDPC and has no connection with the sanction imposed by the Nigerian Federal Competition and Consumer Protection Commission (FCCPC) in July 2024. Indeed, the FCCPC had fined Meta USD 220 million for violations of personal data protection and consumer protection laws arising from the 2021 update of WhatsApp's privacy policy. The two cases, although both related to the regulation of Meta's activities in Nigeria, remain legally and procedurally independent.

### A dispute arising from an in-depth investigation

Everything began in September 2023, when the NDPC launched an investigation into Meta's personal data processing practices in Nigeria.

The findings of this investigation, published in February 2025, were damning: the Commission accused Meta of failing to obtain the explicit consent of Nigerian users for behavioral advertising targeting, of transferring data outside the country without authorization, and of collecting data from non-users through its platforms. Among the measures imposed were a fine of 32.8 million USD, as well as strict obligations such as conducting a data protection impact assessment and updating its privacy policy.

### A compromise with major implications

Rather than continuing with judicial proceedings, both parties chose the path of dialogue. Meta agreed to withdraw its lawsuit and to comply with several requirements, including strengthening transparency in data processing, collaborating with educational institutions, and improving its technical and organizational measures to protect privacy. In return, the NDPC withdrew its initial orders and refrained from enforcing them, while retaining its right to monitor compliance with Nigeria's data protection law.



## TANZANIA

# PRIVACY: THE PDPC SANCTIONS THE PERSISTENCE OF A DATA BREACH

By the editorial team

The Tanzanian Personal Data Protection Commission (PDPC) issued a decision on July 10th, 2025, in favor of a citizen whose photos and videos, published without his consent, continued to circulate on a company's social media networks. This case raises questions about privacy protection in the digital age.

### An emblematic case of privacy violation

An employee of a law firm filed a complaint against a company accused of publishing photos and videos of him, taken in a private context, on its Instagram account between February and April 2023. These images, showing the complainant in an intoxicated state, were published without his authorization and had professional repercussions: he was suspended from his job in August 2024, before being reinstated following an internal investigation that proved the events predated his employment.

### A legal debate on the retroactivity of the law

The Personal Data Protection Act (Cap. 44), which came into force on May 1st, 2023, protects the personal data of Tanzanians. However, the actions the company was accused of dated back to a period before this date. The PDPC had to rule on a crucial point: can a company be penalized for acts committed before the law was adopted?

In its decision, the PDPC recalled that the law does not apply retroactively, but that the persistence of a violation after its entry into force falls within its scope. It thus invoked the principle of continuous violation: although the initial publications took place before May 2023, their maintenance online after the law came into effect constitutes a persistent infringement of the complainant's privacy. It therefore considered the complaint admissible and that the company had to answer for its

actions.

A welcomed decision, but persistent limitations

The PDPC ordered the company to:

- Immediately delete all photos and videos of the complainant from its online platforms;
- Pay financial compensation of 20 million Tanzanian shillings (approximately 7500€) for moral damages.

This decision marks an advancement in personal data protection in Tanzania, but it also reveals the challenges posed by the retroactive application of laws. For experts, it sends a strong signal to companies: privacy protection cannot be ignored, even for old facts, if their consequences persist.

### A call for collective vigilance

The PDPC emphasized that this case was just one example of abusive practices in bars and entertainment venues, where customers are filmed or photographed without their knowledge. A collective awareness is essential, both for professionals and the general public.



## SOUTH AFRICA

# LAUNCH OF A PLATFORM FOR REPORTING DATA BREACHES

By the editorial team

The South African data protection authority (Information Regulator) has launched an online platform dedicated to reporting data breaches. This initiative, announced in a statement published on April 7th, 2025, aims to modernize and simplify the process of declaring personal data breaches. From now on, all public and private organizations are required to use the eServices portal to report any data breach, marking the end of the previous email-based reporting system. This reform reflects a commitment to enhancing transparency, traceability, and efficiency in the management of personal data breaches, in line with the requirements of the Protection of Personal Information Act (POPIA).

### A legal obligation for data controllers

POPIA requires data controllers to immediately notify the Information Regulator in the event of unauthorized access, loss, or unlawful disclosure of personal data. Until now, such notifications could be submitted by email, but as of April 1st, 2025, exclusive use of the eServices portal has become mandatory for all breach notifications. This platform, accessible through the authority's official website, enables organizations to report incidents in a structured and secure manner. In addition to notifying the authority, organizations must also inform the individuals affected by the breach, unless their identities cannot be determined.

### Enhanced support to facilitate the transition

To ensure smooth implementation of this new system, the Information Regulator has published a practical guide detailing the registration process for the portal, the submission of incident reports, and best practices for notification.

The authority has also set up dedicated support channels to assist data controllers in

their procedures. These tools aim to support organizations in achieving compliance and to ensure consistent application of POPIA throughout the country.

### A major advancement for data protection

The introduction of this new platform constitutes a significant step in strengthening South Africa's data protection framework. By centralizing breach notifications, the Information Regulator aims to improve the monitoring and detection of data breaches, analyze cybersecurity trends, and reinforce the protection of individuals' rights as well as the prevention of future incidents. This centralization will foster better coordination between organizations and the authority, enabling a faster, more coherent, and more effective response to personal data compromises.



## SENEGAL

# DEEPFAKES: THE CDP ALERTS ON THE DANGERS OF ARTIFICIAL INTELLIGENCE AND CALLS FOR RESPONSIBLE USE

By the editorial team

In a statement published in October 2025, the Senegalese Data Protection Authority (Commission de Protection des Données Personnelles – CDP) expressed deep concerns over the proliferation on social media of videos and images generated by artificial intelligence (AI). These pieces of content, often intended to manipulate public opinion or harm the reputation of public figures, religious leaders, or ordinary citizens, represent, according to the CDP, a serious threat to human dignity and social cohesion. The authority emphasizes that such practices may lead to criminal and administrative sanctions, as they severely infringe upon fundamental rights, particularly the right to privacy and the protection of personal data.

### Deepfakes and unlawful data collection: multiple risks for citizens

Among the dangers highlighted by the CDP are the large-scale collection and exploitation of personal data without consent, as well as the risks of identity theft, information manipulation, and irreversible reputational damage. The rise of deepfakes—hyper-realistic but falsified and deceptive AI-generated content—heightens these risks by blurring the line between reality and fiction and undermining trust within society. According to the CDP, if these technological drifts remain unregulated, they could weaken social cohesion by fostering manipulation and the widespread dissemination of false information.

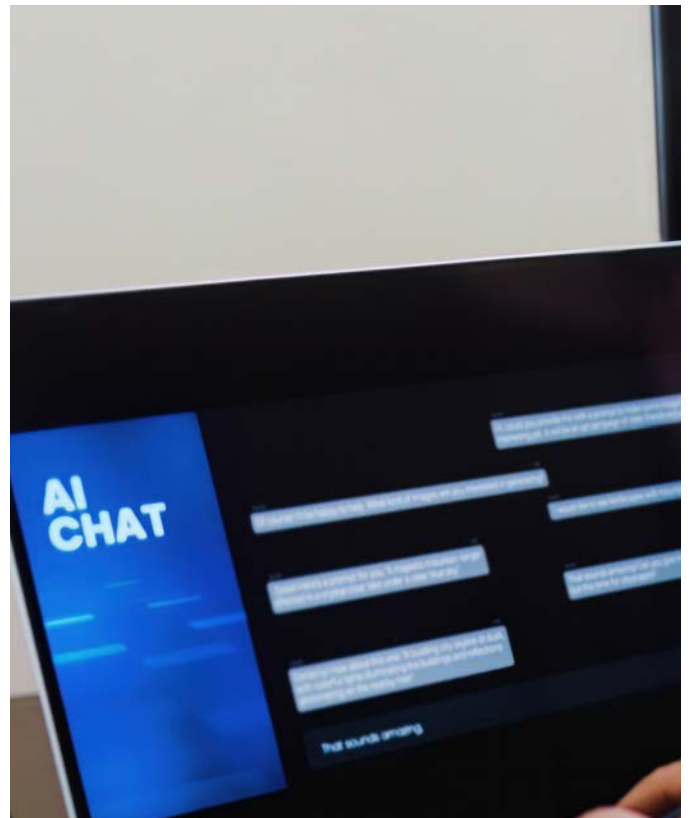
### Call for ethical and responsible use of artificial intelligence

In response to these challenges, the CDP calls for ethical, responsible, and transparent use of AI tools. It urges citizens to exercise heightened vigilance before sharing AI-generated content by verifying its authenticity and

encouraged to avoid any manipulation that could undermine the religious, cultural, or personal values of others. Digital platforms must also strengthen their detection and reporting mechanisms for illegal, misleading, or harmful content in order to limit its dissemination and impact.

### The CDP reaffirms its regulatory and awareness-raising role

In its statement, the CDP reaffirms its commitment to enforcing Law No. 2008-12 of 25 January 2008 on personal data protection and reminds the public that it will continue its awareness-raising efforts among individuals, institutions, and businesses. The authority also intends to adapt its regulatory framework to meet the new challenges posed by generative AI, ensuring a balance between technological innovation, respect for privacy, and the preservation of Senegalese social and cultural values.



## KENYA

## HIGH COURT RULES ON THE CONSTITUTIONALITY OF THE DATA PROTECTION AUTHORITY'S POWERS

By **Arnaud NADINGA**, Doctor of private law

**D**ata protection authorities are an essential component of the mechanism for protecting individuals with respect to the processing of personal data. Entrusted with giving full effect to the dedicated legislation, the choice of their status is crucial: they must have all necessary legal means and provide the required guarantees of competence, independence, and impartiality. As genuine regulatory authorities, they differ from other administrative bodies in the absence of hierarchical subordination or ministerial oversight, without, however, being elevated to the status of courts. This hybrid position is essential. In addition to ensuring impartiality and independence from the executive, it has the dual merit of preserving the integrity of judicial competences by avoiding encroachment and preventing the reproduction of judicial delays in a field that requires great speed. This status has materialised through the model of the independent administrative or public authority, a model that has prevailed despite debate regarding its legitimacy, particularly concerning its compatibility with the strict separation of the judicial and executive powers.

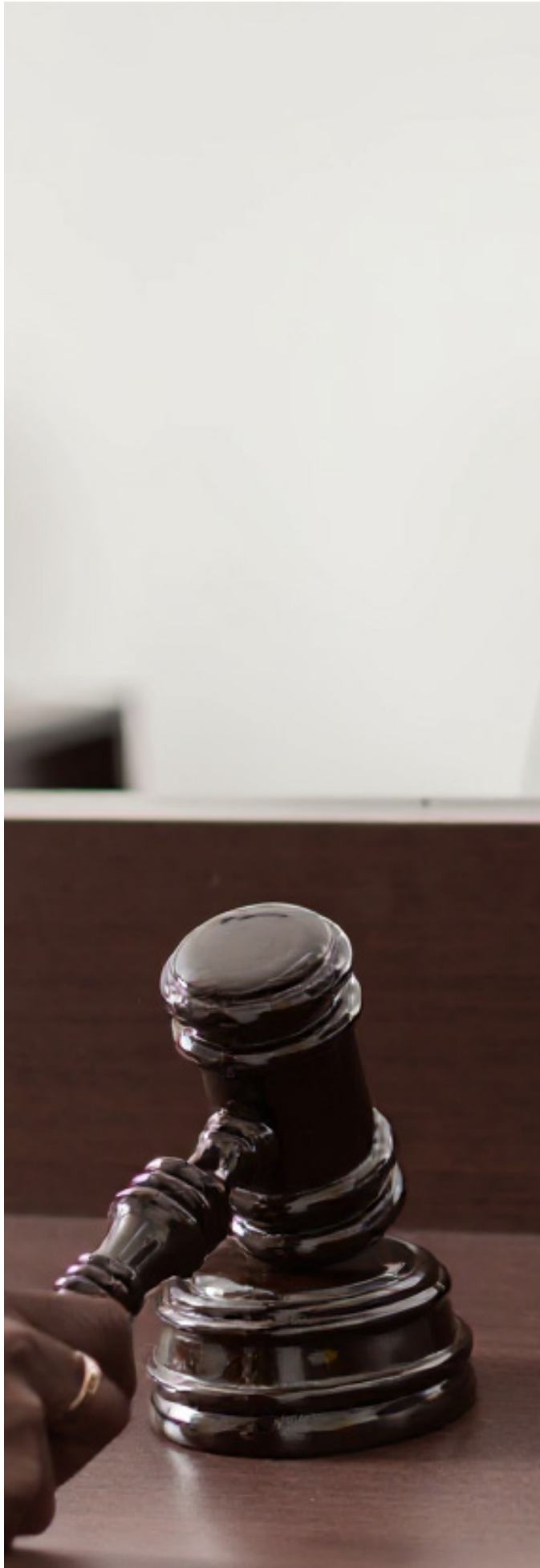
It is precisely this tension surrounding the legitimacy of Kenya's data protection authority (Office of the Data Protection Commissioner – ODPC) that the Constitutional and Human Rights Division of the High Court of Kenya in Milimani had to resolve on 12 August 2025. In Petition No. E010 of February 2nd, 2025, the Court was asked, on the one hand, to declare unconstitutional Section 56 of the Data Protection Act (DPA) and Regulation 14(5) of the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021. Two grounds were advanced in support of this claim. The petitioner first argued that only the High Court is authorised, under Articles 23(1) and 165(3)(b) of the Constitution, to determine matters relating to violations of

the Bill of Rights and to order remedies for breaches of privacy. Granting the ODPC the power to resolve disputes relating to privacy would therefore encroach on the High Court's jurisdiction. Secondly, according to the petitioner, allowing the ODPC to issue binding and enforceable decisions—including corrective measures and compensation—would violate the principle of separation of powers. On the other hand, the Court was invited to declare that the mandate of the ODPC overlaps with that of the Kenya National Human Rights and Equality Commission (KNHREC), which is expressly empowered under Article 59 of the Constitution to investigate human rights violations.

In response, the ODPC, the first respondent, argued that it is a specialised statutory body created to give effect to the fundamental right to privacy, particularly by overseeing the processing of personal data. Moreover, its functions and powers arising under Sections 5, 8(1)(f), 56, 58 and 65 of the DPA—allowing it to receive and process complaints, issue decisions, and deliver enforcement notices—are administrative and quasi-judicial in nature, but not judicial. Furthermore, under Section 64 of the DPA, its decisions are subject to review by the High Court through appeal, thereby ensuring their constitutional conformity. The model is not unprecedented, as similar configurations exist for regulatory authorities in the communications and competition sectors.

The Attorney General, the second respondent, aligned himself with this position, noting that the ODPC's functions are also justified by the principles of exhaustion of remedies and constitutional avoidance. The interested party, the Data Privacy and Governance Society of Kenya, emphasised the ODPC's technical legitimacy due to its expertise, as well as the need for specialised and accessible redress mechanisms in the field of data protection.

## KENYA



The question before the High Court thus concerned the constitutionality of the ODPC's powers in protecting the right to privacy, with the underlying tension relating to the constitutional principle of separation of powers. In its judgment, the High Court concluded that the legal framework provided by the DPA, as currently formulated, is sufficiently constitutional, functional, and necessary to effectively guarantee the right to privacy (para. 60). The ODPC model was therefore upheld, with the Court considering its quasi-judicial powers constitutional, as they are those of a specialised body whose decisions remain subject to judicial oversight. This decision legitimises the ODPC's powers (I) and clarifies its position within Kenya's constitutional architecture (II).

### **I – Confirmation of the legitimacy of the ODPC's Powers**

The Court recognised that the powers of the data protection authority correspond to those of an administrative authority with quasi-judicial functions (A), whose mission is justified by its technical expertise (B).

#### **A – An administrative authority with quasi-judicial powers**

The High Court first rejected the argument that the ODPC encroaches on its exclusive jurisdiction. It held that the ODPC “is rather an important and constitutionally compliant mechanism for the implementation of the right to privacy [...], subject to the supervisory jurisdiction of the High Court as preserved under Section 64 of the DPA” (para. 25). Although Article 23(1) of the Constitution grants the High Court the power to adjudicate violations of the Bill of Rights, this does not mean that every dispute involving a fundamental right must necessarily be initiated before it. The fact that ODPC decisions may be appealed to the High Court ensures respect for its jurisdiction. The existence of the ODPC merely offers administrative remedies to give effect to the fundamental right, alongside the judicial review mechanism provided in Section 64 of the DPA, which guarantees the High Court's supremacy. Moreover, the ODPC does

## KENYA

not issue final determinations of violations of privacy, and its decisions are not “judgments.” It acts rather as a regulator or quasi-judicial body playing a complementary role within the broader constitutional framework. Sections 56 of the DPA and 14(5) of the Regulations “do not confer judicial power on the ODPC but authorise administrative and regulatory functions pursuant to Article 31 of the Constitution. [They] provide the necessary powers for a specialised agency while maintaining judicial safeguards through appellate oversight by the High Court” (paras. 26 ff.). The Court stressed that even though the ODPC is empowered to issue binding decisions, a binding decision does not necessarily imply the exercise of judicial power: the determining criterion is the conclusive interpretation and application of the Constitution (para. 35). The ODPC’s powers do not meet this threshold. They are investigative and regulatory, aimed at ensuring compliance with the DPA. Its decisions are not “judgments” in the strict sense but administrative acts. Moreover, although the ODPC may prescribe corrective measures and order compensation for complainants, such measures are not declarations of rights within the meaning of Article 23(3)(a) of the Constitution, but administrative actions provided for by statute and subject to appeal. This right of appeal preserves constitutional oversight and ensures judicial supremacy.

The judgment also draws on South African case law concerning the Information Regulator established under the Protection of Personal Information Act (POPIA), emphasising that a specialised administrative body may hold quasi-judicial powers subject to judicial review without violating separation of powers. Finally, the ODPC’s powers align with Article 159(2)(c) of the Constitution, which, in pursuit of the constitutional objective of swift and accessible justice, encourages alternative dispute resolution mechanisms, including statutory bodies with quasi-judicial mandates. It should be noted, however, that the power granted to the ODPC to award compensation for individual harm is not found in all systems; it is often reserved to courts, particularly in Francophone countries, where data protection



## KENYA



authorities act in the interest of the law and may impose only administrative sanctions.

### **B – An administrative Authority with specialised expertise**

The Court emphasised the need for specialised institutions with the technical expertise required to handle disputes of a particular nature. The ODPC’s legitimacy stems primarily from its effectiveness and its ability to act where traditional structures are less suited. The Court adopted the argument, raised by the interested party, that the complexity of personal data disputes justifies the involvement of a body with highly specialised technical knowledge. It recalled the case of *Rich Productions Ltd v Kenya Pipeline Co.* [2014] eKLR, which held that “The reason why the Constitution and the law establish different institutions and different mechanisms for dispute resolution in various sectors is to ensure that disputes that may arise are resolved by those with the technical expertise and competence to handle them.” The involvement of the specialised authority ensures, in addition to technical skill, the avoidance of procedural delays in areas requiring speed (Section 56(5) of the DPA requires the ODPC to resolve complaints within 90 days).

### **II – Defining the role of the ODPC within the constitutional framework**

The Court then focused on defining the ODPC’s institutional position, showing that its powers are framed by judicial oversight (A) and coherently aligned with other human rights bodies (B).

#### **A – Powers framed by judicial oversight**

The central argument supporting the constitutionality of the model is the availability of an appeal against ODPC decisions, as provided in Section 64 of the DPA. For the Court, the ODPC’s mission is justified as long as it operates under High Court supervision. The right of appeal preserves judicial control and guarantees the supremacy of the judiciary. Judicial oversight is also reinforced by the

## KENYA

principles of “exhaustion of remedies” and “constitutional avoidance.” The exhaustion principle, grounded in Article 159(2)(c) of the Constitution and Section 9(2) of the Fair Administrative Action Act (FAAA), requires courts to refrain from hearing disputes unless the prescribed administrative procedures have been followed (para. 40). In other words, a person cannot seek judicial review until the available statutory mechanisms have been exhausted, except where the court grants an exemption in exceptional circumstances (ineffective remedies, bias, or manifest injustice). This principle ensures ordered dispute resolution and allows specialised bodies to exercise their mandates. Thus, the ODPC must be seized before any court action in data protection matters.

The principle of “constitutional avoidance” implies that the High Court should only address a constitutional issue if the dispute cannot be resolved by other means. This articulation, consistent with the *Kirimi & Another v Mobi Changa Ltd (2023)* jurisprudence, highlights the complementarity between administrative redress and judicial review. It is nonetheless noteworthy that the application of these principles within a constitutional petition is somewhat surprising.

### **B – A Competence complementary to other human rights institutions**

For the petitioner, since Article 59(2)(e) of the Constitution already establishes the KNHREC and grants it the power to investigate complaints of human rights violations, the ODPC’s mandate would overlap or conflict with that Commission’s powers. Adopting the respondents’ and interested party’s position, the Court acknowledged that the ODPC is a specialised authority with a specific mandate to oversee compliance with data protection legislation adopted under Article 31(c) and (d) of the Constitution, whereas the KNHREC has a broader human rights oversight function. Furthermore, under Article 21(3) of the Constitution, which obliges all State entities to address the needs of vulnerable groups and develop frameworks that enhance the realisation of rights, the creation of the ODPC



## KENYA

ava is not only constitutional but necessary to provide a targeted and expert enforcement mechanism for data protection. The mandates of the two commissions are therefore complementary rather than conflicting. Although both institutions may incidentally deal with the same fundamental right, their functions do not conflict: the KNHREC operates as a constitutional body responsible for general oversight, advocacy, and investigations into human rights violations, while the ODPC is a specialised statutory regulator ensuring technical oversight of data protection and digital privacy issues.

The Court noted that jurisprudence has long acknowledged that implementing the right to privacy requires both general and sectoral enforcement institutions, and that an adequate framework must include specialised oversight to address increasingly complex issues surrounding data governance, including the collection, storage, and use of personal information. It added that the Constitution itself allows for functional decentralisation and delegation. Article 186(2) and the Fourth Schedule envisage the sharing of responsibilities between institutions at different levels of government and across different bodies. Therefore, functional overlap alone is not unconstitutional unless it produces legal contradiction or institutional paralysis. The petitioner showed no evidence of direct conflict between the ODPC and the KNHREC, nor any case of a complaint being handled simultaneously or inconsistently by both bodies. “Accordingly, the [High] Court finds that the mandate of the ODPC does not unlawfully conflict or overlap with that of the KNHREC. On the contrary, the two institutions are designed to complement each other within Kenya’s constitutional and statutory framework for human rights enforcement” (para. 58). The existence of the ODPC “does not detract from the authority or mandate of the KNHREC but provides a necessary, expert, and targeted avenue for addressing privacy-related complaints in a rapidly evolving digital environment” (para. 59).

### Conclusion



## KENYA



This decision should reassure data protection authorities regarding the legitimacy of their powers. The main lesson is that the model of an independent administrative authority equipped with regulatory and sanctioning powers is not inherently contrary to the principle of separation of powers. Its legitimacy stems from the fact that—with guarantees of competence, independence, and impartiality—it gives concrete effect to a fundamental right (the right to privacy) in the technical and complex field of data protection, while remaining subject to high-level judicial oversight. This Kenyan jurisprudence is part of a broader African trend toward recognising regulatory authorities endowed with specialised and quasi-judicial competence, such as South Africa’s Information Regulator, and strengthens the institutional framework for data protection on the continent. It also resolves another crucial issue: the relationship between data protection authorities and National Human Rights Commissions, a situation faced by many African States. The clarification of the complementarity of their mandates helps prevent jurisdictional conflicts and fosters a protection ecosystem in which each institution has a defined role.



**[WWW.AFRICADATAPROTECTION.ORG](http://WWW.AFRICADATAPROTECTION.ORG)**

**[INFO@AFRICADATAPROTECTION.ORG](mailto:INFO@AFRICADATAPROTECTION.ORG)**

**© COPYRIGHT JANUARY 2026 - AFRICA DATA PROTECTION - ALL RIGHTS RESERVED**