

The East African Privacy

Stay Informed, Stay Compliant!



Five Years, 48 Universities and a Title Defended: Inside the Moot Raising East Africa's Privacy Lawyers

Students from Uganda Christian University celebrate after being declared champions of the fifth edition of the Unwanted Witness Privacy Moot Competition. | Photo: Unwanted Witness

Uganda Christian University has done what no team before it had managed: defending both its national and regional crowns as the Unwanted Witness Privacy Moot Court Competition turned five. Our Partnerships & Development Co-Head, Nanyonga Maria, sat down with Allan Sempala Kigozi, Head of Legal and Programs at Unwanted Witness, to talk about loan apps, law schools and the young lawyers changing how East Africa talks about privacy.

(Continued on Page 2)

More in the Issue

■ Uganda

- Data protection complaint filed against Uber following its exit from the Ugandan market.
- Data protection regulator issues decisions on deletion of data and disclosure of birth records.

■ Kenya

- Data protection regulator releases Draft Public Notice on the Prescription of Additional Categories of Sensitive Personal Data.
- Data protection regulator publishes new Guidance Notes for Cross-Border Data Transfers.

■ Across Africa

- Zimbabwe's Postal and Telecommunications Regulatory Authority kicks off mandatory on-site compliance inspections.
- Togo's Personal Data Protection Authority rallies 33 ministries in a public sector compliance drive.
- African data protection authorities celebrate the inaugural Africa Data Protection Day.

From the Editors

Welcome to the sixth issue of **The East African Privacy Monthly** — your regional guide to developments in data protection and privacy. September 2026 was a busy month for the region. In Uganda, the Personal Data Protection Office delivered two decisions on the rights to deletion and rectification, while Uber's sudden exit raised the question of what happens to personal data when a platform leaves the market. Kenya's regulator issued long-awaited guidance on cross-border data transfers, and the continent marked its first Africa Data Protection Day. Globally, key obligations under the EU Data Act and Cyber Resilience Act took effect, Google was fined €403 million, and the UK's ICO became the Information Commission. We are pleased to bring you concise, insightful coverage from across the region and beyond. Most importantly, we feature a story about

Unwanted Witness's work in nurturing privacy lawyers in East Africa through its privacy moot.

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

(Continued from Page 1)

As the Unwanted Witness Privacy Moot Competition marks its fifth edition, Allan Sempala Kigozi reflects on how a small Ugandan competition became a regional training ground, and why the fight for privacy now runs through our mobile wallets.

A man borrows a small amount of money through an app on his phone. A few weeks later, his mother-in-law receives a call: "The man who married your daughter borrowed money and is refusing to pay." Allan Sempala Kigozi tells the story with a laugh, casting himself as the borrower, but his point is serious. The personal details the borrower provided for verification were turned into a tool for shaming him. "People's character, people's image, people's identity has been tainted because of the misuse of personal data," he says.

That everyday harm sat at the heart of the 5th Unwanted Witness Privacy Moot Court Competition, which ended at Uganda Christian University (UCU) in Mukono with the

hosts lifting the trophy for a second year running.

From only six universities to 48

Unwanted Witness, a civil society organisation founded in 2012 to champion digital rights, started the moot in 2022 as an advocacy tool. Its mission, as Sempala puts it, is "to ensure that whatever right you enjoy offline, you enjoy online as well." The moot was meant to do two things: develop young lawyers who can defend the right to privacy and encourage law schools to start teaching it.

"Not so many universities in East Africa, or even in Africa, teach data protection," he says. "Those who try bundle it under technology or cyber law." Yet, he argues, every other right depends on it and the rest of the law "only makes sense if the right to privacy and data protection is enabled and respected."

The first edition drew six Ugandan universities. By 2023 there were about ten, still all Ugandan. In 2024 the competition crossed into Kenya and around 22 universities took part. This year, 48 universities from Uganda,

Kenya, Tanzania and Rwanda signed up.

We asked him about the rest of the region and learned that it has not been forgotten. South Sudan does not yet have a data protection law, while Burundi and the Democratic

Republic of Congo are francophone jurisdictions, and the moot is still working out how to include them. Somalia has a law and a regulator, but insecurity makes national rounds difficult for now. "We are in the process of involving them," Sempala says.



Allan Sempala Kigozi, Head of Legal and Programs at Unwanted Witness, speaking at the finals of the fifth edition of the Unwanted Witness Privacy Moot. According to Allan, "Privacy is not a myth. It is something we live with." | Photo: Unwanted Witness

A case built from everyday life

Every moot edition is built around a real-life theme. Past problems have tackled surveillance, boda boda and transport apps, elections and digital ID. This year's theme, "Protecting Personal Data in Digital Financial Services and Fintech Ecosystems in East Africa", followed the money.

Mobile money, digital wallets and card payments are fast replacing cash, and every transaction leaves a trail. "While you give money to be transferred, you also give your personal data," Sempala says. Providers say they need it for efficiency or security, "but it goes beyond that."

He is quick to add that Unwanted Witness is not opposed to fintech. "We think, yes, we should go paperless. Fintech should be promoted," he says. "But we should do it in a regulated way, in a way that respects people's privacy and data protection."

The hypothetical case pitted Amani Kato and three others against a digital lender, a telecommunications company and the fictional State of Kisumu. Teams had to argue the lawful basis for processing personal data,

consent in digital environments, automated decision-making and algorithmic profiling, cross-border transfers and the State's duty to protect privacy. Even students who went out early, he believes, will now think twice before tapping "accept" on a loan app.



Students prepare for a moot session during one of the rounds in the competition's fifth edition. | Photo: Unwanted Witness

The road to Mukono

Every team filed written memorials for both the applicant and the respondent. Only the four best-scoring universities from each country made it to the national rounds, held in Dar es Salaam, Nairobi, Kigali and finally Mukono. Four national champions, Uganda Christian University (UCU), Kabarak University, the Independent University of Kigali and the University of Dar es Salaam, went on to the regional finals.

Before a word was argued, there was a quieter moment. Each university planted a tree with the Vice Chancellor in Mukono, a living marker of five years of the moot and of the effort to grow privacy and data protection in East Africa.

Semi-finals began on the morning of 29 September, and the final pitted UCU against the University of Dar es Salaam before a three-judge panel comprising Hon. Justice Duncan Gaswaga, a Judge of the High Court

of Uganda and the African Court on Human and Peoples' Rights, Hon. Justice Geoffrey Kiryabwire, a Justice of the Court of Appeal of Uganda and Brian Kalule, a senior lawyer and Partner at AF Mpanga Advocates, one of Uganda's top tier law firms. UCU, represented by Deborah Namiwanda Mulungi and Vanessa Evelyne Nalukwago, won by just 0.6 points while Dar es Salaam's Rosemary Muchondi was named the best oralist.

For Sempala, UCU won the title long before the oral rounds. "They had top marks in both memorials," he says, and the students who wrote them were the ones on their feet in the final. "If you go back to the YouTube recording, you would agree with me that these girls put up a good show."

With the win, UCU became the first university in the moot's history to defend both its national and regional titles.



Deborah Namiwanda Mulungi and Vanessa Evelyne Nalukwago receive the prize cheque from Hon. Justine Kasule Lumumba, Uganda's Minister for ICT and National Guidance.
| Photo: Unwanted Witness

"Are you from Mars?"

Asked about the biggest privacy risks facing users of mobile money and digital lending platforms, Sempala names three.

The first is weak implementation. Laws and regulators exist, he says, but they lack money, technical capacity and the sector-specific rules that would give the law teeth. Kenya has made the most progress in issuing guidance, while Uganda, Rwanda and Tanzania lag behind. "You can have the law," he says, "but enforcement is also another issue."

The second is us. "You borrow money, you don't read privacy policies," he says. "You are too desperate to get the money."

The third is that law schools do not teach data protection. He wants the ministries responsible for ICT and education to work together on a curriculum that teaches data protection as a right, "from primary level to tertiary institutions." Only then, he says, will lawyers stop asking whether there is money in it and start specialising in it.

He remembers when Unwanted Witness was almost alone. "Everyone was looking at us as if, what are you talking about? Are you from Mars?" Today, with more organisations joining the work, "I think what we were saying, we were not daydreaming." He points to a recent

debate in Parliament on digital number plates in which privacy was raised. "We were clapping our hands."

He compares it to the early days of HIV, when people who fell ill would claim they had been bewitched. Acceptance and awareness changed that, and people began living longer. "I think the same thing with privacy," he says. "If we consistently do this, people will be aware."

Where the mooters go

The moot's impact is starting to show in careers. At this year's finale, the finalists received appointment letters for placements with Uganda's Personal Data Protection Office. In Kenya, former mooters now work at the Office of the Data Protection Commissioner. Others describe themselves on LinkedIn as data protection consultants, and every year more finalists write their dissertations on data protection. "That has never happened," Sempala says. "I think that's an impact. It's a milestone."

He sees the moot as a training ground for future Data Protection Officers, human rights activists, academics and practitioners, and he urges organisations to recruit beyond the winners. "From the national rounds, Uganda was more competitive than any other."



Martin Kityo of the Compliance and Investigations Department at the Personal Data Protection Office serves as a judge during the semi-finals. Kityo is a former mooter who was named best oralist in the second edition of the moot. | Photo: Unwanted Witness

A word to next year's cohort

Asked what advice he had for students considering the sixth edition, he advised them to start with the writing. Written and oral marks are averaged, so even brilliant oralists cannot compensate for a weak memorial. Research deeply, he says, and give the

memorial the time it deserves.

And to those still wondering whether privacy is worth a career, he offers an invitation rather than a warning. "It's a good field of law. Not so many people have come into it. It's still fresh," he says. "And yet we are already living in the future."

East Africa

Uganda

Data Protection Complaint Filed Against Uber Following Its Exit from the Ugandan Market

On 2nd September 2026, Uber ended its ride-hailing operations in Uganda and Nigeria, citing a "thorough review" of its business and closing a decade-long presence in Kampala. Drivers and riders were given a 21-day support window. The exit quickly raised questions about the fate of the personal data Uber collected from Ugandan users, including national identity details, driving permits, police clearance letters, photographs, trip logs and location histories.

Following concerns formally raised with the Personal Data Protection Office (PDPO) by activist Lutaaya Godfrey, Tecnolegal Advisory Centre UG and DPO Privacy Centre (East Africa), the PDPO confirmed on 11 September 2026 that it had engaged Uber regarding its obligations for the personal data collected during its operations, and that a follow-up assessment would review any outstanding compliance issues. At the heart of the matter is the storage limitation principle under Section 18 of the Data Protection and Privacy Act, Cap. 97, which bars the retention of personal data beyond the period necessary for its purpose unless retention is required by law, contract or the data subject's consent. Uber reportedly retains some user data for up to seven years for tax, insurance and legal purposes, and it remains unclear whether the Ugandan datasets will be deleted or archived.

Data Protection Regulator Issues Decisions on Deletion of Data and Disclosure of Birth Records

In September 2026, the Personal Data Protection Office (PDPO) delivered two decisions clarifying the rights to deletion and rectification under the Data Protection and Privacy Act, Cap. 97 and the Data Protection and Privacy Regulations, 2021.

In **Lilian Namagembe v Teach For Uganda & Another (Complaint No. PDPO 066/2025)**, the complainant applied for a job with Teach For Uganda, whose recruitment agent, NFT Consult, collected her TIN, NIN, academic transcripts and fingerprints for background checks. When her conditional offer was withdrawn over an alleged undisclosed conflict of interest, she asked both organisations to delete her data, but received no response until the PDPO issued notices and referred the matter to the Criminal Investigations Directorate. In its decision of 8th September 2026, the PDPO found that her data had eventually been deleted, but that the respondents breached Regulation 29(2), read with Sections 16(2) and 16(5) of the Act, by failing to decide on her request within seven days and to notify her of the action taken. The Office noted that the purpose for holding her data ended with the recruitment process. The respondents were cautioned to respond to future requests within the prescribed time, and the Office pointed out that any claim for compensation lies with the

courts under Section 33.

In **Joseline Twemanye v St. Francis Hospital Nsambya (Complaint No. PDPO 120/2025)**, the complainant alleged that the hospital unlawfully disclosed her Birth Notification Record, which named a man other than the father on her birth certificate, to her mother's lawyers, who later relied on it in a dispute over her late father's estate. She also alleged that the hospital refused to rectify the record. In its decision of 7th September 2026, the PDPO dismissed the complaint. It held that disclosure to the registered mother, a verified

co-data subject whose own personal data forms part of the same record, was reasonable under Section 24 of the Data Protection and Privacy Act, and that the later use of the record in succession proceedings was a separate act. On rectification, the Office held that the right arises only once inaccuracy is proved; the hospital's contemporaneous 1983 birth register outweighed later documents, and receipt of the rectification notice was not established. The Office stressed that it was not determining the complainant's parentage or inheritance.

Kenya

Data Protection Regulator Releases Draft Public Notice on the Prescription of Additional Categories of Sensitive Personal Data

On 11th September 2026, the Office of the Data Protection Commissioner (ODPC) published, for public consultation, a draft Public Notice prescribing additional categories of sensitive personal data under Section 47 of the Data Protection Act, 2019. Section 47 empowers the Data Commissioner to designate further types of personal data as sensitive, beyond those already listed in the Act, such as race, health status, ethnic social origin, conscience, belief, genetic and biometric data, property details, marital status, family details, sex and sexual orientation. Once finalised, data in the new categories will attract the stricter processing conditions that apply to sensitive personal data, including the requirement under Section 49 of the Act that it may only be transferred outside Kenya with the data subject's consent and on confirmation of appropriate safeguards. The proposed categories are political affiliation and trade union membership. The deadline for submission of comments closed on 25th September 2026, and we await further updates from the ODPC.

Data Protection Regulator Publishes New Guidance Notes for Cross-Border Data Transfers

On 8th September 2026, the ODPC published its Guidance Notes for Cross-Border Data Transfers. The Guidance provides Kenyan standard contractual clauses for controller-to-controller and controller-to-processor transfers, sets out an approval process for Binding Corporate Rules, and requires a documented transfer impact assessment before the standard clauses are relied on.

Notably, the Guidance treats remote access to data from outside Kenya and the use of cloud servers located abroad as cross-border transfers, and suggests that hosting data on foreign cloud servers for efficiency may be justified by a "compelling legitimate interest." Onward transfers require prior written authorisation, while onward transfers for the recipient's own purposes, such as analytics, profiling or marketing, are prohibited. The Guidance also restates that processing for specified strategic interests of the State, including civil registration, elections, public finance, basic education, and primary and secondary healthcare, must take place through a server or data centre located in Kenya. (Source: Covington)

Across Africa

Zimbabwe

Postal and Telecommunications Regulatory Authority Kicks Off Mandatory On-Site Compliance Inspections

From 1st September 2026, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), acting as the Data Protection Authority, began compliance inspections under the Cyber and Data Protection Act, as announced in its Regulatory Notice 2 of 2026. Taking a risk-based approach, POTRAZ is prioritising sectors that hold large volumes of sensitive data: financial institutions, insurers, local authorities, healthcare providers, mining companies,

religious organisations, schools, universities, professional bodies, government ministries and NGOs.

Inspectors are checking whether organisations hold a Data Controller Licence and have appointed a certified Data Protection Officer, as required by the Licensing of Data Controllers and Appointment of Data Protection Officers Regulations (S.I. 155 of 2024), whose registration deadline passed in March 2025. Processing personal data without a licence attracts a level 11 fine, imprisonment of up to seven years, or both. (Source: The Herald; Veritas)

ECOWAS

ECOWAS Advances Its Landmark Revision of the Supplementary Act on Personal Data Protection

The ECOWAS Authority of Heads of State and Government adopted the revision of Supplementary Act A/SA.1/01/10 on Personal Data Protection at its 69th Ordinary Session held in Lungi, Sierra Leone, on 19th July 2026, replacing the 2010 framework. The adopted text is awaiting publication in the ECOWAS Official Journal.

Based on the Commission's draft, the revised

Act extends to controllers outside the region that target individuals in ECOWAS, requires parental consent for children's data in online services, introduces rights to portability and restriction, and mandates records of processing, impact assessments, breach notification within 72 hours and independent Data Protection Officers. Fines could reach 5% of annual turnover, and a West African Data Protection Authorities Network (WADPAN) would be established. Member States would have up to three years to align their national laws once the Act enters into force. (Source: AME Legal Conseils)

Togo

Togo's Personal Data Protection Authority Rallies 33 Ministries in a Public Sector Compliance Drive

On 15th September 2026, Togo's Instance de Protection des Données à Caractère Personnel (IPDCP) brought together 33 ministries and State institutions in Lomé to explain their obligations under the country's 2019 data protection law. The authority urged each ministry and institution to designate a data protection correspondent in every directorate, inventory the personal data files it holds, and secure its processing, particularly for civil

registration, health, tax and social programme data.

The IPDCP's Head of Compliance, Bialabna Abaloutou, said data protection is both a matter of digital sovereignty and of trust, while IPDCP President Bédiani Béléi said the authority will prioritise support and dialogue over sanctions as institutions move towards compliance. The session forms part of a months-long awareness campaign targeting public and private actors. (Source: Le Nouveau Reporter)

Africa

African Data Protection Authorities Celebrate the Inaugural Africa Data Protection Day

On 21st September 2026, data protection authorities across the continent marked the first Africa Data Protection Day, declared by the Board of the Network of African Data Protection Authorities (NADPA) under the

theme "Protecting data, building trust, powering Africa's digital future." NADPA called on governments, regulators, businesses, civil society, innovators and citizens to raise awareness, strengthen data protection, build privacy into emerging technologies including AI, and cooperate on cross-border data flows, in line with the African Union's Malabo Convention. (Source: Veritas)

Global Privacy Watch

European Union

Data Act "Access-by-Design" Obligation and Cyber Resilience Act Reporting Duties Take Effect

Two pillars of the EU's digital strategy reached binding milestones in September 2026. From 12th September, the access-by-design

requirement under Article 3(1) of the EU Data Act applies to connected products and related services placed on the EU market. Manufacturers must design products such as smart appliances, wearables, vehicles and industrial machinery so that the data they generate is, where relevant and technically

feasible, directly accessible to users by default, easily, securely, free of charge and in a machine-readable format.

A day earlier, on 11th September, the first obligations under the Cyber Resilience Act took effect. Manufacturers of products with digital elements, including products already on the market, must now report actively exploited

vulnerabilities and severe security incidents through ENISA's Single Reporting Platform, with an early warning within 24 hours, a notification within 72 hours, and a final report thereafter. Non-compliance can attract fines of up to €15 million or 2.5% of worldwide annual turnover. (Source: Matheson; Jones Day)

Ireland



Ireland Fines Google €403 Million Over Location Data

On 21st September 2026, Ireland's Data Protection Commission (DPC) fined Google €403 million after finding that it unlawfully and unfairly processed users' location data

through its Web & App Activity, Location History and Location Accuracy settings between May 2018 and February 2020. The inquiry began in 2020 following complaints coordinated by the European Consumer Organisation (BEUC) on behalf of consumer groups in eight countries. Google has six months to bring its processing into compliance.

Deputy Commissioner Graham Doyle warned that users may have been "unaware that their location was being used to, for example, influence them with ads." Google said the case concerns historical policies it has since changed, including auto-deletion of location data and on-device storage of Timeline data. BEUC's Director General, Agustín Reyna, remarked that "late enforcement can be as harmful as no enforcement at all." (Source: The Irish Times)

United Kingdom

The Information Commissioner's Office (ICO) Becomes the Information Commission

On 30 September 2026, the Information Commissioner's Office formally became the Information Commission, as provided for by the Data (Use and Access) Act 2025. The change ends the regulator's "corporation sole" model, under which all legal powers were

vested in a single Information Commissioner, and replaces it with a corporate body governed by a board with seven newly appointed non-executive members. The regulator's functions and responsibilities remain unchanged, and it will continue to be known as the ICO. Organisations should, however, update references to the regulator in their privacy notices and policies. (Source: ICO)

China

Simplified Personal Information Protection Measures for Small-Scale Processors Take Effect

On 1st September 2026, the Provisions on Simplified Personal Information Protection Measures for Small-Scale Personal Information Processors, issued by the Cyberspace Administration of China and the Ministry of Public Security, came into force. The Provisions apply to organisations processing the personal information of fewer than 100,000 individuals, regardless of their size or revenue.

Qualifying processors may meet notice obligations through a published privacy notice, rely on simplified templates for impact assessments and self-assessment audits, and conduct compliance audits once every five years instead of every two. Consent is not required where individuals voluntarily provide data needed for a product or service, but sensitive personal information still requires separate consent, and the relief does not apply where data is shared with third parties or publicly disclosed. (Source: Reed Smith)

United States

California's Data Broker Deletion Platform Enters Its First Enforcement Cycles

Under California's Delete Act, consumers have since January 2026 been able to submit a single deletion request to all registered data brokers through the Delete Request and Opt-Out Platform (DROP), operated by the California Privacy Protection Agency. Since 1st

August 2026, data brokers have been required to access DROP at least once every 45 days to retrieve and process these requests and to report the status of each request within 45 days. By September, brokers were working through their first mandatory processing cycles. Non-compliance attracts a penalty of \$200 per request for each day of non-compliance. (Source: Alston & Bird)

DID YOU KNOW?

Unlike regulators in Kenya, Nigeria and the European Union, Uganda's Personal Data Protection Office cannot impose administrative fines. In its September 2026 decision in *Joseline Twemanye v St. Francis Hospital Nsambya*, the Office confirmed that the only fines contemplated under the Data Protection and Privacy Act, Cap. 97 are penal fines imposed by a court upon conviction, and that claims for compensation under Section 33 must likewise be brought before a court.



About DPO Privacy Centre (East Africa)

DPO Privacy Centre (East Africa) is a regional hub that supports Data Protection Officers, legal practitioners, and organisations across East Africa in navigating data privacy compliance. Our work includes advocacy, policy development and training. Our aim is to foster a culture of privacy and enrich privacy discussions across East Africa.

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

substack.com/@privacycentreea 

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

info@dpoprivacycentre.com 

Follow us on X and LinkedIn:

[DPO Privacy Centre East Africa](#)  

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

© DPO Privacy Centre (East Africa) 2026