

The East African Privacy

Stay Informed, Stay Compliant!



Peter Ndegwa, Group CEO for Safaricom PLC speaking recently at Strathmore University, Kenya. (Photo by: Safaricom)

More in the Issue

■ Uganda

- The Forum for Data Protection Practitioners Uganda (FDPPU), Scrutinizes USA Uganda Health Data Sharing Agreement.
- Court convicts three for unlawfully disclosing personal data

■ Kenya

- High Court finds Safaricom PLC in violation of subscribers' constitutional rights to privacy, dignity, and consumer protection.
- DPGSK releases annual report.
- Statistics Bill 2026 introduced.

■ Tanzania

Regulator announces 1st Annual Data Protection Conference

■ Across Africa

- South Africa Information Regulator extends deadline for comments on Code of Conduct.
- Nigeria hosts 9 African data protection regulators.

■ Global Insights

- Canadian privacy regulators find Open AI in privacy violation.
- UK Government takes progress in online safety.
- Singapore's Ministry of Health releases Cybersecurity and Data Security Essentials

BTA Summit Gears Up With More Partners Coming on Board.

The inaugural Africa Big Tech Summit, convened by Adlegal International will take place between 30th – 31st July 2026 at Mestil Hotel and Residences in Kampala, Uganda, under the theme: "Big Tech, Data Governance, and Competition Policy in Africa's Digital Economy". The two-day event will spotlight critical issues shaping Africa's digital future: Day one will focus on data protection, while day two will explore competition and consumer rights.

The Summit will feature distinguished experts from across the continent and beyond, including Dr. Vellah Kedogo Kigwiru (Kenya), Babatunde Irukera (Nigeria), Mercy Mutemi (Kenya), Dr. Faith Amarachi Okpara (Nigeria), Olumide Babalola (Nigeria), and Dr. Patricia Boshe (Tanzania), with additional speakers to be announced.

(Continued on Page 2)

Key partners supporting the summit include the Africa Digital Rights Hub, Data Privacy Lawyers Association of Kenya, Africa Competition & Consumer Protection Centre, DPO Privacy Centre (East Africa), CIO-CxO Digital Leadership Forum, East African Community Competition Authority, Alba Advocates, and Datavara Tech Solutions. Registration fees are set at USD 290 for in-person attendance and USD 150 for online participation.

From the Editors

Welcome to the second issue of *The East African Privacy Monthly* – your trusted regional guide to developments in data protection and privacy. While May 2026 has been relatively quiet in some jurisdictions within the region, notable updates have emerged from Kenya and across the continent. Meanwhile, the global privacy landscape continues to buzz with activity.

We remain committed to delivering concise, insightful coverage from across the region and beyond.

Stay Informed. Stay Compliant.

Editorial Team



Namugera Joel Peter,
Head – Research, Training &
Capacity Building Desk,
DPO Privacy Centre (East Africa)



Hellen J. Ndagire,
Associate – MMAKS Advocates

East Africa

Uganda

FDPPUG Scrutinises US-UGANDA Health Data Sharing Agreement

The Forum for Data Protection Practitioners Uganda (FDPPU), an association of privacy professionals, including legal experts, technologists, and digital rights advocates, convened a public X Space on 14th May 2026 to examine the data protection implications of the Uganda–United States Health Data Sharing Framework. The Framework comprising a Memorandum of Understanding and a Data Sharing Agreement, both signed on 10th December 2025, under the US government's America First Global Strategy, has raised significant concerns.

The discussion, hosted in collaboration with the African Centre for Digital Justice

(ADIJUST), moderated by Patrick Mugalula, featured panellists; Morgan Muhindo, Namugera Joel Peter, and Ssekamwa Frank. Participants highlighted several critical inconsistencies between that Framework, as currently disclosed, and Uganda's Data Protection and Privacy Act in several critical respects including; the absence of a Data Protection Impact Assessment, the lack of an adequacy or equivalence determination, the complete exclusion of the Personal Data Protection Office from the Framework, among others.

Court Convicts Three for Unlawfully Disclosing Personal Data

On 5th May 2026, a Magistrate Court in Makindye, Kampala convicted three mobile money agents affiliated with an online lending company, Easy Pesa for unlawfully obtaining and disclosing a client's personal data.

The accused entered guilty pleas under a plea bargain to charges of unlawful access and disclosure of personal data, contrary to Section 35 of the Data Protection and Privacy Act Cap 97 and Regulation 34 of the accompanying regulations. They further admitted to failing to register with the Personal Data Protection Office (PDPO) in

violation of Section 29(3) of the Act..

The three were convicted and each fined Ugx 120,000 or in default face three months imprisonment. This marks the second conviction under the country's data protection following an earlier case against a director of a digital lending app.

Kenya

High Court finds Safaricom in violation of subscribers' privacy rights.

On 13th May 2026, Kenya's High Court delivered a landmark Ruling against Safaricom PLC, finding that the company violated subscribers' constitutional rights to privacy, dignity, and consumer protection following a systemic breach involving unauthorised extraction and dissemination of subscriber data between 2018 and 2019.

The Court held that data controllers bear direct constitutional obligations and cannot avoid liability merely by attributing breaches to "rogue employees" where systemic governance and security failures exist. Importantly, the Court affirmed that in large-scale data breach cases, affected individuals are not required to prove the precise extraction of their specific data where the data controller exclusively controls the underlying systems and records.

The judgment significantly strengthens the constitutional protection of informational privacy, the accountability of private entities handling personal data, the recognition of positive obligations in data governance, and the horizontal application of constitutional rights in the digital economy.

The Court awarded KShs 900,000 in constitutional damages to each petitioner and underscored the need for robust technical and organisational safeguards by entities processing personal data.

DPGSK Releases Annual Report

The Data Privacy and Governance Society of Kenya (DPGSK), established in 2023 to unite privacy professionals across the country, has released its annual report highlighting its notable achievements, including membership growth to 900 members, involvement in over six litigation cases, the successful organisation of townhall dialogues, and engagement with various government entities including the Office of the Data Protection Commissioner. The Society also collaborated with organisations such as Amnesty International and the Tanzania Privacy Professionals Association, among others. It is currently chaired by Dr. Mugambi Laibuta.

Statistics Bill, 2026 to Redefine Data Governance in Kenya

The Kenyan government has tabled the Statistics Bill, 2026, marking a significant shift in Kenya's data governance architecture. The Bill transitions Kenya from a fragmented, sector-driven approach to a coordinated, system-wide model anchored in official statistics.

The Bill proposes to establish a central authority with legal power to access administrative data, regulate data collection activities, and set binding standards across both national and county levels, effectively positioning statistics as a core governance infrastructure rather than a technical function. The Bill also expands the data ecosystem to include big data, citizen-generated data, and even biometric data, while simultaneously embedding safeguards on confidentiality, purpose limitation, and secure processing, aligning statistical production with modern data protection principles.

For data governance practitioners, the Bill implies stronger state-led coordination and increased obligations on data holders to share data for statistical purposes, as well as a regulatory framework for data interoperability and standardisation. It also raises important

questions around data access powers, proportionality, and the interface with the Data Protection Act, particularly where administrative and personal data are repurposed at scale for statistical use.

Tanzania

PDPC.TZ Announces 1st Tanzania Annual Data Privacy Conference.

With Tanzania's Personal Data Protection Act now in full enforcement, the Personal Data Protection Commission has announced Tanzania's 1st Annual Data Privacy Conference, to be held between 29th June – 1st July 2026 at Mlimani City Conference Hall, Dar es Salaam, under the theme "Data Privacy as the Pillar: Securing an Inclusive Digital Future Towards Vision 2050".

The conference is expected to bring together executives, policymakers, industry leaders, and professionals to advance dialogue on compliance with the Personal Data Protection Act and the future of data governance in Tanzania's digital economy.

Across Africa

South Africa

Information Regulator Extended Deadline for Public Comments on Code of Conduct.

South Africa's Information Regulator has extended the deadline for submitting written comments on the draft Code of Conduct relating to the processing of personal information at gated access points. The deadline, which was initially set for 13th May was extended to 29th May 2026, to allow more stakeholders the opportunity to contribute to the process.

Nigeria

Nigeria Hosts Regulators from 9 African Countries

On 4th May 2026, Nigeria hosted data protection authorities from nine African countries in Abuja to drive cross-border regulatory cooperation and harmonise data privacy frameworks. The peer exchange programme, organised by the Nigeria Data Protection Commission (NDPC) in

collaboration with the World Bank and Smart Africa, focused on strengthening institutional enforcement and supporting seamless cross-border data flows.

It convened data protection authorities and policymakers from The Gambia, Burundi, Somalia, Sierra Leone, Liberia, Zambia, Malawi, Ethiopia, and Kenya, alongside representatives from regional bodies including ECOWAS, CEMAC, and IGAD.

Global Privacy Watch

Canada

Privacy Regulators Find OpenAI's ChatGPT Training Violated Privacy Laws

In May 2026, the Office of the Privacy Commissioner of Canada, together with provincial privacy regulators in Québec, British Columbia, and Alberta, concluded a joint three-year investigation into OpenAI's ChatGPT.

The regulators found that OpenAI's initial training and deployment of ChatGPT breached federal and provincial privacy laws, citing concerns including the overcollection of personal information, lack of valid consent and transparency, inaccurate personal information, inadequate rights to access, correction and deletion, and insufficient accountability.

OpenAI has committed to a series of corrective measures. This follows similar investigations by data protection authorities in Italy, Spain, France, and other jurisdictions, reflecting growing global scrutiny of AI companies' data practices.

United Kingdom

UK Government Takes Significant Steps Forward in its Online Safety Agenda

On 29th April, two major pieces of legislation; the Children's Wellbeing and Schools Act (CWSA) and the Crime and Policing Act (CPA), received royal assent.

The CWSA grants the Government regulation-making powers that enable sweeping changes to the Online Safety Act 2023 (OSA) and the UK GDPR, with a duty to have regard to the outcomes from its children's online safety consultation, which closed on 26th May 2026. The CPA grants the Government regulation-making powers to extend the reach of the OSA to capture more AI chatbots, and includes other AI and online safety-related provisions.

Singapore

Health Ministry Publishes Cybersecurity and Data Security Essentials

Singapore's Ministry of Health has published the "Cybersecurity and Data Security Essentials" guidelines, which set out cybersecurity and data security requirements for healthcare providers processing health information pursuant to the Health Information Act (HIA).

The Guidelines form part of the implementation resources for the HIA's

progressive roll-out through early 2027. They apply to HIA entities, that is, persons to whom the HIA applies including licensees under the Healthcare Services Act 2020 (HCSA), National Electronic Health Record (NEHR) contributors and users, and other prescribed entities enabled to share health information under the HIA.

The Guidelines emphasise the importance of emergency planning, advising HIA entities to establish business continuity arrangements to withstand service disruptions arising from cybersecurity attacks or data breaches.

DID YOU KNOW?

As of 2026, 35 African data protection authorities are operational, yet 15 African jurisdictions still lack an established authority despite having enacted data protection laws!



About DPO Privacy Centre (East Africa)

DPO Privacy Centre (East Africa) is a regional hub supporting Data Protection Officers, legal practitioners and organisations across East Africa in navigating data privacy compliance. We provide training, advisory services including outsourced DPO services, and publications like this to foster a culture of privacy in the region. Our aim is to be leaders of privacy discussions across the region.

Subscribe to our Substack to receive our next issue and similar publications direct to your inbox.

substack.com/@privacycentreea

If you want to partner or publish with us, contact us via the email below.

privacycentreeastafrica@gmail.com

Follow us on X and LinkedIn:

[DPO Privacy Centre East Africa](#)

Until next time... **Stay Informed. Stay Compliant.**