Technology

New study exposes data protection challenges in Uganda

DEVON SSUUBI

In Uganda, most companies and government agencies face challenges in implementing privacy policies and security measures to protect the data of users.

This is the key finding from the recently-released 2023 privacy scorecard report by Unwanted Witness Uganda, a leading digital rights organization. The report, released at Hotel Africana on February 29, highlights that there is also low public awareness of privacy rights, which poses a significant threat to the public as this increases the risks of personal data misuse, breaches and unauthorized surveillance.

Freda Nalumansi-Mugambe, the head of Research at Unwanted Witness, revealed varying performances across different sectors which leave a lot to be desired in terms of user's protection in case of any data breaches.

"There is generally limited understanding of data protection and privacy legislation that exists in the country. There is insufficient regulatory capacities, resource constraints, weak accountability culture, rapid technological changes, low public awareness, and political associations in the different jurisdictions," she said.

The survey was conducted in 2023 between the months of January and September and involved the assessment of 48 companies across four countries which included Kenya, Mauritius, Zimbabwe and Uganda. The companies were drawn from six sectors, including e-commerce, financial services, telecommunications, digital services, online betting, and e-government. Each country had two companies per sector assessed, resulting in a total of 12 companies per sector across the four countries.

POSITIVES

According to the report, selected sectors in Uganda demonstrated strong performances in existence of an accessible and noticeable privacy policies indicator, with telecom companies Lyca Mobile and MTN having the highest average score of 100%. Financial services such as Stanbic bank and Pride microfinance also showed robust performance in this aspect, scoring 100%.

Unwanted Witness' Allan Sempala Kigozi (L) chats with a guest at the event

E-commerce companies, including Jiji and Jumia Uganda, the online betting sector with Fortbet and one X bet, digital services companies like Mangu cash and Dave cash all performed well in the privacy policy indictor. When it comes to E-government, the Directorate of Citizenship & Immigration Control (DCIC) and National Identification & Registration Authority (NIRA) exceedingly performed well in the availability of accessible privacy policy indicator.

FLIPSIDE

However, the report reveals that these sectors face significant challenges when it comes to data protection practices which not only jeopardize the security and privacy of individuals' information but also undermines trust and accountability within organizations such as financial losses reputation damage and legal implications. This underscores the importance of addressing gaps in data protection practices and enhancing regulatory

According to the report, DCIC and NIRA scored poorly in accountability, availability of internal redress mechanisms for data breaches and data collection and third-party data transfers. These agencies being responsible for storing sensitive biometric information for Ugandans, inadequate data protection measures could lead to unauthorized access exposing sensitive personal information of Ugandans to malicious actors, on the other hand this could undermine public trust in government institutions. This inconsistency in performance highlights the need for improved data protection practices and accountability measures within these government sectors.

Telecoms, financial services and digital services face challenges as well in areas of such as accountability data security, informed consent and internal redress mechanism for those breaches performed poorly as well in term of the indicator on robust data security

Allan Sempala Kigozi, the head of Legal and Programmes at Unwanted Witness, noted that inadequate data protection measures can lead to a range of risks and consequences, including increased vulnerability to data breaches, identity theft and cyber-attacks.

"The lack of robust data protection measures can expose sensitive data to unauthorized access, leading to privacy violations and potential misuse of personal information," he said.

Kigozi adds that companies should clearly outline in their privacy policies, how they handle data breaches and what mechanisms they have in place to mitigate their impacts.

"When information goes out and there is no mechanism to address that breach, it puts the owner at a risk because it can be used by anyone. The law requires companies to have such mechanisms."

The report comes at a time when the rapid growth of digital services and the extensive adoption of technologies has led to massive increase in the number of cybercrimes every day that passes, which creates a gap between existing data protection legislation and its practical implementation. This remains a challenge among many companies and raises concerns around the capacity and resources of data protection offices tasked with ensuring compliance.

According to 2022/2023 Annual police report released recently, there was an increase in cases of cybercrimes by fraudsters. The police report revealed that this was orchestrated by people pretending to be from telecommunication networks who could call victims and take their money on the accounts through false pretence. "Scammers use the internet to reach potential victims and obtain their personal data and use it to steal money," noted the police report. Matters are not helped that most victims suffer quietly without reporting such cases to the police.

It was further noted that in the same year, hackers infiltrated the Airtel mobile wallet, a platform for banking transactions, and siphoned out large amounts of money believed to be between Shs 30bn and 50bn.

However, Airtel management stated the incident has had no impact on any balances on mobile money accounts and that customers continue to enjoy all other mobile money services uninterrupted.

For one, Gabriel Buule, a social media user, said he used is X handle to narrate how he experienced unauthorized withdrawals from his Airtel mobile wallet without him initiating any transactions or entering a PIN. He discovered that an Airtel app was registered under his number without his knowledge, and despite notifying customer care, he did not receive help. The customer care informed him that someone had opened an Airtel app with his number and was able to withdraw money from his account without his consent

Amidst the increasing fraud cases, Kigozi states that companies and government agencies should aim at Implementing transparent and accountable data practices aligned with national legislation to demonstrate commitment beyond passive privacy policies in order to protect users. "Companies should publish detailed privacy policies that offer exhaustive inventories of data types rather than vague summaries, outlining specific retention periods tailored to different categories of user information instead of indefinite storage, describing the security protections in place comprehensively, and establishing functional mechanisms for users to submit access, correction, or deletion requests and obtain remedies" said Kigozi.

These recommendations aim to enhance data protection practices, improve transparency, and accountability, ultimately ensuring that data subjects' rights are respected and protected effectively.