# AFRICA PRIVACY REPORT 2023/2024

A Review of Policy Trends and Digital Frontiers in the Data Protection Landscape

www.lawyershub.org

LAWYERS HUB
Tech for Justice

# Table of Content

# AFRICA PRIVACY REPORT 2023/2024

A Review of Policy Trends and Digital Frontiers in Africa's Data Protection Landscape

A LAWYERS HUB PUBLICATION

Published by Lawyers Hub
1st Ngong Avenue, Nairobi
ACK Garden House-Block D, 6th Floor
Email: info@lawyershub.ke
Tel: +254 784 840 228 /+254 111 215 675
www.lawyershub.org

Published in January 2023

Editorial Team: Linda Bonyo, Jorge Clarke, Risper Onyango, Dickson Ogugu
Design and Layout by: Michael Ogutu

# EXECUTIVE SUMMARY

This report encapsulates the outcomes of research endeavors conducted by the Lawyers Hub, focusing on the dynamic landscape of privacy and data protection in Africa throughout the year 2023. Beyond presenting findings, the report serves as a resource, unraveling trends and significant milestones that contribute to shaping the continent's approach to data protection. The exploration of these insights aims not only to inform but also to foster the implementation of robust data protection measures and encourage active stakeholder participation in this pivotal domain.
The report presents the following critical findings into key areas that shaped digital governance and protection of personal information in the continent in 2023:

a. **The Malabo Convention attained enforcement status; 6 additional countries enacted Data Protection Legislations/approved Data Protection Bills.**

The **Malabo Convention achieved ratification** by Mauritania, Côte d'Ivoire, and the Central African Republic, marking its official enforcement on June 8, 2023. Adopted on June 27, 2014, this marked a significant milestone, making it the sole binding regional treaty on data protection outside of Europe, after a nine-year journey. The Convention has been ratified by 15 countries, and 12 countries have signed the convention out of the 55 African countries.

During the same period, five countries, namely **Tanzania, Nigeria, Algeria,** and **Mauritius**, successfully **enacted data protection laws.** This progress was also visible in Malawi and Seychelles which laid the foundation for the development of a comprehensive data protection Bill.

b. **Mauritius and Nigeria operationalised their Data Protection Offices as several jurisdictions such as Kenya and Senegal pursued robust activities towards ensuring compliance with data protection laws in their countries.**

Among the countries mentioned above as having recently enacted data protection laws, **Mauritius** and **Nigeria** have since **established Data Protection Offices.** The Mauritius Data Protection Office operates as a public office under the Ministry of Technology, Communication, and Innovation. On the other hand, Nigeria's Data Protection Commission functions as an independent body. Prior to it, data protection compliance in Nigeria was supervised by the Nigeria Data Protection Bureau (NDPB), which was under the jurisdiction of the National Information Technology Development Agency (NITDA). The NDPB was tasked with overseeing the implementation of the Nigeria Data Protection Regulation (NDPR), a subsidiary legislation of the NITDA Act, 2007 (now replaced by the Nigeria Data Protection Act). Needless to say, the approach to the discourse on the independence and impartiality of data protection authorities in Africa varies significantly among different countries.

Additionally, the commitment to robust compliance mechanisms and the resolution of privacy concerns was evident across the continent. Kenya, for instance, expanded its reach by **establishing regional offices in Mombasa and Nakuru, enhancing accessibility to compliance services and data**

**protection awareness creation.** Furthermore, **Kenya launched its Data Protection Registration System** to streamline regulatory processes.

Meanwhile, **Senegal** took proactive measures by **issuing guidance on the processing of biometric data in the workplace** and **unveiling a National Data Strategy.**
These initiatives collectively reflect the dynamic efforts undertaken by African nations to fortify data protection frameworks and address emerging privacy challenges.

**c. In 2023, there were over 6 significant data privacy fines issued by Data Protection Authorities in 6 different African countries**

Compared to preceding years, the continent experienced a notable surge in enforcement actions targeting privacy violations, as indicated by the actions taken by data protection authorities in various jurisdictions.

**Kenya** emerged as a **frontrunner,** with over **six significant determinations** impacting institutions spanning the lending sector, education, entertainment, digital identity, and digital currencies. Despite issuing the highest number of penalties, the **combined monetary value of fines in Kenya** (approximately USD $. 124,700) was **still less than individual fines imposed in South Africa** (USD $. 279,000), **Nigeria** (USD $. 218,459), and **Angola** (USD $ 150,000).

**Nigeria**'s data protection authority imposed fines on Nigerian banks, telecommunications firms and digital lending institutions, albeit without individual names disclosed, for infringements related to data privacy.

**South Africa**'s Information Regulator (IR) **issued the only reported penalty to a public body in the region** - an infringement notice that imposed a ZAR 5 million (USD 279,000) fine on the Department of Justice and Constitutional Development (DoJ&CD) for violations of the Protection of Personal Information Act (POPIA).[1] The breaches primarily involved the Department's failure to renew licenses for critical cybersecurity components, including anti-virus, security information and event management (SIEM), and intrusion detection solutions. In a separate incident, the Information Regulator also issued an enforcement notice to Dis-Chem for POPIA violations stemming from a data breach experienced by one of its vendors on September 6.[2]

**Angola**'s National Data Protection Authority fined Africell $150 000 for failing to get prior authorisation from the NDPA when they processed their customers' personal data[3]

**d. There was heightened monitoring of Online Digital Lenders and their Data Practices across the continent**

Regulators in various jurisdictions within the region were diligent in overseeing the activities of online digital lenders throughout 2023. Kenya, Nigeria, Ghana, and Uganda all saw their regulators release lists of approved and unapproved digital lenders, indicating those licensed or prohibited from operating within each country.

1 Li, R. (2023) South African government fined for data breach, ALB. Available at: https://www.africanlawbusiness.com/news/19143-south-african-government-fined-for-data-breach (Accessed: 23 January 2024).
2 Ahmore Burger-Smidt. "Enforcement Notice Issued to Dis-Chem Due to Contravention of POPIA." Werksmans Attorneys, September 18, 2023. https://www.werksmans.com/legal-updates-and-opinions/enforcement-notice-issued-to-dis-chem-due-to-contravention-of-popia.
3 Sheik, S. (2023) Data Protection Fines in Africa, Michalsons.com. Available at: https://www.michalsons.com/blog/data-protection-fines-in-africa/64822 (Accessed: 23 January 2024).

Kenya, taking a cautious stance, **approved the least number of digital lenders (32 out of over 400 applications**).

**Nigeria had 154 approved digital lenders** with 40 under conditional approval, **Uganda reported 2,132 licensed money lending businesses**, and **Ghana published a list of 97 digital money lenders barred from operating** without proper regulatory licensing.

**e. In comparison to previous years, there was more engagement across jurisdictions in the adoption and regulation of Artificial Intelligence; however, such adoption remained limited to countries such as Kenya, South Africa, Nigeria and Egypt.**

Several African nations recognized the potential offered by AI; however, **the widespread adoption of AI in Africa remains limited, with only a few exceptions such as South Africa, Nigeria, Ethiopia, Kenya, Zimbabwe, Togo, Libya, and Ghana actively embracing AI.** Numerous African countries still face challenges related to essential requirements for technology adoption, including infrastructure, data ecosystems, STEM education, and governance frameworks. Despite these obstacles, notable progress is underway in adopting digital solutions.

Several **countries have existing legal frameworks which offer potential avenues for incorporating AI elements such as the enactment of data protection laws across 36 countries.**

Countries such as **Senegal** have in the past **introduced National Data Strategies**: **Rwanda is the latest to have an official National AI Policy,** however, the rapid advancement of this technology continues to outpace the scope of most of these laws.[4]

**f. With the growing digitisation across the region, 2023 witnessed an increase in cyberattacks and incidents across multiple countries such as Nigeria, South Africa and Kenya, with targeted attacks on critical infrastructure, financial institutions, governments, and businesses.**

The global cybersecurity trends revealed a significant increase in cyberattacks, particularly ransomware attacks, with 66% of companies worldwide reporting such incidents, up from 51% in 2020, according to a survey by Sophos.[5] Kaspersky ICS CERT reported that attacks were detected on 32% of Industrial Control System (ICS) computers in Africa.

Drawing from extensive research, this report finds a **concerning trend of escalating cyber threats.** The documented average of 1158 weekly cyber attacks across various sectors serves as a testament to the persistent challenges faced by organizations in safeguarding digital assets.

Africa **witnessed a substantial 12% YoY increase in the average number of weekly attacks per organization, reaching an average of 1900 attacks.**[6] Cyberattacks across African countries targeted critical infrastructure, financial institutions, governments, and businesses.[7] The financial sector was the most targeted, with 18% of cyberattacks, followed by telecommunications (13%), government agencies (12%), trade (12%), and industrial sectors (10%).[8]

On a positive note, **2023 marked the implementation of the Malabo Convention, –the only cyberse-**

4 Siele, M.K.N. (2023) *Kenya's tech industry is fighting AI regulation plans*, *Semafor*. Available at: https://www.semafor.com/article/12/05/2023/kenya-ai-regulation (Accessed: 22 January 2024).
5 2023 Ransomware Report: Sophos State of Ransomware"123 https://www.sophos.com/en-us/content/state-of-ransomware
6 Ibid
7 Sun Evo Technologies (2023) *Africa: 2023 Cyberthreats Landscape, next year predictions*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/africa-2023-cyberthreats-landscape-next-0waue/?trk=article-ssr-frontend-pulse_more-articles_related-content-card (Accessed: 22 January 2024).
8 Ibid

**curity convention in the world that combines cybersecurity, cyber crime, electronic transactions, and data protection in a single legal instrument.** Its activation holds considerable importance in the fight against cybercrime and the enhancement of cybersecurity. Notably, it would help establish dual criminality and simplify the categorization of cybercrimes across jurisdictions, facilitating the generation of evidence.

African nations have the opportunity to utilize the Malabo Convention for fostering the creation of mutual legal assistance treaties (MLATs). These agreements would facilitate the exchange of information on cyber incidents and establish continuous information-sharing mechanisms or networks among member states. Such initiatives aim to streamline the process from incident reporting to the prosecution of cyber crimes.[9]

9 CEIP (2023) *Continental Cyber Security Policymaking: Implications of the Entry Into Force of the Malabo Convention for Digital Financial Systems in Africa*, *carnegieendowment.org*. Available at: https://carnegieendowment.org/2023/07/10/continental-cyber-security-policymaking-implications-of-entry-into-force-of-malabo-convention-for-digital-financial-systems-in-africa-event-8146 (Accessed: 22 January 2024).

# INTRODUCTION

As we navigate through the digital age, privacy has become a fundamental human right that is often threatened by the very technologies that promise progress and convenience. In Africa, this issue takes on added layers of complexity due to factors such as varied socio-economic conditions, diverse cultural norms, and a rapidly evolving digital landscape.

In an increasingly interconnected world, the importance of privacy cannot be overstated. This report aims to provide an overview of the current state of privacy in Africa, a continent of rich diversity and rapid digital transformation.

The research is structured and elucidated through five central themes, each offering a nuanced perspective to the intricacies of Africa's privacy landscape. These themes delve into various aspects of privacy, encompassing individual rights, data protection, governmental policies, and corporate practices.

Chapter one provides an overview of data protection in Africa, encompassing recent trends, a comprehensive examination of the continent's advancements, the enactment and review of legislation, and the activities undertaken by data protection authorities.

Chapter two explores emerging practices and trends related to data protection and privacy in the continent, such as Artificial Intelligence, cybersecurity (including incidents and risks associated with digital democratic processes), data practices in lending, privacy considerations in the age of big tech and innovation, and user data protection.

The report concludes by highlighting the unique challenges and opportunities confronting Africa in the development of data protection policies, actions, and trends within the privacy ecosystem in the year 2023. Additionally, it examines privacy predictions and policy developments in select African countries, providing a succinct summary of the continent's commitment to privacy and its accomplishments over time.

Evidently, the "Africa Privacy Report 2024" serves as a good resource for stakeholders seeking an understanding of the complex and dynamic privacy landscape in Africa. Its findings and analyses contribute to ongoing discussions on cybersecurity, regulatory compliance, and the broader implications of emerging technologies on privacy rights across the continent.

# CHAPTER ONE

**Overview of Data Protection in Africa**

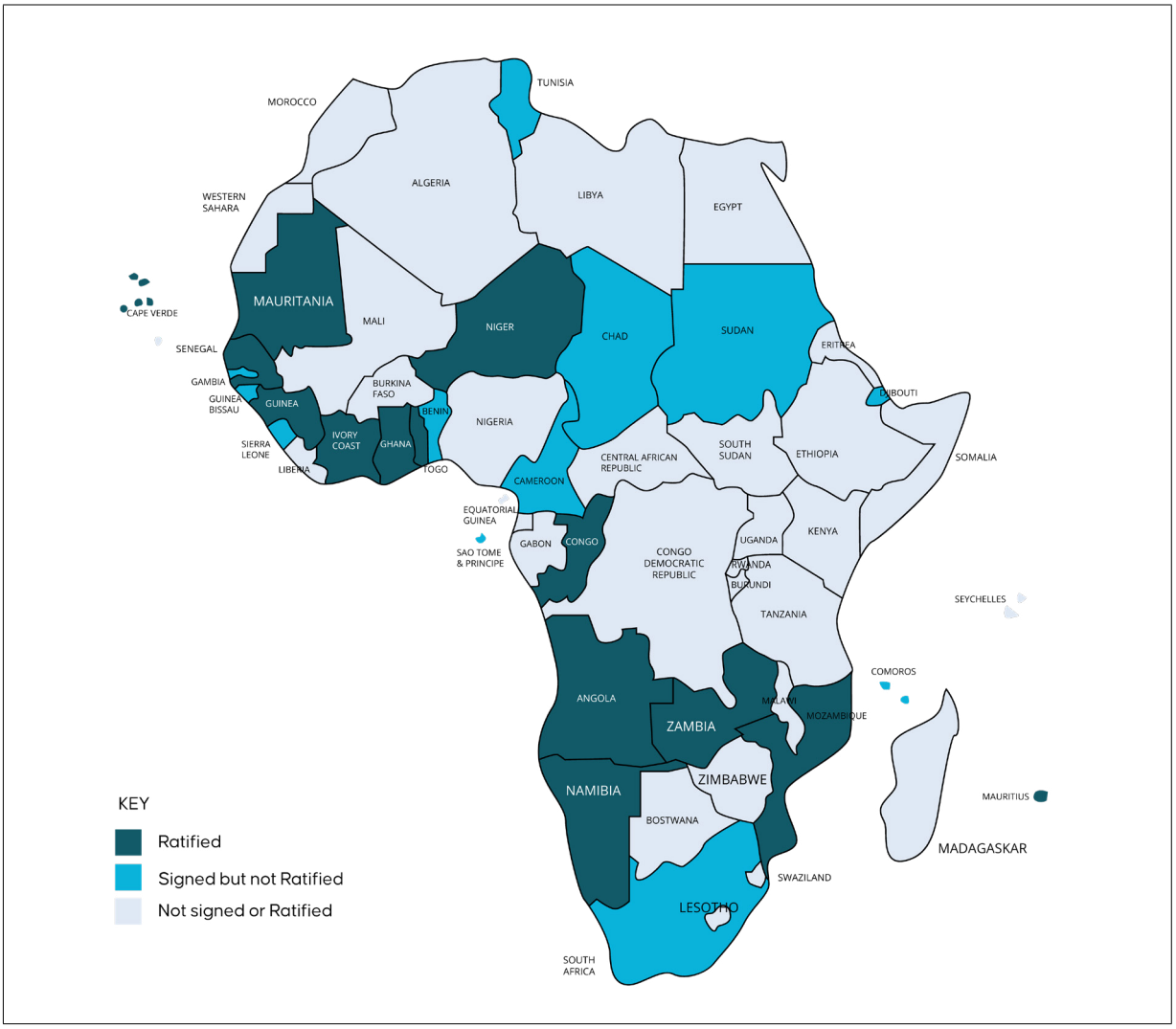
In the digital age, data protection has emerged as a critical issue worldwide, and Africa is no exception. Data protection in Africa is a multifaceted issue, influenced by a variety of factors including legal frameworks, technological advancements, and socio-cultural norms. Despite the challenges, many African nations have made significant strides in establishing data protection laws and regulations. These efforts are often driven by the need to balance the benefits of digital innovation with the imperative to protect individuals' privacy rights. However, the implementation and enforcement of these laws vary widely across the continent, influenced by factors such as resource constraints, varying levels of digital literacy, and differing cultural attitudes towards privacy.

The landscape of data protection in the year 2023 witnessed dynamic shifts and transformative trends, reflective of the continuous evolution of digital ecosystems and heightened awareness surrounding privacy issues. The year unfolded against a backdrop of increased regulatory scrutiny, technological advancements, and growing public concern for safeguarding personal information. As nations grappled with the intricate balance between fostering innovation and protecting individual privacy rights, emerging themes in data protection encompassed legislative developments, enhanced cybersecurity measures, the rising influence of artificial intelligence, and a renewed focus on user consent and transparency.

The **Malabo Convention achieved ratification** by Mauritania, Côte d'Ivoire, and the Central African Republic, marking its official enforcement on June 8, 2023. Adopted on June 27, 2014, this marked a significant milestone, making it the sole binding regional treaty on data protection outside of Europe, after a nine-year journey. The Convention has been ratified by 15 countries, and 12 countries have signed the convention out of the 55 African countries.

In 2023, the Convention was ratified by three countries: Mauritania (May 9), Côte d'Ivoire (April 3) and the Central African Republic (July 19). Additionally, it was signed by Sudan (March 15), South Africa (February 16), and Djibouti (May 12).

The Map below shows the list of countries that have signed and those that have ratified the convention as of the date of this Report;




**Countries that enacted Data Protection Laws in 2023**

In 2023, Africa witnessed advancements in the legislation and regulation of Data Protection and privacy. Five countries enacted their own data protection laws, bringing the total to 36 out of 54 countries with such laws. The countries that enacted their data protection laws in 2023 include:

## NIGERIA

On June 12, 2023, President Bola Ahmed Tinubu signed the Nigeria Data Protection Act, 2023 into law. This law replaced the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019, providing a new legal framework for personal data regulation in Nigeria.

The key change was the establishment of the Nigeria Data Protection Commission (NDPC) and its Governing Council. The Commission oversees the Act's implementation, enforcing rules and regulations while regulating the processing of personal information. The Council provides overall policy direction for the NDPC.

The Act's main goals include safeguarding data subjects' rights, regulating personal data processing, promoting best practices for data security and privacy, and providing recourse for breaches. It also ensures data controllers and processors meet their obligations and contributes to Nigeria's digital economy while participating in global economies through trusted use of personal data.

## TANZANIA

On 1 May 2023, the Personal Data Protection Act 11 of 2022 came into effect in Tanzania, marking a significant step forward for data protection in the country. The Act establishes minimum requirements for the collection and processing of personal information to safeguard the right to privacy. It defines offenses related to the unauthorized disclosure, destruction, deletion, concealment, or alteration of personal information, imposing penalties on individuals, organizations, and officers found guilty of these offenses. Tanzania also enacted the Personal Data Collection and Processing Regulations, G.N No. 349 of 2023 (Data Collection Regulations) and the Complaint Handling and Breach of Personal Data Regulations, G.N No. 350 of 2023 (Complaint Handling Regulations) collectively referred to as the Regulations. Effective from May 12, 2023, these Regulations, operating under the authority of the Minister of Information, Communication, and Information Technology, oversee aspects such as data collection and processing, as well as procedures for filing complaints under the Personal Data Protection Act 2022 (Act). Currently, the ACT and the Regulations are available only in Kiswahili.

## ALGERIA

Law No. 18-07, came into effect on August 10, 2023. It establishes, among other things, fundamental requirements for general personal data protection, encompassing elements such as explicit consent, data processing notifications, data subject rights, and constraints on direct marketing and data transfers. Notably, this law introduces significant penalties, potentially including imprisonment for a period ranging from two to five years.

**Countries that have draft Data Protection legislation**

In 2023, Africa witnessed 3 countries presenting their draft data protection legislations in their respective parliaments and cabinets for enactment. We anticipate that in 2024, these laws will be officially enacted. They include:

## MALAWI

On **7 December 2023**, the **Data Protection Bill 2023 was introduced in the Malawi Parliament**. The Bill establishes several data processing principles including lawful processing, purpose limitation, data minimisation and accuracy and storage limitation. Furthermore, the Bill establishes data subjects certain rights such as the right to access personal data, the right to data portability, the right to rectification of personal data, the right to erasure of personal data, the right to restriction of processing personal data, right to object.

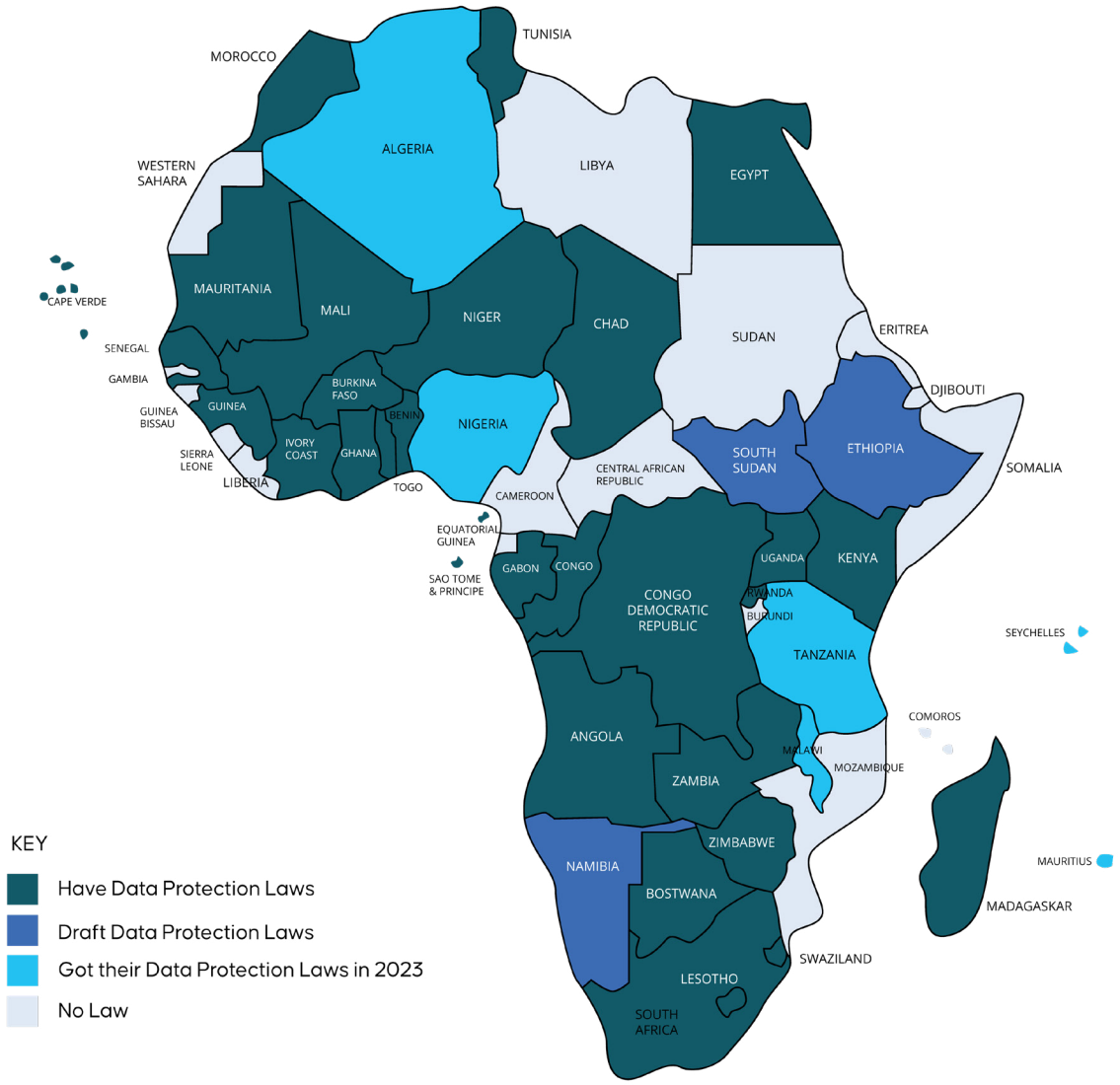
## SEYCHELLES

In Seychelles, the **Data Protection Bill** was introduced and **obtained Cabinet approval on September 7, 2023.** The Cabinet of Seychelles had approved the Data Protection Bill, 2023, on June 22, 2023. This bill, initially introduced on March 16, 2023, by the Department of Information Communications Technology, is specifically designed to replace the existing Data Protection Act of 2003.

## GAMBIA

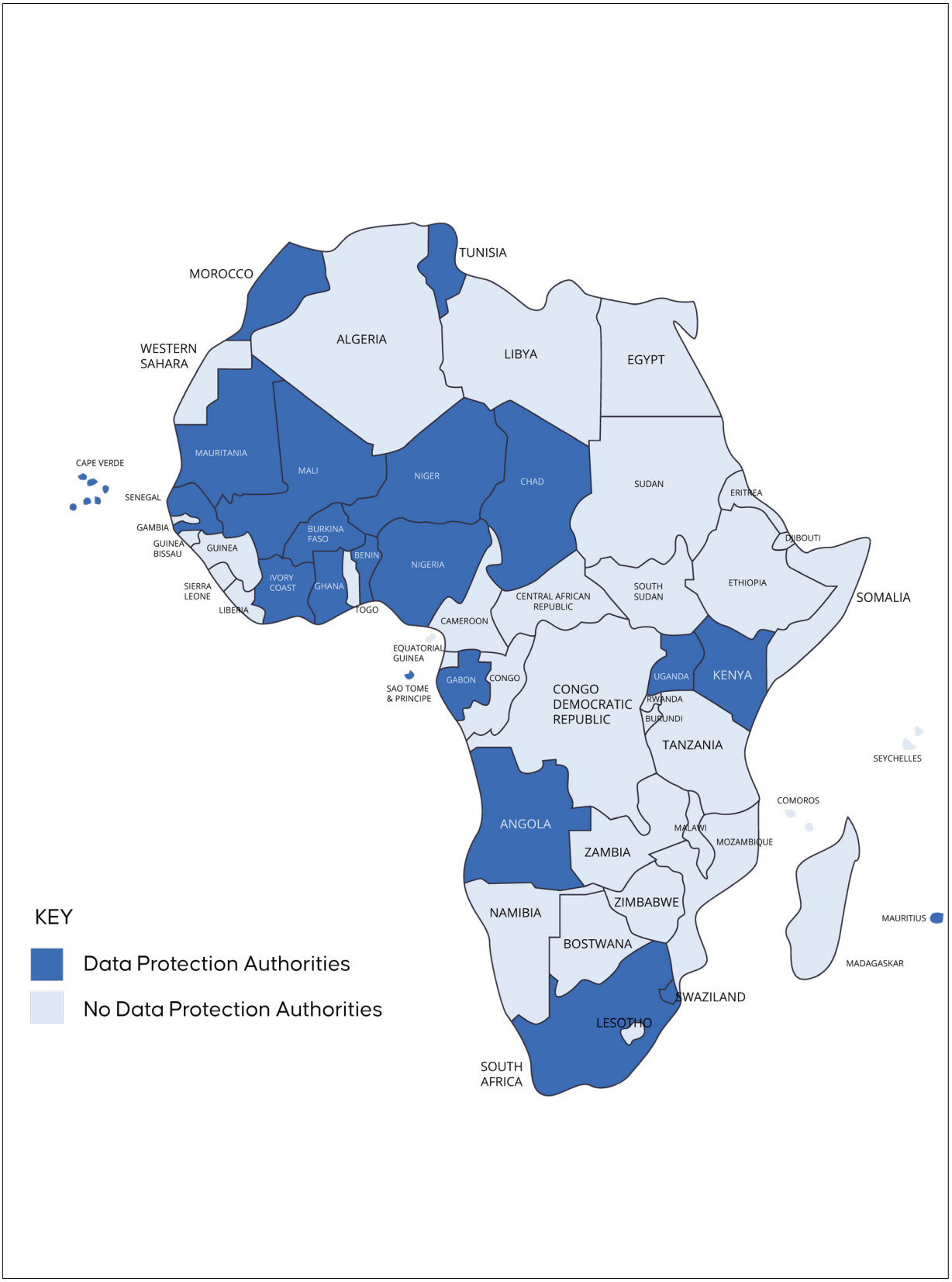
The Gambia Data Protection Bill was finalized in December 2020 with the support of the Council of Europe and the European Union. The bill is currently awaiting approval by the National Assembly. The bill was presented to the cabinet in 2023. Hopefully, before the end of 2024, it will be tabled before the National Assembly, and the nation will have its law by the end of the year, 2024.

## Data Protection Laws in Africa



**Data Protection Authorities in Africa**

There are presently 21 Data Protection Authorities, who are members of the Network of African Data Protection Authorities (NADPA/RAPDP) established in 2016.



**Data Protection Fines and Penalties issued in 2023**

The following are decisions and penalties for privacy violations emanating from these authorities across the region.

| Country | | Fines/Penalty Notice |
|---|---|---|
|  | South Africa | South Africa's Information Regulator (IR) issued an infringement notice imposing a ZAR 5 million (USD 279,000) fine on the country's Department of Justice and Constitutional Development (DoJ&CD) for breaches of the Protection of Personal Information Act (POPIA). Contraventions include a failure to renew the licenses for its anti-virus, security information and event management (SIEM), and intrusion detection solutions, thereby leaving its technology infrastructure vulnerable to attack.[10]<br><br>Regulator issued an enforcement notice to Dis-Chem for POPIA violations following a vendor's data breach on September 6. |
|  | Ghana | The Data Protection Commissioner issued a Press Release, a public warning addressing online apps breaching privacy rights for individuals. |
|  | Nigeria | Nigerian banks and institutions were fined over N200 million ((USD $. 218,459) for data privacy violations, particularly violating the data privacy of Nigerian citizens.[11] |
|  | Angola | The National Data Protection Authority fined Africell $150 000 for failing to get prior authorisation from the NDPA when they processed their customers' personal data.[12] |
|  | Côte d'Ivoire | On November 8, 2023, the Telecommunications/ICT Regulatory Authority of Côte d'Ivoire (ARTCI) announced that it had published, on August 23, 2023, its decision No. 2023-0937, in which it issued a warning to Yango CIV LLC and formal notice for violations of the Law 2013-450 on the Protection of Personal Data (the Law). The orders included: a warning for illicit recordings of conversations of passengers on the YANGO app; a formal notice to deactivate the YANGO app without delay and, until further notice, the option to record telephone conversations on it; a warning for non-compliance with data protection obligations; blocking and immediate deletion of customer audio recording data; and designate the correspondent for data protection in the company, within seven days of receipt of the decision.[13] |

10 Li, R. (2023) *South African government fined for data breach*, *ALB*. Available at: https://www.africanlawbusiness.com/news/19143-south-african-government-fined-for-data-breach (Accessed: 23 January 2024).

11 *Nigerian Banks and Institutions fined over N200 million for Data Privacy Violations* (2023) *Techpoint Africa*. Available at: https://techpoint.africa/2023/06/20/nigerian-banks-fined-200-million-data-privacy-violations/ (Accessed: 22 January 2024).

12 Sheik, S. (2023) *Data Protection Fines in Africa*, *Michalsons.com*. Available at: https://www.michalsons.com/blog/data-protection-fines-in-africa/64822#:~:text=In%20January%202023%2C%20the%20NDPA,on%20BPC's%20special%20media%20pages. (Accessed: 23 January 2024).

13 DataGuidance (2023) *Ivory Coast: ARTCI issues formal warning and orders deactivation of Yango app* , *dataguidance.com*. Available at: https://www.dataguidance.com/news/ivory-coast-artci-issues-formal-warning-and-orders (Accessed: 25 January 2024).

| | | |
|---|---|---|
|  | Kenya | A Penalty Notice issued against Whitepath Company Limited & Regus Kenya for failure to comply with an ODPC's enforcement notice while Regus Kenya was non-cooperative and failed to Respond to a notification of a complaint and an enforcement notice.<br><br>An Enforcement Notice issued against Ecological Industries Limited on April 17, 2023 due to non-cooperation with several notifications of a complaint against them for publishing a personal photo on a company catalog and calendar for marketing purposes.<br><br>The ODPC made a determination regarding WorldCoin's operations within the country. Holding Tools for Humanity Corporation (TFH) and Tools of Humanity GmBH, the entities behind WorldCoin in Kenya, responsible for breaching Kenya's Data Protection Act and its associated regulations. The ODPC also expressed concern about WorldCoin's failure to submit a Data Protection Impact Assessment (DPIA). Furthermore, the ODPC scrutinized the transfer of personal data by WorldCoin and TFH outside Kenya in relation to Data Protection Act regulations. The office concluded that the transfer of sensitive personal data of Kenyan data subjects out of Kenya was unlawful due to invalid consent. Additionally, TFH and Worldcoin failed to obtain confirmation of appropriate safeguards from the ODPC, as required by Section 49(1) of the Act, for the transfer of sensitive personal data out of Kenya.<br><br>The ODPC issued three penalty notices. Roma School was fined $30,774 (KeS 4.55 Million) for posting a minor's image without parental consent, while Casa Vera received a $12,512 penalty (KeS 1.85 Million) for sharing a customer's image on their social media platform without the person's consent. Mulla Pride Ltd., the operator of KeCredit and Faircash mobile lending apps, was fined $20,128 (Ksh.2.975.000). They were found to have used names and contact information from third parties to send threatening messages and make phone calls to complainants. |

**A case study of notable cases on privacy and data protection in Kenya**

***Kenya***

*In 2023, the Kenyan case of **Ondieki v Maeda (E153 of 2022)**,[14] a significant legal issue concerning the right to privacy under Article 31 of the Kenyan constitution was addressed. The petitioner contended that the respondent's installation of CCTV cameras in the petitioner's compound, capturing his residence, constituted a violation of his and his family's privacy rights under Article 31 and the Data Protection Act. The petitioner argued that the CCTV cameras were set up without his consent or prior notice, with the intention of spying, monitoring, and recording images of his property. The central question before the court was whether the respondent's actions had infringed upon the petitioner's right to privacy as guaranteed by Article 31 of the Constitution.*

*The court ruled that the respondent, as a data controller under the Act, must adhere to its provisions to safeguard the privacy rights of the petitioner and other neighbors. The court emphasized that the respondent had an obligation to be registered with the Data Commissioner and to demonstrate that explicit and unequivocal consent had been obtained from the petitioner, as consent cannot be assumed under the Act. Despite acknowledging the respondent's legitimate reasons for installing the CCTV camera, the court found that the process should have been conducted in an organized manner, either through consent or through the management of the properties, especially given the proximity of the two parties as neighbors.*

*In conclusion, the court determined that the respondent had breached the petitioner's right to privacy, underscoring the importance of respecting privacy rights even when pursuing legitimate interests such as security through surveillance measures.*

*In the case of **Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another (Interested Parties)**[15], where the court was called upon to determine 'whether the Office of the Data Protection Commission (ODPC) acted in excess of its jurisdiction by rendering a decision on a complaint outside the 90-day timeframe set by section 56(5) of the Data Protection Act,' the court agreed with the applicants that pursuant to the provisions of section 56(5) of the Act,[16] the ODPC had a time-bound jurisdiction to investigate and determine the complaint.*

*When the 90 days' period ended, the respondent jurisdiction also came to an end by way of effluxion of time; "The moment the 90 days ended, the respondents' jurisdiction also lapsed. The finding that was rendered outside time was without jurisdiction and therefore a nullity, bereft of any force of law."*

14 Ondieki v Maeda (Petition E153 of 2022) [2023] KEHC 18290 (KLR) (Constitutional and Human Rights) (31 May 2023) (Judgment).
15 Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another (Interested Parties) (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR) (Judicial Review) (12 May 2023) (Judgment)
16 A complaint made to the Data Commissioner shall be investigated and concluded within ninety days, section 56(5) of the Data protection Act.

# CHAPTER TWO

**Privacy and Data Protection Developments in 2023**

This chapter explores emerging practices, trends and developments related to data protection and privacy in the continent, such as and including Artificial Intelligence, cybersecurity (including incidents and risks associated with digital democratic processes), data practices in lending, privacy considerations in the age of big tech and innovation, and user data protection.

## A. Privacy and AI

### i. Global AI Governance Trends

The adoption of Artificial Intelligence (AI) by both businesses and individuals is rapidly gaining momentum, marked by the emergence of new platforms like ChatGPT, each appearing to enhance existing market offerings.

Globally, the year 2023 was a landmark year for artificial intelligence (AI), marked by the rise of generative AI models such as Google Bard, OpenAI ChatGPT, DALL-E 3, and Midjourney. Significant strides were made in AI regulation, with the European Union's AI Act leading the way, and AI-related summits like the Hiroshima G7, Global Partnership AI Summit, and the Whitehouse Executive Order on AI gaining prominence.

The year also saw the release of several proposed ways of governing AI, including the G7's International Guiding Principles for Advanced AI Systems and International Code of Conduct for Organizations Developing Advanced AI Systems, as well as the Bletchley Declaration that emerged from the UK AI Safety Summit.

### ii. Continental AI Governance Trends

At continental level, although more African countries are recognizing the potential of AI in improving decision-making, social and economic well-being, there remain critical challenges in embracing AI. In terms of infrastructure, urban hubs across Africa are undergoing swift digitalization, yet numerous rural areas grapple with intermittent internet connectivity and power shortages. While there is a burgeoning enthusiasm for technology among the human capital, specialized training in AI-driven methodologies is essential and remains lacking. Overcoming financial constraints presents a challenge, requiring innovative funding models and strategic partnerships. Additionally, many countries lack robust policies and legislation on digitalization.[17]

Encouragingly, collaborations with tech industry leaders and international organizations are starting to address some of these gaps, and **the emergence of institutions dedicated to AI research is becoming more prevalent across the continent.**

The African Union (AU) has demonstrated active engagement in AI governance. The AU High-Level Panel on Emerging Technologies (APET) and the African Union Development Agency (AUDA-NEPAD) convened AI experts in Kigali, Rwanda, from February 27 to March 3, 2023, to finalize the **African Union**

17 Chinganya , O. (2023) The future of AI in statistics in Africa: Is The continent ready?, ISI. Available at: https://www.isi-web.org/article/future-ai-statistics-africa-continent-ready (Accessed: 22 January 2024).

**Artificial Intelligence (AU-AI) Continental Strategy for Africa** which seeks to position Africa at the forefront of harnessing artificial intelligence for socioeconomic development ethically and inclusively. The Strategy is projected to contribute a staggering $15.7 trillion to global GDP by 2030, aiming to significantly impact the attainment of Agenda 2063 and the Sustainable Development Goals (SDGs) by stimulating economic growth, driving innovation, generating employment opportunities, supporting education, and improving public service delivery.[18] The Strategy also addresses the technological, ethical, economic, security, and social perspectives of AI and establishes the context and defining guiding principles, vision, mission, pillars, and strategic objectives of the Continental AI Strategy.[19]

At the national scale, numerous countries are acknowledging the possibilities presented by AI. Nevertheless, the **adoption of AI in Africa remains restricted, with only a handful of exceptions such as South Africa, Nigeria, Ethiopia, Kenya, Zimbabwe, Togo, Libya,** and **Ghana actively embracing AI**.[20] Several African nations continue to grapple with fundamental prerequisites for technology adoption, including infrastructure, data ecosystems, STEM education, and governance frameworks.[21] Despite these challenges, notable strides are being made to adopt these digital solutions.

In AI policy development, countries that include Ethiopia, Ghana, Morocco, Rwanda, South Africa, Tunisia, and Uganda, took steps to formulate AI policies, while other countries adopted a piecemeal approach to governance by creating task forces or research labs.[22] Many countries have existing legal frameworks which offer potential avenues for incorporating AI elements, but the rapid advancement of this technology has outpaced the scope of these laws.[23]

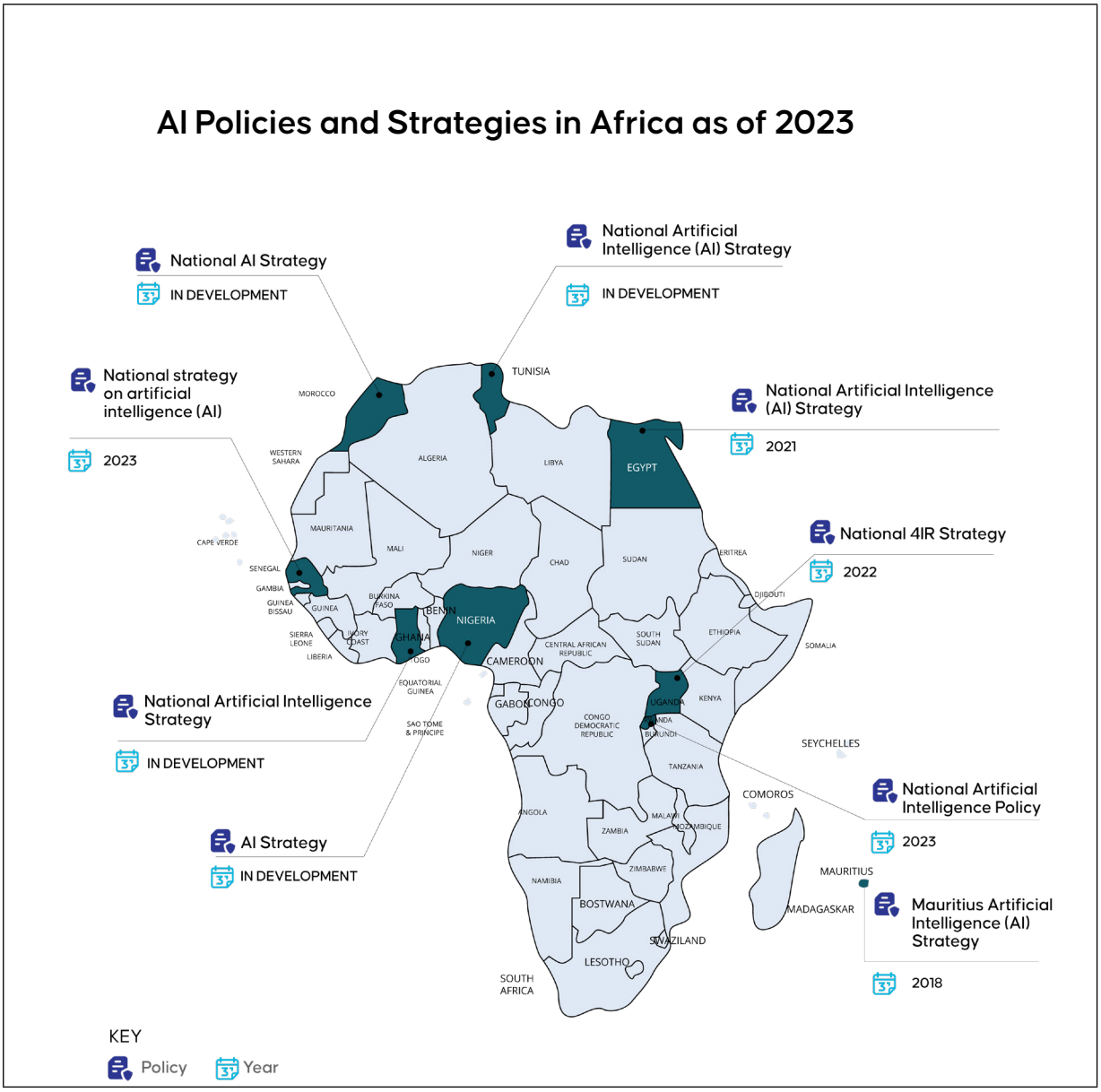
**Senegal** developed its National AI Strategy between June and July 2023, aiming to position itself as an AI leader in West Africa. In Rwanda, the Cabinet approved the National AI Policy on April 20, 2023, outlining a comprehensive plan to leverage AI's transformative potential in key sectors such as healthcare, agriculture, public services, education, finance, and smart cities.
**Egypt** made notable advancements by introducing the Egyptian Charter for Responsible AI. This initiative combines insights with actionable measures to facilitate the responsible development, deployment, management, and utilization of AI systems.

**Kenya** saw legislative action with the introduction of the "Kenya Robotics and Artificial Intelligence Society Bill, 2023" in Parliament seeking the formulation of a regulatory framework on AI. Inversely, Kenya's tech sector is opposed to the new bill aimed at regulating artificial intelligence (AI) in the country, arguing that it would stifle innovation and put off investors.[24] The country also introduced resources such as the Guide for AI Practitioners and reported a significant rise in AI-related searches in Kenya, with a surge of 270% in 2023 compared to the previous year (Google).

The **total number of published AI strategies has seen a decline in 2023** compared to previous years.[25] 2023 marked the most diverse collection of new or upcoming AI strategies to date. Half of the AI strategies that were published or announced come from low and lower middle income countries with Rwanda becoming the first country within the low income bracket to publish an AI Strategy. Similarly,

18 African Union Development Agency (AUDA-NEPAD). (2023). "Fifth Ordinary Session of the Specialized Technical Committee on Communication and Information Communications Technology (STC-CICT-5) of the African Union." https://au.int/en/5thstccict
19 African Union High-Level Panel on Emerging Technologies (APET). (2023). "Continental Strategy on AI." https://au.int/en/5thstccict
20 Chinganya , O. (2023) *The future of AI in statistics in Africa: Is The continent ready?*, *ISI*. Available at: https://www.isi-web.org/article/future-ai-statistics-africa-continent-ready (Accessed: 22 January 2024).
21 Ibid
22 Abuya, K. (2023) *Scaling the impact of AI in Africa*, *TechCabal*. Available at: https://techcabal.com/2023/08/08/scaling-the-impact-of-ai-in-africa/ (Accessed: 22 January 2024).
23 Siele, M.K.N. (2023) *Kenya's tech industry is fighting AI regulation plans*, *Semafor*. Available at: https://www.semafor.com/article/12/05/2023/kenya-ai-regulation (Accessed: 22 January 2024).
24 Ibid
25 Our income group classification is based on the World Bank's Group country classifications by income level for 2023-2024

lower middle income countries in Africa, including Senegal and Benin, have published AI Strategies this year, while Ethiopia is set to release theirs.




**Nigeria** launched a new AI research scheme in October. The scheme is expected to give a total of $290,000 in grants to 45 AI-focused startups and researchers and is designed to identify applications of AI in key sectors including agriculture, education, healthcare, finance and governance.[26] In **South Africa**, the South African Artificial Intelligence Association (SAAIA) was launched in July 2023 in partnership with the Tshwane University of Technology (TUT), aiming to promote responsible AI adoption and showcase South African AI innovation.

### iii. Privacy in AI Adoption and Use in Africa 2023

In light of policy advancements, the most significant milestone in 2023 for data protection and AI adoption was **the implementation of the Malabo Convention**. This Convention serves as a crucial instrument for regulating aspects of AI, particularly the automated processing of personal data. How-

26 Siele, M.K.N. (2023) *Kenya's tech industry is fighting AI regulation plans*, *Semafor*. Available at: https://www.semafor.com/article/12/05/2023/kenya-ai-regulation (Accessed: 22 January 2024).

ever, to effectively regulate AI in Africa, it remains essential to enact relevant national laws in the 18 African countries that currently lack data protection legislation.[27] Furthermore, Blueprint regulations addressing use of personal data by different AI technologies (such as facial recognition) are yet to be developed and disseminated for consideration at national government level in most jurisdictions.[28] The most active countries in the African region that are leading in AI development, such as Egypt, Kenya, South Africa, for example, have enacted data protection laws in place.

There were **several direct references to AI in a 2023 amendment to the Gabon law on personal data protection** (Loi N° 025/2023 portant modification de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel). This includes definitions for AI-related terms such as artificial intelligence, profiling, facial recognition, and natural language processing.[29] Conversely, in several countries, including South Africa, there are **no specific regulations governing the utilization of technologies such as ChatGPT,** either within the scope of data protection or otherwise. The Protection of Personal Information Act 4 of 2013 (POPIA) solely oversees the processing of personal information through automated means and does not encompass the complete capabilities of AI systems like ChatGPT.[30] South Africa's Information Regulator sought to identify approaches to the regulation of viral chatbot ChatGPT and other artificial intelligence (AI) technologies, to ensure they don't violate data privacy laws.[31]

As relates to the adoption of digitization on the continent, the rise in enterprise data volume, and the growing awareness towards the potential benefits of data monetization, resulted in Africa's Data Monetization Market being projected to grow at a CAGR of 18.47% by 2027.[32] The challenge witnessed by data-driven models in the region has however been raising significant issues about the effectiveness of consent for all users.

Court decisions also supported the adherence of privacy in the use and deployment of emerging technologies. On May 31, 2023, in the case of ***Ondieki V Maeda (Petition E153 of 2022)***, the High Court granted a petition addressing the violation of the constitutional right to privacy in the context of installing CCTV cameras in a residential area. Considering the Respondent as a data controller, the High Court ruled that the Respondent should have been registered with the Data Commissioner and obtained the Petitioner's consent to collect data through the CCTV cameras. Ultimately, the High Court, by allowing the claim, issued a declaratory order stating that the actions of the Respondent violated the Petitioner's rights under Article 31 of the Constitution and his rights as a data subject under the Data Protection Act.

27 ecdpm (2023) *Navigating the intersection of AI, Data Protection, and gender in Africa: A feminist approach - centre for intellectual property and information technology law*, *Looking into the Crystal Ball: Artificial Intelligence Policy and Regulation in Africa*. Available at: https://ecdpm.org/work/looking-crystal-ball-artificial-intelligence-policy-regulation-africa#:~:text=rights%20of%20individuals.-,The%20role%20of%20data%20protection%20law%20in%20AI%20regulation,automated%20processing%20of%20personal%20data. (Accessed: 24 January 2024).

28 Ibid

29 *New AI rules in Gabon's Personal Data Protection Law* (no date) *African AI Observatory*. Available at: https://www.africanobservatory.ai/social/new-ai-rules-in-gabons-personal-data-protection-law (Accessed: 22 January 2024).

30 Malinga, S. (2023) *InfoReg examines regulation of ChatGPT, AI in SA*, *itweb.ca.za*. Available at: https://www.itweb.co.za/article/inforeg-examines-regulation-of-chatgpt-ai-in-sa/JN1gPvOAxVXMjL6m (Accessed: 22 January 2024).

31 Ibid

32 Knowledge Sourcing Intelligence LLP (2023) *Middle East and Africa Data Monetization Market anticipated to grow at a CAGR of 18.47% over the next five years*, *einpresswire.com*. Available at: https://www.einpresswire.com/article/646854692/middle-east-and-africa-data-monetization-market-anticipated-to-grow-at-a-cagr-of-18-47-over-the-next-five-years (Accessed: 22 January 2024).

AI's privacy dilemma rests on key issues;[33]

- The technology's use of data (also personal data) to feed its machine-learning algorithms has raised serious concerns about data storage, usage, and access. Where does this data originate? How and where is it stored? Who has access to it, and under what circumstances? These are questions that traditional data protection laws are not equipped to answer.
- AI's capacity to analyze data and make complex analyses amplifies privacy concerns. Its potential to infer sensitive information, such as a person's location, preferences, and habits, poses risks of unauthorized data dissemination. Coupled with the potential for identity theft and unwarranted surveillance, AI presents a unique set of challenges that demand immediate proactive solutions.

AI advancements are prompting a call for ethical guidelines and best practices to mitigate privacy risks. Noteworthy actions have been taken by industry leaders, such as Elon Musk's open letter in March 2023 advocating for a six-month pause on AI development to evaluate the societal impact of the technology. This unprecedented move has compelled the industry to closely examine the implications of AI.[34]

Several esteemed organizations have responded to this challenge by proposing ethical benchmarks. The Partnership on AI (PAI), a coalition comprising leading companies, organizations, and individuals impacted by artificial intelligence, stands out as a guiding force. PAI brings together diverse stakeholders, ranging from tech giants to AI users, to create a collaborative platform. Their mission is centered on establishing common ground, positioning PAI as a unifying catalyst for positive change within the AI ecosystem.[35]

Simultaneously, the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems has a clear directive: "to ensure every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained, and empowered to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity." They advocate that AI, both in its design and application, should inherently prioritize human welfare, emphasizing that ethical considerations should be integral to AI's evolution, not mere afterthoughts.[36]

### B. Privacy and Cybersecurity Landscape in 2023

According to IBM Security's annual "Cost of a Data Breach" report, the average data breach cost for South African organizations reached an all-time high of R49.45 million in 2023. This is an 8% increase over the last 3 years, and a 73% increase since South Africa was added to the report 8 years ago.

The Democratic Republic of Congo in 2023 enacted the Digital Code 2023, specifically targeting cybercrimes. This legislation, comprising an ordinance law, serves to operationalize legal and regulatory provisions related to cybercrimes. The code's scope encompasses digital activities, services, electronic tools, service providers, digital content, and the security and global protection of computer systems. Despite the Digital Code's focus on cybercrimes, there is a notable absence of laws or regulatory instruments addressing data protection and privacy, consumer protection, electronic transactions, or e-commerce. However, the DRC Constitution recognizes the right to privacy in correspondence, telecommunications, and other forms of communication. Additionally, the Framework Law contains only partial penal stipulations, indicating a potential gap in comprehensive legal frameworks for certain aspects of digital activities in the country.

33 Gai Sher and Ariela Benchlouch. "The Privacy Paradox with AI." Reuters, October 31, 2023. https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/.
34 Gai Sher and Ariela Benchlouch. "The Privacy Paradox with AI." Reuters, October 31, 2023. https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/.
35 Ibid
36 Ibid

In the second quarter of 2023, global breached accounts witnessed a significant surge of 156%, as reported by Surfshark's research. A staggering total of 110.8 million accounts were exposed during this period, equating to an alarming rate of 855 accounts leaked every minute.[37]

The geographical breakdown in this quarter revealed a notable shift. While Asia, Africa, and Antarctica experienced a downturn, North America, Europe, Oceania, and South America encountered a rise in the number of leaked accounts.[38]

Notably, three regions—Asia, Africa, and Antarctica—experienced a reduction in breached accounts compared to the previous quarter. Asia, which held the second-highest number of breaches in the last quarter, witnessed a notable decline from 10.9 million to 5.8 million leaked accounts. Similarly, Africa observed a slight quarterly decrease, with breached accounts dropping from 1 million to 980,000.[39] Kenya saw a significant surge in cyberattacks, with 860 million incidents reported in the past year. One notable incident involved a cyberattack on the eCitizen platform in July 2023, disrupting access to over 5,000 government services provided by ministries, county governments, and agencies.[40] read more here.

### i. Incidences

Uganda's Personal Data Protection Office issued an Abridged Investigation Report of the Data Security Breach at Uganda Security Exchange (USE) in June 2023. This was after the Authority became aware of the unauthorized access to USE's third party technologies logging servers that received data from USE's Easy Portal which compromised the privacy of the Personal Data under their custody. The authority found that both parties were negligent in the handling of personal data and that it was non-compliance with the Data Protection and Privacy Act. The authority gave USE and Soft Edge Uganda Limited a three months time frame to rectify all non-compliant areas outlined in the report.

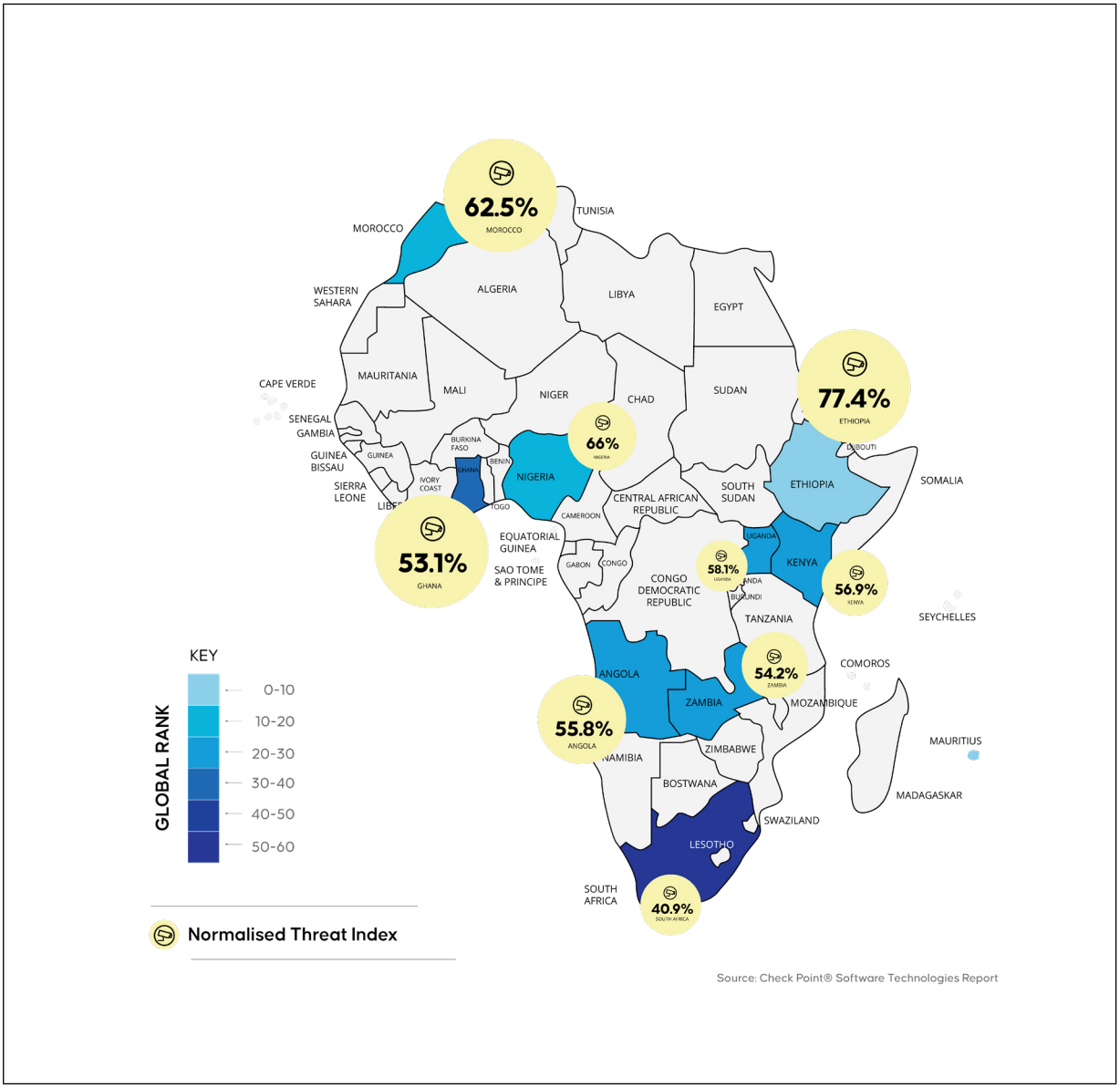
Kenya's Local supermarket chain Naivas Limited experienced a data breach resulting in the unauthorized transfer of 611 GB of personal data from customer loyalty programme information. Appearing before the Senate ICT committee, the Data Commissioner indicated that the supermarket chain did not follow the law in reporting the ransomware attack and that Naivas breached the law by failing to report theft of customer data within 72 hours as is required by law and could face a Sh5 million penalty.

In February 2023, the Nigeria Data Protection Bureau commenced a probe into two of Nigeria's tier 1 banks over data breaches and cyber fraud losses reaching millions of naira. Data from Nigeria's payment settlement system show that within the first nine months of 2020, fraudsters attempted 46,126 cyber attacks against banks and were successful 41,979 times, representing a staggering 91 percent fraud success rate.[41]

37 "Data Breaches Ramped up Globally as 2023 Reaches Midpoint." Surfshark, August 1, 2023. https://surfshark.com/research/study/data-breach-statistics-q2-2023.
38 Ibid
39 Ibid
40 Musau, D. (2023) *Kenya Hit By Record 860 Million Cyber-Attacks In 2023*, *citizen.digital*. Available at: https://www.citizen.digital/news/kenya-hit-by-record-860-million-cyber-attacks-in-2023-n328649 (Accessed: 24 January 2024).
41 Samson Akintaro, "Nigeria Data Protection Bureau Probes Two Banks Over Alleged Data Breach," Nairametrics, January 31, 2023, https://nairametrics.com/2023/01/31/nigeria-data-protection-bureau-probes-two-banks-over-alleged-data-breach.

Check Point® Software Technologies Report revealed the top 10 African countries that were most susceptible to cyber threats.[42]

**AI Policies and Strategies in Africa as of 2023**




## ii. Privacy and Cybersecurity in Africa's Democratic Process

Elections continue to be considered an essential aspect of the democratic process and in 2023, Africa had elections held across Madagascar, Liberia, Nigeria, Gabon, Sierra Leone and Zimbabwe. In the **Nigerian** presidential elections, the Minister of Communication and Digital Economy disclosed that the country encountered a total of 12,988,978 cyberattacks in the days leading up to and during the election, originating from both within Nigeria and externally.[43] The reported attacks on the Independent National Electoral Commission (INEC's) results viewing portals during the 2023 national elections indicated the potential for data breaches involving Personal Identifiable Information. Given the widespread use of technology in various election phases, including voter registration, identifi-

42 Henriques, B. (2023) *Top 10 African countries most vulnerable to cyber threats • 360 mozambique*, *360 Mozambique*. Available at: https://360mozambique.com/world/africa/top-10-african-countries-most-vulnerable-to-cyber-threats/ (Accessed: 22 January 2024).

43 Kaunert, C. and Sibe, R. (2023) *TECHNOLOGY, CYBER SECURITY AND THE 2023 ELECTIONS IN NIGERIA Prospects, Challenges and Opportunities*, *eisa.org*. Available at: https://www.eisa.org/storage/2023/11/2023-journal-of-african-elections-v22n2-technology-cyber-security-elections-eisa.pdf.pdf (Accessed: 22 January 2024).

cation, and vote tabulation, INEC was exposed to potential risks of data breaches and information governance challenges. Intelligence reports revealed an average of 1.55 million cyberattacks per day in the days preceding the elections, reaching a peak of 6.99 million on election day. These indicators suggested that INEC lacked the necessary cybersecurity and privacy readiness.[44]

In **Zimbabwe**, in the lead-up to the August 2023 general elections, citizens reported receiving unsolicited messages from the ruling party that promoted Mnangagwa's reelection.[45] Econet and the ZEC have been accused of providing voters' personal data to ZANU-PF, as was the case ahead of the 2018 elections[46]

In **Senegal,** A group of hackers called Mysterious Team made multiple Senegalese government websites go offline overnight by hitting them with denial-of-service (DDoS) attacks, according to a government spokesperson. The group claimed responsibility for the cyber attacks in a series of Twitter posts using the hashtag #FreeSenegal used by campaigners alleging political repression in Senegal. The attacks come at a time of heightened political tensions in Senegal.[47]

### C. Data Practices in Lending

The growing automation of lending technologies and services raises concerns about the possible reinforcement of biases and discrimination, potentially exacerbating the marginalization of underrepresented groups. For instance, biased historical data in loan decision-making algorithms can result in disadvantages for women and people of color.[48]

The financial landscape in Africa is evolving with the advent of data and digitisation which has led to the rise in financial transaction volume underscoring the need for digital identification to help businesses conduct know-your-customer (KYC) checks and safeguard against fraud. Digitisation is also resulting tremendous innovation within the fintech sector, which is likely to be concentrated in markets such as Cameroon, Côte d'Ivoire, Egypt, Ghana, Kenya, Morocco, Nigeria, Senegal, South Africa, Tanzania, and Uganda (together they account for 70 percent of Africa's GDP and half of its population).[49]

Additionally, these developments have resulted in the consolidation of national identity databases and identification cards across the continent as government services become digitized, wherein Smile Identity H1 KYC reported that there was an enhancement in the uptime of national ID databases across Africa in 2023, compared to 2022.

#### i. Digital lending practices across African countries

As of March 2023, Crunchbase reported a thriving fintech industry in Africa, boasting 529 consumer-lending companies. These firms provide an alternative credit source for individuals unable to secure traditional bank loans. Despite the positive impact of fintech in expanding financial services access, it has also led to a rise in predatory lending practices in various African countries, trapping borrowers in perpetual cycles of debt. We illustrate below lending practices and resultant regulatory frameworks in some of the African countries.

44 Ibid
45 "Freedom House on the Net 2023." Freedom House, n.d. https://freedomhouse.org/country/zimbabwe/freedom-net/2023.
46 Ibid
47 "Senegalese Government Websites Hit with Cyber Attack." Reuters, May 28, 2023. https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/.
48 Mudongo, O. (2023) *Navigating the intersection of AI, Data Protection, and gender in Africa: A feminist approach - centre for intellectual property and information technology law*, *Centre for Intellectual Property and Information Technology law - Centre for Intellectual Property and Information Technology law*. Available at: https://cipit.strathmore.edu/navigating-the-intersection-of-ai-data-protection-and-gender-in-africa-a-feminist-approach/ (Accessed: 24 January 2024).
49 McKinsey & Company (2022) *Fintech in Africa: The end of the beginning*, *McKinsey & Company*. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/fintech-in-africa-the-end-of-the-beginning (Accessed: 25 January 2024).

### Kenya

Kenya has seen significant regulatory reforms in the digital credit market over the years, which includes unregulated fintech lenders, mobile banking-enabled lenders, and digital overdraft facilities provided by Mobile Network Operators (MNOs). These have included issuance of Gazette Notice No. 55 to eliminate negative Credit Reference Bureau (CRB) listings for small amounts and restrict non-bank Digital Credit Providers (DCPs) from participating in credit information sharing, The 2021 amendment to the Central Bank of Kenya Act to supervise previously unregulated fintech DCPs, and the Central Bank of Kenya (Digital Credit Providers) Regulations, 2022, which focus on corporate governance, transparency, and anti-money laundering measures for DCPs thereby bringing them under regulatory oversight and aligning them with data protection and consumer protection laws.

These reforms were prompted by concerns about high default rates, aggressive loan recoveries, and unethical practices as reported by The FinAccess Household Survey. The Competition Authority of Kenya underscored a significant average Annual Percentage Rate (APR) of 280.5% among unregulated DCPs, leading to public outcry and policy concerns regarding money laundering and data abuse.[50] Since March 2022, the CBK has received over 400 applications from DCPs in light of the mandate by the Central Bank of Kenya to licenses Digital Credit Providers (DCPs) under Section 59(2) of the Central Bank of Kenya Act. The decision to regulate and oversee DCPs was prompted by public concerns about the predatory practices of unregulated DCPs, including their high costs, unethical debt collection practices, and the misuse of personal information.

In January 2023, the CBK announced the **licensing of 12 Digital Credit Providers (DCPs),** and by May 2023, it announced the **licensing of an additional 20 Digital Credit Providers,** bringing the total number of licensed DCPs to 32.

Such measures have however not stopped unscrupulous activities by certain industry players. In September 2023, Mulla Pride Ltd, a digital credit provider that operates KeCredit and Faircash, used names and contacts obtained from third parties, and subsequently sent threatening messages and phone calls, a clear violation of data protection regulations. In response to this violation, the Data Protection Commissioner imposed a fine of Sh2.97 million on Mulla Pride Ltd.[51]

### Nigeria

As in Kenya, there are several laws and regulations in place that govern digital lenders in Nigeria. The Consumer Protection Framework of 2016 prohibits financial institutions under the jurisdiction of the Central Bank of Nigeria from disclosing customers' personal information. These institutions are required to establish suitable data protection measures and staff training programs to prevent unauthorized access, alteration, disclosure, accidental loss, or destruction of customer data.

The Cybercrimes (Prohibition, Prevention Etc) Act of 2015 sets forth various requirements for financial institutions to retain and protect data, and criminalizes the interception of electronic communications, The Consumer Code of Practice Regulations of 2007, issued by the Nigerian Communications Commission (NCC), outlines general principles related to the collection and maintenance of customer information by licensees while The Credit Reporting Act of 2017 grants data subjects the right to pri-

50 Report on the Competition Authority of Kenya Digital Credit Market Inquiry (Competition Authority of Kenya, May 2021): https://www.cak.go.ke/sites/default/files/Digital_Credit_Market_Inquiry_Report_2021.pdf

51 Abuya, K. (2023) *Kenya fines two digital lenders $20,000 for abusing user data*, *techcabal.com*. Available at: https://techcabal.com/2023/09/26/digital-lenders-fined-in-kenya/#:~:text=Mulla%20Pride%20Ltd%2C%20which%20operates,borrowers%20into%20paying%20their%20loans. (Accessed: 22 January 2024).

vacy, confidentiality, and protection of their credit information. These regulations collectively ensure that digital lenders operate within a framework that prioritizes data protection and consumer rights. In light of these regulations, the Joint Regulatory and Enforcement Task Force (JRET) conducted investigations into potential violations of privacy and other rights by Digital Money Lenders. Additionally, the Federal Competition and Consumer Protection Commission resumed its activities, registering digital money lending apps under the Limited Interim Regulatory Framework and Guidelines for Digital Lending 2022.[52]

In August 2023, the Federal Government, through the **Federal Competition and Consumer Protection Commission, published a list of 154 fully approved digital lenders authorized to operate in the country.** Additionally, 40 others received conditional approval, 20 were placed on a watch list, and nine apps were delisted.

Consumers have also actively pursued the rights under these laws, with a noteworthy case being that of Mr. Garba, **a Nigerian individual,** who **lodged a complaint with the National Information Technology Development Agency (NITDA) against 9Credit**, a digital credit provider. In his petition dated September 17, 2023, Mr. Garba alleged cyber-bullying and harassment by 9Credit, seeking N50 million in damages for what he deemed "defamatory, derogatory, and malicious actions."[53] Similarly, **Soko Loan faced a NITDA fine of N10 million for data privacy breaches following multiple complaints.**

### Ghana

In 2023, Ghana, as was the case in multiple jurisdictions, witnessed a proactive regulatory effort aimed at safeguarding consumers and users of digital lending services from predatory practices and privacy infringements. The Bank of Ghana cautioned the public against unlicensed entities that are engaged in the provision of loans through mobile applications to the Ghanaian public, which was in contravention of the Banks and Specialized Deposit-Taking Institutions Act, 2016 (Act 930).[54] The Notice reiterated that the activities of these entities significantly breach customer data and privacy laws, as well as consumer protection requirements and norms, with unfavorable implications on the integrity and wellbeing of their patrons.[55] **The Bank proceeded to list 97 loan applications which offered products on the market without a license or authorisation from the Bank of Ghana.** The Cybersecurity Authority of Ghana also put out an Alert warning the public against 10 mobile apps as per their findings, they are not sanctioned by the Bank of Ghana and the Data Protection Commission. Their findings revealed that these apps victims would typically have granted these Apps permissions during installation (unknowingly or without proper scrutiny), to access their data and personal identifiable information (PII) e.g., name, phone number, Ghana card ID number, contacts, photos etc. and hence their access and use of the data and PII of users are in violation of the Data Protection Act, 2012 (Act 843).[56]

A joint initiative led by the Cyber Security Authority, the Bank of Ghana, and the Economic and Organized Crime Office (EOCO) led to a significant crackdown on illicit loan app operators. Over 420 individuals in Ghana were apprehended as part of this operation, targeting various illegal activities

52 FCCPC (2023) *Registration of Digital Money Lenders*, *fccpc.gov.ng*. Available at: https://fccpc.gov.ng/registration-of-digital-money-lenders/ (Accessed: 22 January 2024).
53 Kunle Sanni. "INVESTIGATION: How Digital Loan Providers Breach Data Privacy, Violate Rights of Nigerians." Premium Times, n.d. https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html?tztc=1.
54 Bruce, E. (2023) *See BoG's list of 97 unlicensed entities providing loans through mobile apps , Looking into the Crystal Ball: Artificial Intelligence Policy and Regulation in Africa*. Available at: https://www.graphic.com.gh/business/business-news/see-bogs-list-of-unlicensed-entities-providing-loans-through-mobile-apps.html (Accessed: 24 January 2024).
55 Ibid
56 Cyber Security Authority (2023) *Cyberbullying By Digital Lending Mobile Application Owners*, *csa.gov.gh*. Available at: https://www.csa.gov.gh/cert-gh-alert10.php (Accessed: 22 January 2024).

such as cyberbullying, extortion, misuse of data and privacy, and, in extreme cases, issuing death threats.[57]

### Uganda

The Uganda Microfinance Regulatory Authority, in collaboration with the Ministry of Finance and the Bank of Uganda, released Digital Lending Guidelines set to be implemented in December. These guidelines, part of a collective effort, aim to protect customer information and restrict the sharing of customer details with the Credit Reference Bureau unless explicit consent is provided at least 30 days in advance.[58]

Earlier in the year, **the regulator had also issued a list of 2,132 licensed money lending businesses, encompassing digital money lending operations, authorized to operate within the country.**[59]

## D. Innovation and User Data Protection

### i. Startup Trends in Africa

Building on Africa's enhanced connectivity, a new wave of African startups has emerged, tackling some of the continent's biggest challenges with "homemade" digital technologies. In 2023, the startup landscape in Africa saw significant developments in legislation, funding, and innovation.

The Ivorian government introduced its Startup Act, which is currently awaiting parliamentary approval. Nigeria launched the Startup Support and Engagement Portal,[60] which was a key part of the implementation of the Nigeria Startup Act to promote the identification and consolidation of Nigerian startups, venture capital firms, hubs, and innovation centers.

Kenya's President William Ruto pledged to sign the Start-up Bill 2022 into law by April 2024,[61] aiming to bolster the country's startup sector. Should this be actualised, the extensive two-year process of formulating Kenya's pro-startup legislation would reach its conclusion.

Similar urgency was observed in Rwanda, where the government initiated a Policy Hackathon in May, bringing together prominent local founders and investors to contribute their experiences in building and expanding businesses, ensuring that insights from the field inform the development of the Rwanda Startup Act. Furthermore, the government engaged the services of the Innovation for Policy Foundation (i4Policy), a firm that has played a pivotal role in crafting startup Acts in other countries, such as Tunisia and Senegal.[62]

During the second African Startup Conference in Algiers (December 5-7, 2023), technology ministers from Algeria, South Africa, Tunisia, Botswana, and Nigeria unveiled plans to introduce startup visas with the aim of facilitating the free movement of startups on the continent and boost the mobility of young entrepreneurs.

57 Staff Reporter (2023) *Ghana's Rogue Loan Apps Syndicate Draws Massive Crackdown*, *weetracker.com*. Available at: https://weetracker.com/2023/07/14/ghana-loan-app-crackdown/ (Accessed: 22 January 2024).
58 Samilu, B. (2023) *Govt sets new rules for online money lending*, *monitor.co.ug*. Available at: https://www.monitor.co.ug/uganda/news/national/govt-sets-new-rules-for-online-money-lending-4336196 (Accessed: 22 January 2024).
59 Ibid
60 Jackson, T. (2023) *New startup support portal launched as part of Nigeria Startup Act implementation*, *Disrupt Africa*. Available at: https://disrupt-africa.com/2023/11/27/new-startup-support-portal-launched-as-part-of-nigeria-startup-act-implementation/ (Accessed: 22 January 2024).
61 KPILAAKAA, J. (2023) *Kenya's Startup Bill set to become law by April 2024*, *Benjamindada.com*. Available at: https://www.benjamindada.com/kenya-start-up-bill-signed-april-2024/ (Accessed: 22 January 2024).
62 Ashimwe, E. (2023) *Rwanda: Nine Major Incentives in Rwanda's Proposed Startup Act*, *Allafrica.com*. Available at: https://allafrica.com/stories/202309260092.html (Accessed: 22 January 2024).

In terms of funding, African startups secured $3.4 billion in 2023, marking a 32% decrease from the $5 billion recorded in 2022. Notably, equity funding saw a substantial 60% reduction.[63] Fintech remained a focal point, with eight companies ranking among the top 20 most funded startups in Africa.

### ii. Regulatory Compliance for Startups

As more countries seek to ensure vigilance in regulating the digital space, including privacy and data protection, the gig economy, etc. startups across the region are grappling to tackle the necessary regulatory compliance required on different fronts.

Startups processing personal data are now required to contend with amongst other privacy implications on their users' data: adherence to the data protection principles, requirement to register as data controllers and data processors, cross border transfer of data, handling of sensitive data. Despite these laws being in place, there is no record showing the extent of compliance by startups operating in the different sectors.

Additionally, while several countries have enacted data protection laws and policies, **regulation still tend to be broad in outlook and are not necessarily focused specifically on each of the different sectors startups are operating in** i.e. e-health, ed-tech, fintech, logistics, legal tech etc, the data these startups generates or how to safeguard it.[64]

The fintech sector is comfortably the most-populated vertical within Africa's wider tech ecosystem, having maintained its steady growth with the number of fintech startups active in Africa having increased by 125.2 per cent between 2017 and 2023.[65] It is similarly more regulated by governments who are investing in protecting the consumers and upholding their rights, including privacy and competition rights.

Countries are also taking a live time-bound testing of innovations approach to regulation to accommodate more sustainable and successful startups. The Bank of Tanzania introduced the Fintech Regulatory Sandbox Regulations in 2023. These regulations are designed for licensed financial service providers, fintech firms partnering with licensed providers, and fintech companies aiming to provide solutions within the regulated financial services sector overseen by the Bank of Tanzania. This marked a significant step towards fostering innovation and growth in the fintech sector. The Central Bank of Nigeria's regulatory sandbox was expected to provide startups with a way to test innovative ideas in a secure environment with guidance from the CBN. The Regulatory Sandbox initiated by the Communication Authority of Kenya is designed to promote closer collaboration between ICT innovators and the regulatory body. Launched in 2023, it is an alternative regulatory tool that allows innovators to test emerging ICT products and services in a controlled environment. The sandbox is open to a wide range of innovations, including innovative telecommunication solutions, cybersecurity tools, IoT devices, e-health solutions, e-learning platforms, drone technologies, AI-driven services, new broadcasting technologies, smart city solutions, and digital identity solutions. The Bank of Ghana (BOG) launched its Regulatory Sandbox in 2023, a supportive and controlled policy environment that allows financial service providers to test innovative products, services, and business models in a live environment under the supervision of a regulator. The first cohort window largely accepted innovations from priority areas such as payments, remittances, crowdfunding, and micro-lending.

63 African startups raise $2.9 billion last year". The Guardian Nigeria

64 CIPESA (2023) *Patient Data Privacy in the Age of Telemedicine: Case Studies from Ghana, Rwanda and Uganda*, *opennetafrica.org*. Available at: https://www.opennetafrica.org/patient-data-privacy-in-the-age-of-telemedicine-case-studies-from-ghana-rwanda-and-uganda/ (Accessed: 22 January 2024).

65 Jackson, T. (2023b) *Number of active African Fintech Ventures jumps 17.7% in 2 years*, *disruptafrica.com*. Available at: https://disruptafrica.com/2023/08/24/number-of-active-african-fintech-ventures-jumps-17-7-in-2-years/ (Accessed: 22 January 2024).

### E. Privacy in the age of Big Tech

Big Tech companies, including Google, Facebook, Amazon, Apple, and Microsoft, have posed a substantial privacy challenge, particularly in the Global South, in the AI era. Their accumulation of extensive user data grants them unparalleled control over personal information and technologies driven by data, presenting a significant concern for privacy[66] and have led to these companies having faced scrutiny for using unethical practices.

Africa saw a big win in 2023 as a **Kenyan Court** found Facebook was a proper party to the case filed by Daniel Motaung, a former content moderator for Facebook. This decision marked a significant milestone in the continent's legal landscape, acting as a precedent that the tech companies can be sued in African courts. The Kenyan Court's decision to recognize Facebook as a proper party in the case marked a turning point in African legal history. It not only demonstrated the judiciary's commitment to addressing suits against big tech companies but also emphasized that multinational tech giants are subject to legal scrutiny within the continent. This landmark ruling emboldened the pursuit of justice for privacy-related matters, encouraging individuals and advocacy groups to hold tech companies accountable for their actions on African soil.

Google was another tech giant which faced a lawsuit in Kenya over alleged privacy violations. The company was accused of illicitly tracking Android users and gathering personal data, including facial images of internet users. This class-action lawsuit was lodged by the African Centre for Corrective and Preventive Action (ACCPA), in conjunction with 31 Google users who employ its mobile applications on the Android platform.[67] The petitioners argued that Google, via the Global Positioning System (GPS), was effectively able to monitor the movements of Android users without their explicit consent.

In **Nigeria**, the National Commissioner of Nigeria's Data Protection Commission (NDPC) disclosed that OPay, Meta, and DHL are under investigation for alleged data privacy violations, as stipulated in Section 48 (5) of the Nigeria Data Protection Act of 2023. If found culpable, these companies may face fines amounting to 2% of their gross revenues from 2022. OPay is being probed for accusations of unauthorized account creation, while the specific details of Meta and DHL's potential infractions remain unclear. Reports suggest that Meta faced customer complaints about engaging in behavioral advertising without obtaining their consent.[68]

66 Abiero, D., Kutima, V. and Wairegi, A. (2023) *Unveiling Privacy in the AI Era*, *cipit.org*. Available at: https://cipit.org/wp-content/uploads/2023/10/Unveiling-Privacy-in-the-AI-Era_Infographic_compressed.pdf (Accessed: 22 January 2024).
67 Nancy Gitonga. "Lobby Group Sues Google over Privacy." People Daily, March 10, 2023. https://www.pd.co.ke/news/lobby-group-sues-google-over-privacy-172524/.
68 Olaoluwa, J. (2023) *OPay, DHL, Meta may face steep fines as NDPC begins investigation into alleged data privacy violations*, *techcabal.com*. Available at: https://techcabal.com/2023/10/10/opay-dhl-meta-risk-fines-as-ndpc-begins-privacy-investigation/ (Accessed: 24 January 2024).

# CONCLUSION

Following the review of Privacy Trends in the 2023/2024 period, we anticipate a surge in policy developments and the fortification of Data Protection and Privacy measures across the continent. This evolution aims to safeguard citizens in light of the rapid evolution of internet usage in Africa, which witnessed a substantial increase to approximately 570 million users in 2022, more than doubling the 2015 figures according to Statistica.

In the realm of Data Protection regulations, we expect countries in Africa lacking existing Data Protection Acts or regulations to either enact or draft legislations. Those with draft regulations, such as Malawi and Seychelles, are anticipated to progress to the enactment of their draft legislation. Our focus will be on monitoring developments in data protection authorities, their powers to ensure regulatory adherence, and the anticipated establishment of data protection officers in other countries.

The implementation of the Malabo Convention will trigger further discussions and decisive actions, with stakeholders persistently assessing its effectiveness. Positive developments may be attributed to assertions that the Convention will facilitate dual criminality, streamline the delineation of cybercrime across jurisdictions, and enhance information exchange on cyber incidents. Additionally, initiatives like revising the Convention through the formulation of guidance notes and protocols will ensure alignment with evolving trends in the data protection and cybersecurity domain.

In the cybersecurity domain, we foresee substantial investments by African governments and the private sector to protect the personal data they collect and store. This proactive approach is expected to preempt or minimize data breaches, which experienced a surge in previous years.

Regarding the startup ecosystem, especially the burgeoning fintech sector, we anticipate jurisdictions prioritizing the implementation and compliance with existing Data Protection regulations. Furthermore, we look forward to witnessing the enactment of Startup Acts and Legislations in the coming year, notably from countries such as Kenya, where such legislations are currently under consideration in Parliament.

# ANNEXURES

**COUNTRY REPORTS**

## a. Kenya

**i. New Laws**

Personal Data protection in Kenya is governed by the Data Protection Act of 2019. There were no amendments or new laws/regulations enacted in Kenya in 2023. However, the Office of the Data Protection Commissioner (ODPC) took significant steps to enhance understanding and compliance with the Act;

The ODPC published the Data Protection Handbook, designed to provide simplified information to Data Controllers and Data Processors and acts as an awareness wallet for data subjects to better understand their rights and available legal and institutional framework to protect their personal data from processing that is not covered under the existing personal data laws.

In 2023, the ODPC also published various guidance notes aimed at specific sectors.

These include;

- The Guidance note on consent aimed at assigning data controllers and processors understand their duties under the Act.
- The Guidance note for the communication sector that provides important information and direction for service providers operating in Kenya.
- The Guidance note for the Education sector that aims to provide the education stakeholders with a comprehensive overview of their obligations when processing personal data and practical steps to ensure compliance with the law.
- The Guidance note on the processing of Health Data which aims to provide healthcare institutions and the respective stakeholders with a comprehensive overview of their obligations when processing personal data and practical steps to ensure compliance with the law.
- The Guidance note for Digital Credit Providers aims to provide a roadmap for how DCPs should safeguard the right to privacy and data protection for data subjects while at the same time supporting responsible innovation and sound operations within their sector.

The ODPC also published the Complaint Management Manual that provides guidance on complaints management process focusing on inquiry or preliminary investigations only.

**ii. Case Law**

On May 31, 2023, in the case of ***Ondieki V Maeda (Petition E153 of 2022)***, the High Court granted a petition addressing the violation of the constitutional right to privacy in the context of installing CCTV cameras in a residential area. Considering the Respondent as a data controller, the High Court ruled that the Respondent should have been

registered with the Data Commissioner and obtained the Petitioner's consent to collect data through the CCTV cameras. Ultimately, the High Court, by allowing the claim, issued a declaratory order stating that the actions of the Respondent violated the Petitioner's rights under Article 31 of the Constitution and his rights as a data subject under the Data Protection Act.

On May 12, 2023, in the case of ***Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another***[69] where the court was called upon to determine 'whether the Office of the Data Protection Commission (ODPC) acted in excess of its jurisdiction by rendering a decision on a complaint outside the 90-day timeframe set by section 56(5) of the Data Protection Act' the court was in agreement with the applicants that pursuant to the provisions of section 56(5) of the Act the ODPC had a time-bound jurisdiction to investigate and determine the complaint. When the 90 days' period ended, the respondent jurisdiction also came to an end by way of effluxion of time.

On March 31, 2023, in the case of ***Mwanzia v Rhodes (Constitutional Petition E115 of 2022) [2023] KEHC 2688 (KLR)***,[70] The court asserted that the Data Commissioner has the jurisdiction to determine whether Privacy rights in the Bill of Rights are denied, violated, infringed or threatened. The Commissioner has further powers to order appropriate compensation in the event of proof of the infringement.

**iii. Data Protection Authority**

The Data Protection Authority in Kenya is the Data Commissioner.

2023 marked the establishment of the Office of the Data Protection Commissioner's First Regional Office in Mombasa and another one in Nakuru Region. President William Ruto launched the Data Protection Registration System as Kenya commemorated the Data Privacy Day 2023.

The year also saw the ODPC launch a countrywide awareness campaign.

**iv. Fines/Penalties**

The ODPC issued Penalty Notices Against Whitepath Company Limited & Regus Kenya, an Enforcement Notice Against Ecological Industries Limited and other three Penalty Notices against Mulla Pride LTD, Casa Vera Lounge and Roma School Totalling To Kenya Shillings 9, 375,000.

**v. Data Breaches**

In April 2023, Naivas chief commercial officer Willy Kimani revealed that the retail giant suffered a ransomware attack that compromised some of its data. Appearing before the Senate ICT committee, Data Commissioner Immaculate Kassait said the supermarket chain did not follow the law by failing to report theft of customer data within 72 hours as is required by law and could face a Sh5 million penalty. She said the data breach resulted in the unauthorized transfer of 611 GB of personal data from customer loyalty programme information.

69 Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another (Interested Parties) (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR) (Judicial Review) (12 May 2023) (Judgment).

70 Mwanzia v Rhodes (Constitutional Petition E115 of 2022) [2023] KEHC 2688 (KLR) (Constitutional and Human Rights) (31 March 2023) (Judgment)

## b. Uganda

### i. New Laws

The Law governing data protection in Uganda is the Data Protection and Privacy Act and the Regulations that took effect on 12 March 2021. In 2023, Uganda did not witness any amendments or addition of new data protection laws/regulations.

On May, 2023, The Uganda Personal Data Protection Office published the Guidance Note On The Completion Of The Annual Data Protection And Privacy Compliance Report and developed a template for the Annual Data Protection and Privacy Compliance Report that outlines expectations for all organizations required to submit the Annual Data Protection and Privacy Compliance Report at the end of each Government of Uganda financial year and serves as a guide for reporting. In addition, to ensure adequate compliance levels, the authority expanded the scope of this report by invoking Regulation 4(b) of the same Regulations. This expansion aimed to provide the authority with a comprehensive overview of organizations' compliance efforts with the Act and its Regulations.

### ii. Data Protection Authority

The Data Protection Authority in Uganda is the National Personal Data Protection Director head of the Personal Data Protection Office. In 2023, the office participated in the NGO's Annual Legal and Regulatory Compliance Symposium 2023 organized by TASLAF Advocates to empower Non-Governmental Organizations(NGOs) on how they can comply with the Data Protection and Privacy Act.

### iii. Fines/Penalties

Uganda's Personal Data Protection Office issued an Abridged Investigation Report of the Data Security Breach at Uganda Security Exchange (USE) in June 2023. This was after the Authority became aware of the unauthorized access to USE's third party technologies logging servers that received data from USE's Easy Portal which compromised the privacy of the Personal Data under their custody. The authority found that both parties were negligent in the handling of personal data and that it was non-compliance with the Data Protection and Privacy Act. The authority gave USE and Soft Edge Uganda Limited a three months time frame to rectify all non-compliant areas outlined in the report.

### iv. Data Breaches

In June 2023, the Uganda Securities Exchange (USE) encountered a severe data security breach, causing alarm over the privacy and protection of personal data.[71] In June 2023, an entire DDoS campaign was discovered targeting financial and government institutions in Uganda. Among the victims were the Bank of Uganda, the stock exchange, the parliament, as well as many ministries.[72]

71 "Unveiling the Data Security Breach at Uganda Securities Exchange: Lessons in Personal Data Protection." Centre for Technology Disputes Resolution - Uganda, July 14, 2023. https://www.linkedin.com/pulse/unveiling-data-security-breach-uganda/?trk=organization_guest_main-feed-card_feed-article-content.

72 "Cybersecurity Threatscape of African Countries 2022–2023." Positive Technologies, July 28, 2023. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/.

## c. Tanzania

### i. New Laws

On **1 May 2023**, the **Personal Data Protection Act 11 of 2022 came into effect in Tanzania,** marking a significant step forward for data protection in the country. Tanzania also enacted the **Personal Data Collection and Processing Regulations, G.N No. 349 of 2023 (Data Collection Regulations**) and the **Complaint Handling and Breach of Personal Data Regulations, G.N No. 350 of 2023 (Complaint Handling Regulations)** collectively referred to as the Regulations. **Currently, the ACT and the Regulations are available only in Kiswahili.**

### ii. Case Law

In a groundbreaking lawsuit presented at the Shinyanga High Court in northern Tanzania, a Tanzanian entrepreneur has filed a case against the telecommunications company Vodacom Tanzania Ltd, seeking a substantial 10 billion Tanzanian shillings (approximately $4.1 million) in damages. Sayida Masanja contends that Vodacom, South Africa's-founded mobile operator, holding a dominant 29.4% market share in Tanzania with over 17 million customers, wrongfully and deliberately enabled unauthorized access to his personal data and confidential network information by a third party without obtaining his consent.[73]

### iii. Data Protection Authority

Effective from May 12, 2023, the Regulations and the Act, operating under the authority of the Minister of Information, Communication, and Information Technology, oversee aspects such as data collection and processing, as well as procedures for filing complaints under the Personal Data Protection Act 2022 (Act).

### iv. Fines/Penalties

There were no reported Fines/Penalties issued in 2023.

### v. Data Breaches

There are no specific reports of data protection breaches in Tanzania during 2023. However, it's worth noting that Tanzania has been making significant strides in data protection. The country promulgated the Personal Data Collection and Processing Regulations, G.N No. 349 of 2023, and the Complaint Handling and Breach of Personal Data Regulations, G.N No. 350 of 2023. These regulations are intended to regulate the collection and processing of data and procedures for presenting complaints under the Personal Data Protection Act 2022.

73 Osman, M. (2023) *Vodacom Faces Landmark $4 Million Lawsuit Over Alleged Data Breach in Tanzania*, *en.sputniknews.africa/*. Available at: https://en.sputniknews.africa/20230714/tanzanias-vodacom-faces-landmark-4-million-lawsuit-over-alleged-data-breach-1060530723.html (Accessed: 22 January 2024).

## d. Rwanda

### i. New Laws

The Law relating to protection of personal data and privacy is Law No 058/2021 of 13/10/2021. There were no data protection law amendments or new regulations enacted in 2023. In 2023, the data protection office published;

1. The Data Controller and Data Processor registration guide, to assist the citizens in ascertaining if they are a data controller or processor and provide a step by step overview of the registration and certification process.
2. The Guidance Note On Complaints Lodging that contains practical guidance on how to lodge complaints with the Data Protection and Privacy Office and aims to help the citizens know how to lodge complaints with the Data Protection and Privacy Office.
3. The Guidance on Personal Data Inventory and Readiness Checklist Tools, to assist organizations to implement data protection and privacy compliant arrangements.
4. The Data Protection Impact Assessment guide and form, to guide data controllers and data processors through the process of determining whether their data processing operations require a DPIA and understanding when and how the DPIA should be carried out.

### ii. Case Law

In 2023, a significant case in Rwanda revolved around potential breaches of the Data Protection Act 1998 and the UK General Data Protection Regulation (UK GDPR) in the implementation of the Rwanda policy.

The case of R (AAA and others) v Secretary of State for the Home Department [2023] EWCA Civ 745 questioned whether such breaches could invalidate decisions made under paragraphs 345A or 345C of the Immigration Rules. Despite the compelling arguments presented, the Divisional Court dismissed the data protection grounds and refused permission to appeal. The court concluded that **even if the complaints about the transfer of personal data to Rwanda, non-compliance with Article 13 of the UK GDPR, and the defective data protection impact assessment were valid, they would not necessitate the quashing of the decision to relocate the individual known as SAA**. This case underscores the complex interplay between data protection laws and immigration rules, highlighting the ongoing challenges in ensuring data protection in policy implementation.

### iii. Data Protection Authority

The supervisory authority regarding Data protection is the National Cyber Security Authority.

Through November 1-2, 2023, Rwanda's Data Protection and Privacy Office and Mastercard hosted a 2-day Data protection training for more than 80 Data Protection Officers across different sectors in Rwanda. The training, aimed at providing a hands-on and interactive workshop for Data Protection Officers on conducting data protection impact assessments and data breaches management.

From October 1, 2023, to November 17, 2023, NCSA delivered the annual national cyber security and data protection awareness campaign under the theme 'Tekana Online: Protect Personal Data and Privacy!' The Tekana Online campaign sensitized the public on their rights as Data Subjects, and Data Controllers and Data Processors of their obligations to protect personal data and guarantee privacy.

On June 23, 2023, National Cyber Security Authority, Centre for the Fourth Industrial Revolution Rwanda and Covington & Burling LLP closed a three-day workshop on implementation of Rwanda's personal data protection & privacy law. The workshop explored strategic approaches to authorization and certification of international data transfers under Rwanda's Law on Protection of Personal Data and Privacy. The output of the workshop was the creation of multi-stakeholder consultation groups, with actionable items under international data transfers including the development of a certification scheme, creating a standard data transfer agreement, and drafting regulatory guidance on authorization and exemptions.

**iv. Fines/Penalties**

No specific information about any fines or penalties issued by the Data Protection and Privacy Office in 2023.

**v. Data Breaches**

There was no specific information about any data breaches reported in 2023.

## e. Egypt

### i. New Laws

There were no new Laws/regulations or amendments recorded in 2023 in the area of Data protection and Privacy.

### ii. Case Law

There was no specific information about any Data Protection cases reported in 2023.

### iii. Data Protection Authority

The Personal Data Protection Centre (the "Centre") is a public economic authority that is under the authority of the Minister of Communications and Information Technology.

### iv. Fines/Penalties

No specific information about any fines or penalties issued by the Data Protection and Privacy Office in 2023.

### v. Data Breaches

Human Rights Watch reported that, for a duration of eight months, the Egyptian government, along with the British company Academic Assessment Ltd., exposed extensive personal information of tens of thousands of children online. This breach not only infringes upon the privacy of the children but also exposes them to potential serious harm, potentially violating data protection laws in both Egypt and the United Kingdom.

The compromised data encompasses more than 72,000 records, including children's names, dates of birth, gender, home addresses, email addresses, phone numbers, school details, grade levels, personal profile photos, and even copies of their passport or national ID. Shockingly, this sensitive information remained unprotected on the open web throughout this period.

Furthermore, the Ministry of Health and Population confirmed a data leak, initially reported on July 23. Personal data of 2 million Egyptian patients was discovered being sold online for $5,000 on a website. The leaked data comprises patients' names, national ID numbers, provinces, decision numbers, diagnoses, surgical interventions, and referral destinations linked to the presidential initiative to eliminate waiting lists from January 2019 to January 2023.[74]

74 AhramOnline (2023) *Authorities dealt with leak of data for 2 million Egyptian patients: Health minister*, *english.ahram.org.eg*. Available at: https://english.ahram.org.eg/News/505943.aspx (Accessed: 22 January 2024).

## f. Algeria

### i. New Laws

Law No. 18-07, came into effect on August 10, 2023. It establishes, among other things, fundamental requirements for general personal data protection, encompassing elements such as explicit consent, data processing notifications, data subject rights, and constraints on direct marketing and data transfers. Notably, this law introduces significant penalties, potentially including imprisonment for a period ranging from two to five years.

### ii. Data Protection Authority

The national authority, an independent administrative authority for the protection of personal data. Its members and Chairman were appointed by Presidential Decree no. 22-187 of 18 May 2022 for a term of 5 years and officially appointed on 11 August 2022.[75]

### iii. Fines/Penalties

There was no specific information about any Data Protection fines/penalties issued in 2023

### iv. Data Breaches

Trend Micro solutions detected and blocked over 19 million (19,552,217) email threats, prevented over 400,000 (417,156) malicious URL victim attacks, and 34,023 URL hosts. In addition, over half million (508,815) malware attacks were identified and stopped.[76]

75 Algeria Press Service, "Installation of the chairman and members of the National Authority for the Protection of Personal Data", article available at: https://www.aps.dz/algerie/143710-installation-du-president-et-des-membres-de-l-autorite-nationale-de-protection-des-donnees-a-caractere-personnel

76 "Trend Micro Blocked over 29.7 Million Threats in Algeria: Reveals Annual Cybersecurity Report." Trend Micro, n.d. https://www.trendmicro.com/en_ae/about/newsroom/press-releases/2023/05-06-2023.html.

## g. Nigeria

### i. New Laws

On June 12, 2023, President Bola Ahmed Tinubu signed the Nigeria Data Protection Act, 2023 into law. This law replaced the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019, providing a new legal framework for personal data regulation in Nigeria.

The Nigeria Data Protection Commission (NDPC) in 2023 published;

The Code of Conduct for Data Protection compliance organizations with an objective, among others, in promoting professionalism in compliance delivery services within the Data Privacy and Protection ecosystem.

The Strategic Roadmap and Action Plan to provide impetus for articulating and implementing existing and news policies in the Data Privacy Sector.

The Nigeria Data Protection Bureau (NDPB) authority also affirmed the commitment of the government to ensuring Nigeria meets the global benchmark for privacy regulations.

### ii. Case Law

Socio-Economic Rights and Accountability Project (SERAP) has initiated legal proceedings against the Central Bank of Nigeria (CBN) concerning "the failure to remove the blatantly unlawful provisions in the Central Bank of Nigeria (Customer Due Diligence) **Regulations instructing banks to acquire information on customers' social media handles for identification purposes.**" SERAP argues in the lawsuit that "the mandatory requirement of social media handles or addresses of customers does not serve any legitimate aim. Such information may be used to unjustifiably or arbitrarily restrict the rights to freedom of expression and privacy."[77]

In the case with suit number ***FHC/L/CS/1410/2023*** filed at the Federal High Court in Lagos, SERAP is requesting "an order of mandamus to direct and compel the Central Bank of Nigeria to withdraw its directive dated 20th June, 2023, to banks and other financial institutions to obtain information from customers' social media handles."

### iii. Data Protection Authority

The 2023 Act established the office of the Nigeria Data Protection Commission (NDPC) and its Governing Council. The Commission oversees the Act's implementation, enforcing rules and regulations while regulating the processing of personal information. The Council provides overall policy direction for the NDPC. The Voice of Nigeria VON in 2023 partnered with the Nigeria Data Protection Bureau to harness the Fourth Industrial Revolution (FIR) era as they promote Data Protection and Privacy in the country.

### iv. Fines/Penalties

Nigeria Data Protection Bureau (NDPB) in 2023 investigated four banks, one telecommunications firm, consulting firms and a large number of loan sharks for various alleged data breaches, according to Dr. Vincent Olatunji, National Commissioner/Chief Executive Officer, NDPB. Olatunji said investigations would continue as NDPB planned to beam searchlights on other sectors, which are heavy on data.

### v. Data Breaches

According to Surfshark, a cybersecurity firm, data breach incidents in Nigeria increased by 64% in Q1 of 2023, recording 82,000 cases

77 Nathaniel, S. (2023) *SERAP Sues CBN Over 'Unlawful Regulations On Customers' Social Media Handles'*, *channelstv.com*. Available at: https://www.channelstv.com/2023/07/23/serap-sues-cbn-over-unlawful-regulations-on-customers-social-media-handles/ (Accessed: 25 January 2024).

of data breaches in Q1 2023, up from 50,000 recorded in Q4 2022.[78]

The Nigeria Data Protection Commission (NDPC) announced that it is actively investigating 17 major cases of data breaches across various sectors, including finance, technology, education, consulting, government, logistics, and gaming/lottery. Adding that it had received over 1000 complaints of data breach, which led to the investigations.[79]

In June 2023, NDPC disclosed that Zenith, GTB, Fidelity, Leadway Insurance, Babcock University, and some companies were under investigation for alleged data breaches. By October 2023, the Commission said it was investigating Opay, Meta, and DHL for alleged data breach.[80]

78 Usman Aliyu. "Data Breaches and Nigeria's Right to Privacy." News Agency Nigeria, December 23, 2023. https://nannews.ng/2023/12/23/data-breaches-and-nigerians-right-to-privacy

79 Sami Tunji. "NDPC Investigating 17 Major Cases of Data Breach in Nigeria, Earns N400 Million." Nairametrics, n.d. https://nairametrics.com/2024/01/29/ndpc-investigating-17-major-cases-of-data-breach-in-nigeria-earns-n400-million/.

80 Sami Tunji. "NDPC Investigating 17 Major Cases of Data Breach in Nigeria, Earns N400 Million." Nairametrics, n.d. https://nairametrics.com/2024/01/29/ndpc-investigating-17-major-cases-of-data-breach-in-nigeria-earns-n400-million/.

## h. Ghana

### i. New Laws

There were no new Laws/regulations or amendments recorded in 2023 in the area of Data protection and Privacy.

### ii. Data Protection Authority

The Data Protection Commission ('Commission') is the Data Protection Authority.

### iii. Fines/Penalties

The Data Protection Commissioner issued a Press Release, a public warning addressing online apps breaching privacy rights for individuals.

Furthermore, the Ghana Data Protection Commission (DPC) detained individuals from five organizations in September for breaches of the Data Protection Act. The apprehended individuals were affiliated with various institutions, including Care Flight Ghana, the Morning Star School, Kabfam, Embassy Gardens, and Grace Homeopathy Clinic.[81]

In a distinct enforcement operation conducted in August, the DPC, in conjunction with the Criminal Investigations Department (CID), arrested representatives from three other organizations. Additionally, representatives from two additional organizations were summoned for questioning.

### iv. Data Breaches

On June 13, 2023, Ghana's Data Protection Commissioner issued a Press Release, a public warning addressing online apps breaching privacy rights for individuals.

Five persons suspected to have breached data protection laws were arrested by a joint team operation led by the Data Protection Commission (DPC) and the Ghana Police Service. The arrests were made on Thursday, September 28, as part of the DPC's ongoing enforcement operations to crack down on businesses and institutions that are collecting and using personal data without authorization.[82]

81 Oduro-Mensah, D. (2023) *Five suspects arrested for breaching Data Protection laws, citinewsroom.com*. Available at: https://citinewsroom.com/2023/09/three-suspects-arrested-for-breaching-data-protection-laws/ (Accessed: 22 January 2024).

82 Daniel Oduro-Mensah. "Five Suspects Arrested for Breaching Data Protection Laws." Citi Newsroom, September 28, 2023. https://citinewsroom.com/2023/09/three-suspects-arrested-for-breaching-data-protection-laws/.

## i. Senegal

### i. New Laws

In Senegal, the Commission de Protection des Données Personnelles du Sénégal released guidance on processing biometric data in the workplace in August. Senegal published its National Data Strategy, developed with the nonprofit Smart Africa and German development agency GIZ.

### ii. Data Protection Authority

The National Data Protection Authority is the "Commission de Données Personnelles" ("CDP") which is an independent administrative authority. In July, the Personal Data Protection Commission (CDP) of Sénégal and the Personal Data Protection Authority of Mauritania signed a cooperation agreement to exchange knowledge about data protection.

### iii. Fines/Penalties

No specific information about any fines or penalties issued by the Data Protection and Privacy Office in 2023. Nevertheless, the Personal Data Protection Commission (CDP) released its third quarterly report outlining its activities from July to September 2023. According to the report, the CDP issued four warnings and a formal notice to three organizations for contravening data protection laws.[83]

### iv. Data Breaches

A group of hackers called Mysterious Team made multiple Senegalese government websites go offline overnight in May by hitting them with denial-of-service (DDoS) attacks. The group claimed responsibility for the cyber attacks in a series of Twitter posts using the hashtag #FreeSenegal used by campaigners alleging political repression in Senegal.[84]

83 CPD (2023) *Personal Data Protection Commission (CPD) Quarterly Report 2023*. Available at: https://drive.google.com/file/d/1ghuTYMI-1KUGYjcb-goKWaN89GJ7LhSY9/view (Accessed: 25 January 2024).

84 Reuters (2023) *Senegalese government websites hit with cyber attack, reuters.com*. Available at: https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/ (Accessed: 25 January 2024).

## j. Benin

**i. New Laws**

The data protection regime in Benin is governed by two pieces of legislation namely the Law No. 2017-20 of April 20, 2018 on the digital code and the Law No. 2009-09 of May 22, 2009 Dealing with the Protection of Personally Identifiable Information. There were no new Laws/regulations or amendments recorded in 2023 in the area of Data protection and Privacy.

**ii. Data Protection Authority**

The APDP (The Beninese data protection authority) is the regulator. It is an independent body.

**iii. Fines/Penalties**

No specific information about any fines or penalties issued by the Data Protection and Privacy Office in 2023.

## k. Angola

### i. New Laws

Personal data protection is regulated by Law No. 22/11 of 17 June 11, the Personal Data Protection Law, which determines the legal rules applicable to the processing of personal data.

### ii. Data Protection Authority

The Data Protection Law establishes the Agência de Proteção de Dados (APD) as Angola's data protection authority.

### iii. Fines/Penalties

No specific information about any fines or penalties issued by the Data Protection and Privacy Office in 2023.

### iv. Data Breaches

The apex of Angola (Banco Nacional de Angola) suffered a cyberattack on its systems on January 6th, 2024. The Bank says that the breach was however mitigated by its cybersecurity setups, with no significant impact on its data. Speaking at a cybersecurity forum held in Luanda in May 2023, the Bank's governor, José de Lima Massano, said the Bank "registers about 350 cyber attacks daily". He also stressed that the systems have "managed to remain resilient".[85]

85 Andrew Christian. "Angola's Central Bank Tames Latest Data Breach." Benjamindada.com, January 18, 2024. https://www.benjamindada.com/angolas-central-bank-cyberattack/.

## I. South Africa

### i. New Laws

There were no new Laws/regulations or amendments recorded in 2023 in the area of Data protection and Privacy. However, Mauritius and South Africa's DPAs signed a cooperation agreement to collaborate on areas of mutual interest.

### ii. Case Law

There was no specific information about any Data Protection cases reported in 2023.

### iii. Data Protection Authority

The Information Regulator of South Africa is an independent body empowered to monitor and enforce compliance by public and private bodies with the provisions of the Promotion of Access to Information Act, 2000 (Act 2 of 2000), and the Protection of Personal Information Act, 2013 (Act 4 of 2013). The country marked its 10th anniversary of the Protection of Personal Information Act (POPIA) on November 19.

The Regulator also conducted the DIKOPANO Information Regulator roadshow and community engagements guiding the public through the POPIA and PAIA.

### iv. Fines/Penalties

South Africa's Regulator issued its first administrative fine in the amount of ZAR 5 million against the Department of Justice and Constitutional Development (DoJ&CD) on 3 July 2023. It also issued an enforcement notice to Dis-Chem for POPIA violations following a vendor's data breach on September 6.

### v. Data Breaches

In 2023, IBM Security released its annual Cost of a Data Breach Report, revealing that the average data breach cost for South African organizations had reached an all-time high of R49.45 million. This represented an 8% increase over the previous three years and a significant 73% surge since South Africa was first included in the report eight years ago.

It was reported that two of the country's largest consumer credit reporting agencies, TransUnion and Experian, were hit by a fresh data hack, potentially exposing the financial and personal data of South Africans to risk. The hackers, the Brazil-based N4ughtySec-TU Group, demanded $30m (R562.5m) from each of these companies.[86]

86 Sabelo Skiti. "Hackers Demand $60m from TransUnion, Experian for 'new' SA Data Theft." TimesLive, November 23, 2023. https://www.timeslive.co.za/news/south-africa/2023-11-23-hackers-demand-60m-from-transunion-experian-for-new-sa-data-theft/.

## m. Namibia

### i. New Laws

Save for the right to privacy as a fundamental human right under Article 13 of the Namibian Constitution, Namibia has not enacted comprehensive data privacy legislation.

### ii. Case Law

There was no specific information about any Data Protection cases reported in 2023.

### iii. Data Protection Authority

There is no national data protection authority in Namibia.

### iv. Fines/Penalties

No specific information about any fines or penalties issued by the Data Protection and Privacy Office in 2023.

### v. Data Breaches

There was no specific information about any data breaches reported in 2023.


Lawyers Hub Offices, ACK Garden House, 1st Ngong Avenue, Upper Hill, Nairobi, Kenya.

+254 111 215 675 (WhatsApp)
Call: +254 784 840 228
Email: info@lawyershub.ke
www.lawyershub.org