CM ADVOCATES LLP

Insights on the Regulation of Telecommunication Service Subscribers' Data in Kenya

Kenya is home to a highly vibrant telecommunications industry. In recent decades, the sector has grown significantly into a complex and digitised ecosystem that is responsible not only for connectivity but also mobile financial services.

According to a recent Communication Authority of Kenya ("CAK") report the total mobile subscriptions in the country stood at 78.4 million.

This high uptake reflects a deep integration of mobile services into everyday life of Kenyans.

Telecommunication operators utilize subscribers' data to facilitate an array of services such as mobile money transfers, e-commerce, e-government services and social connectivity.

It is against this backdrop that there exists a robust framework on the legal and regulatory requirements governing such subscriber data.

Legal and Regulatory Underpinnings

- **The Constitution of Kenya, 2010**

The primary force behind the regulation of subscribers' data in the modern digital ecosystem is Article 31 (c) and (d) of the Constitution of Kenya, which guarantees every citizen the right to privacy, specifically the right not to have their private communications intercepted or their person, home, or property searched unnecessarily.

To operationalize this fundamental right in an increasingly digitised world, some core statutes enacted by Kenya's parliament provide key legislative anchors.

- **Data Protection Act, Cap. 411C**

Enacted in 2019, the Data Protection Act ("DPA") serves as the primary pillar of Kenya's data governance regime.

The Act gives effect to Article 31(c) and (d) of the Constitution by regulating the collection, processing, storage, security and disclosure of personal data.

Among its salient features is the provision for registration of data controllers (persons who determine the means and purpose of processing personal data) and data processors (persons who process personal data on behalf of controllers).

This implies that all telecommunication operators must register with the Office of the Data Protection Commissioner ("ODPC") accordingly.

Furthermore, the DPA outlines the foremost principles of lawful personal data processing such as data minimization, data privacy, transparency, accountability, purpose limitation and storage limitation.

Additionally, the DPA provides for data subject rights such the right to be informed on data use, right of access, right to rectification, right to data portability and the right to accuracy.

When subscribers' (data subjects) rights are violated, they can lodge complaints with the ODPC which is the regulator established under the DPA to oversee data compliance in all sectors including the telecommunications sector.

- **Kenya Information and Communication Act, Cap. 411A ("KICA")**

KICA is another piece of legislation that places emphasis on data protection for the licensed telecommunication service providers.

Section 23 of KICA states that the Communications Authority of Kenya ("CAK") must ensure that the personal data of subscribers is processed in line with the principles of data protection.

To complement KICA's provisions, further protection mechanisms are afforded under the Kenya Information and Communications (Registration of Telecommunications Service Subscribers) Regulations 2025. (the "Regulations").

These Regulations state that a telecommunications operator shall take all reasonable steps to guarantee the security and confidentiality of its subscribers' personal data and registration particulars in accordance with the DPA.

The Regulations also posit that operators must report to CAK on the strategies put in place to ensure the security and confidentiality of their subscribers' particulars. Additionally, the right to data accuracy is also emphasized under the Regulations.

- **The Computer Misuse and Cybercrimes Act, Cap. 79C**

The Computer Misuse and Cybercrimes Act provide an enforcement framework for the digital security subscribers' information and data.

It provides for the protection of critical information infrastructure and data and provide a legal basis for prosecuting offences against computer systems such as hacking and identity theft.

The Act also criminalizes unauthorized access to computer systems and the unlawful interception of electronic data, which may belong to subscribers of telecommunication services.

- **ODPC Guidance Note for the Communications Sector**

In December 2023, the ODPC published the Guidance Note for the Communication Sector which applies to telecommunication service operators processing personal data.

The Guidance Note provides considerations that must be present when the personal data, location, geographical data and the network traffic of subscribers is processed.

The Guidance Note reinforces that data protection in the sector must be anchored on the fundamental tenets of the DPA such as consent, contractual bases, legitimate interest and public interest among others.

As such, processing is not automatic and has to be justified in every instance. Other key obligations that can be deciphered from the Guidance Note include mandatory registration with the ODPC, inculcation of privacy by design, data protection impact assessments and breach notifications as may be necessary.

CONCLUSION - ENFORCEMENT TRENDS

The telecommunications sector is slowly becoming a notable source of complaints before the ODPC. One example that fits the context of this discussion is *Alston v Liquid Telecommunications Kenya Limited (2025)* where the complainant alleged that his personal data was recorded by the data controller without consent (Liquid Telecommunications) who subsequently failed to fulfill his right of erasure.

The ODPC observed that a data controller's legitimate interest in preserving evidence for legal defense does not override a data subject's right to privacy when transparency is lacking. It further ruled that the Liquid Telecommunications violated the principle of purpose limitation as the data subject was never informed that their data recording would be repurposed for legal proceedings.

HOW CM ADVOCATES LLP CAN ASSIST

Our Technology, Media & Telecommunications (TMT), Data Protection & Cybersecurity Practice provides:

- **End-to-end regulatory compliance advisory** - alignment with the Data Protection Act, Kenya Information and Communications Act, and sector-specific guidance, with a focus on lawful processing, consent frameworks and privacy by design.
- **Telecommunications data governance and risk management** - drafting and review of data processing agreements, structuring lawful data use (including mobile money and subscriber data) and advising on data protection impact assessments and breach response.
- **Regulatory engagement and enforcement defence** - representation and advisory in matters before theODPC, including investigations, complaints, and dispute resolution in line with emerging enforcement trends.

CONTACT US!

At CM Advocates LLP, we provide stakeholders in the telecommunications sector with tailored advice and compliance support in line with the requisite regulatory frameworks. For further guidance or assistance in navigating the relevant data protection laws within the telecommunications sector, please contact our Technology, Media & Telecommunications (TMT), Data Protection & Cybersecurity Practice at law@cmadvocates.com or the contributors below.

CONTRIBUTORS

Brandon Otieno
Senior Associate
Email: botieno@cmadvocates.com
CM Advocates LLP

Mujahid Mithwani
Legal Trainee
Email: mmithwani@cmadvocates.com
CM Advocates LLP