PwC Kenya Legal Bulletin

Beyond the Tick Box: Rethinking Consent as a Lawful Basis in Data Protection and Privacy Compliance

September 2025 Edition

Legal Bulletin

Welcome to the September 2025 edition of the PwC Kenya Legal Business Solutions Bulletin. In this issue, we focus on a critical facet of data protection and privacy - consent as a lawful basis for processing personal data under Kenya's Data Protection Act, 2019 (the "Act").

With growing regulatory scrutiny from the Office of the Data Protection Commissioner (the "ODPC") and rising public awareness, it is time for organisations to move beyond "tick box" consent and rethink how consent operates as a lawful basis for personal data processing. Sharp consent management practices are no longer a nice-to-have; they are business imperative.

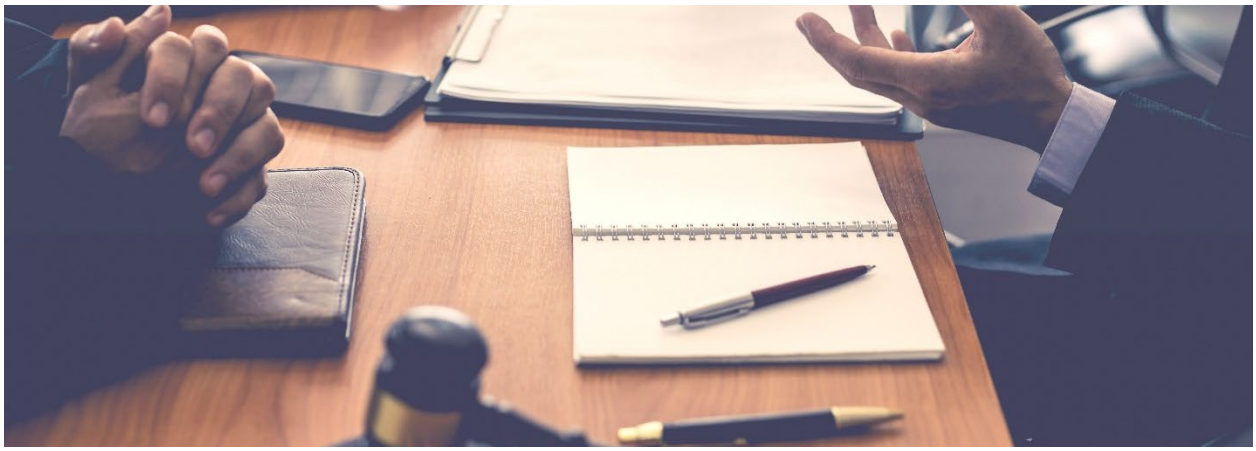
In this bulletin, we outline key legal considerations and enforcement trends shaping consent-based data processing in Kenya.

Why Consent Matters

Consent is not just a legal formality; it is a cornerstone of responsible personal data handling. It is recognized under the Act as a lawful basis for processing personal data, but only when it meets strict criteria; as will be discussed in this bulletin.

Moreover, in today's data-driven environment, data subjects expect transparency. Data subjects want to know how their information will be used. In the ODPC's Guidance Note on Consent, the ODPC also mandates that data controllers and processors not only obtain consent but also provide clear evidence that this consent aligns with legal requirements and respects data subjects' rights.

In addition to this, when viewed through a strategic lens, consent becomes a powerful business asset. Properly managed, consent fosters trust, strengthens customer/client loyalty, and enhances brand reputation. Organisations that embed transparent, respectful consent processes minimize regulatory risks and differentiate themselves in increasingly competitive markets.



Understanding Consent as a Lawful Basis

The Act elaborates that consent must be express, unequivocal, informed, specific, freely given and actively affirmed by the data subject. Passive or implied acceptance or consent buried in lengthy, unread terms and conditions does not constitute meaningful consent.
This means that valid consent requires a deliberate, affirmative action from the data subject, whether it is ticking a box, signing a form, or giving recorded verbal approval. Additionally, consent must be voluntary. Tying consent to non-essential services or contract terms undermines its validity and can result in legal challenges. Notably, ambiguous or overly broad consent exposes your business to risk as it leaves too much to interpretation.

Transparency is non-negotiable. Data subjects need to know exactly who is processing their personal data, why it is needed, how it will be used and who it will be shared with. Equally important is informing them of their rights and the straightforward process to withdraw consent at any time.

Finally, as personal data practices evolve, so must consent. Any expansion or change in processing purposes demands fresh consent, ensuring ongoing compliance and maintaining data subjects' trust.

Lastly, for consent to serve as a lawful basis for data processing, it must meet key legal conditions under the Act, which include:

a) data controllers and processors must be able to demonstrate that consent was clearly and freely given by the data subject for a specific purpose;

b) data subjects have the right to withdraw their consent at any time, and this withdrawal must be effected without delay;

c) while processing of personal data pre-withdrawal remains lawful, continued processing after withdrawal is not; and

d) consent is not valid if access to a service is made conditional on agreeing to share personal data that is not necessary for that service.

Consent in Practice: Where it is non-negotiable.

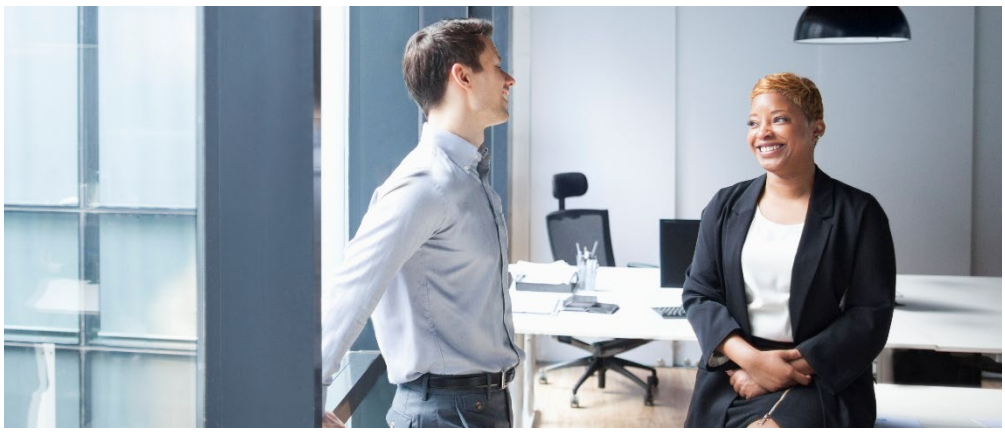
There are specific scenarios where consent is not just recommended; it is legally required. These include:

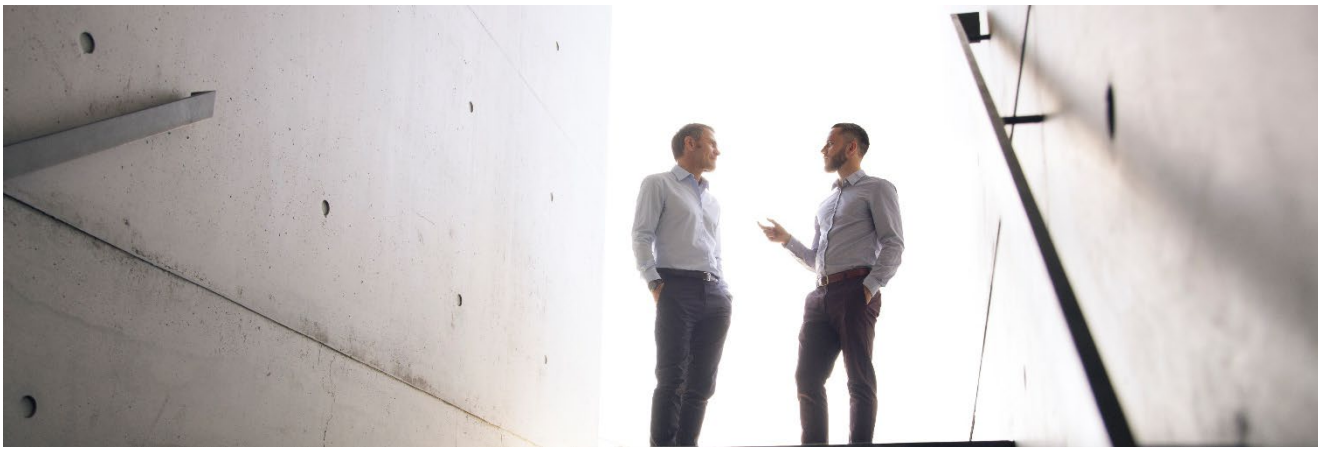
a) during direct marketing and profiling activities, where consent must be explicit and informed ;

b) processing of children's data, which requires verifiable consent from a parent or legal guardian ;

c) processing sensitive personal data, such as health, biometric, religious, or sexual orientation information, which demands heightened protection ; and

d) during cross-border data transfers, particularly involving sensitive data, where both explicit consent and ODPC approval are mandatory .





[1]Regulation 15(1)(c) of the Data Protection (General) Regulations

[2]Section 13(1)(a) of the Data Protection Act 2019

[3]Regulation 15(1)(c) of the Data Protection (General) Regulations

[4]Section 49(1) of the Data Protection Act 2019

Regulatory Lens: Enforcement and Trends

In the recent past, the ODPC has signalled that it will closely scrutinize consent practices. Enforcement trends include the following weaknesses:

a) consent obtained through bundling (such as forcing customers to agree to unnecessary processing);

b) inducements that compromise freedom of choice;

c) lack of transparency around cross-border transfers; and

d) failure to provide easy withdrawal mechanisms.

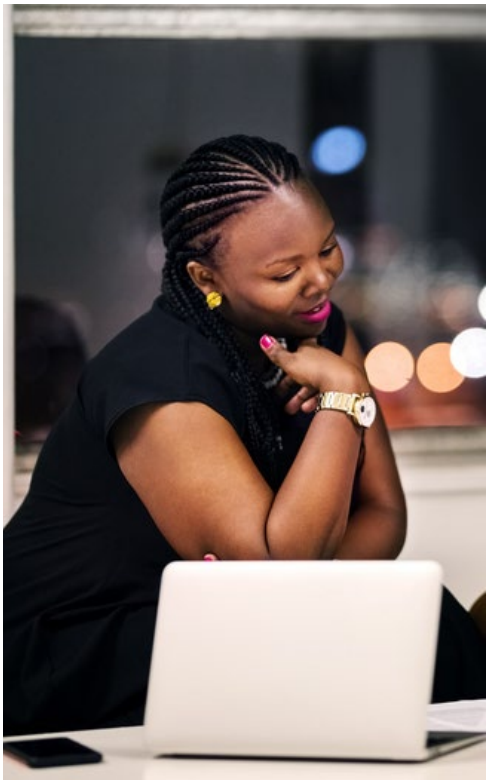
From ODPC audits, complaints, and guidance, organizations should expect scrutiny of consent practices around:

a) whether data subjects were clearly informed of who collects their data and why;

b) how records of consent are kept and managed;

c) whether withdrawal mechanisms are accessible, simple, and effective; and

d) if consent is being relied upon in contexts where another lawful basis may be more appropriate.



Recently, a data handler was found liable in a class-action lawsuit over the handling of data from a Health app that tracked female menstruation cycles and was used by women worldwide. The app had assured users that their sensitive reproductive health information and survey questions would not be disclosed.

However, the app shared this sensitive data with third party search engines and online social media apps through their respective online ad-related tools known as software development kits (SDKs) that enabled analytics and advertising. Although the data handler claimed its policies prohibit developers from sending sensitive data, the California jury held it liable, ruling that consent obtained was neither informed nor explicit.

Additionally, an online retailer was fined by Luxembourg's data protection authority, Commission Nationale pour la Protection des Données (CNPD) for processing personal data for targeted advertising without obtaining valid consent under the General Data Protection Regulation (GDPR). The online retailer had relied on "legitimate interest" as its lawful basis for data processing, but the regulator held that targeted advertising requires explicit consent.

The CNPD further found that the retailer failed to provide sufficient transparency about its data practices and did not adequately address user rights requests. Although the retailer argued that the interpretation of GDPR provisions was subjective and lodged an appeal, the Luxembourg Administrative Court upheld the penalty.

“Consent or Pay” and Power Imbalance

While not formally recognized under the Act, the "consent or pay" model is a prominent topic in global privacy debates. Businesses are using consent or pay to balance ad revenue with privacy obligations. However, the Act requires that consent be freely given, meaning individuals should not be penalized for refusing consent. When individuals are required to "pay," such as by surrendering their personal data to access services otherwise available without charge, genuine freedom of consent may be compromised.

Regulatory guidance from bodies such as the European Data Protection Board (EDPB) and the UK Information Commissioner's Office (ICO) asserts that any power imbalance between businesses and consumers undermines the validity of "consent or pay" models for data processing, as it impedes a truly voluntary choice between consenting to data use or paying a fee. For business to lawfully implement, a "consent or pay" framework, they must ensure there is no power imbalance, impose fees that are reasonable, provide equivalent services for paying users, and be structured in accordance with established privacy principles.

Compliance Checklist: Building Trust Through Consent

To align with the ODPC expectations and build data subjects’ trust, data controllers and processors should:

a) notify the data subjects by disclosing the purpose of collecting personal, scope, and their right to withdraw consent;

b) use plain language in consent forms;

c) avoid relying on consent where contractual or legal obligations already apply;

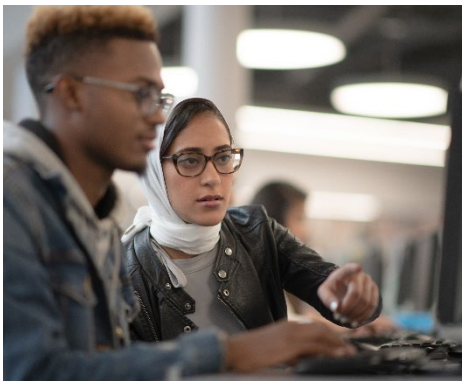
d) Leverage on consent management tools to keep an audit trail that includes records of when, how, and for what consent was obtained;

e) conduct regular staff trainings on consent requirements under the Act;

f) ensure the third parties they are working with are bound by data protection laws and regulations;

g) establish a rapid reporting and mitigation protocol for any suspected data breach to limit legal and reputational harm; and

h) regularly review and refresh consent where processing activities evolve.



Did You Know?

- Consent must be as easy to withdraw as it is to give. This means businesses cannot bury withdrawal mechanisms in lengthy policies, or make customers jump through hoops to opt out. If consent was obtained with a single click or simple signature, withdrawal must be equally straightforward. For instance, if you run digital campaigns, a working “unsubscribe” button is may be legally required. Therefore, data controllers and processors should design frictionless withdrawal processes that respect customer choice while maintaining a positive brand experience.

- Generic signage/notices may no longer meet the legal threshold for valid consent under Kenya’s Data Protection Act. The ODPC has made it clear that consent must be explicit, informed, and demonstrable. In 2023, a Kenyan restaurant was fined KES 1.85 million for posting a patron’s image online without proper consent, despite having general signage. Similarly, a school was fined KES 4.55 million for publishing images of minors without parental consent. These rulings confirm that implied consent through signage is insufficient; organizations must implement lawful consent mechanisms or risk penalties. In a recent determination (ODPC Complaint No. 0280 of 2024), the ODPC found a healthcare provider in breach of the data protection law after placing a patient’s sensitive medical details outside the packaging of prescribed medication. This meant third parties could easily access the information. The ODPC held that health data is highly sensitive and cannot be disclosed or processed without the patient’s explicit, informed, and specific consent.

- The ODPC has enforcement powers with real business impact. The ODPC has the authority to impose penalties of up to KES 5 million or 1% of an organization’s annual turnover (whichever is lower) for violations of the Act. Where no specific penalty is provided, offenders may face fines of up to KES 3 million, imprisonment for up to 10 years, or both. In addition to financial penalties, the ODPC may order compensation for affected individuals or seek court-issued preservation orders to prevent data loss or tampering,

Contact us

Titus Mukora
Partner,
Legal Business Solutions
+254 20 285 5000
titus.mukora@pwc.com

Caroline Wanja
Associate Director,
Legal Business Solutions
+254 20 285 5000
caroline.wanja@pwc.com

Herbert Njoroge
Manager,
Legal Business Solutions
+254 20 285 5000
herbert.njoroge@pwc.com

Tracy Odipo
Manager,
Legal Business Solutions
+254 20 285 5000
tracy.odipo@pwc.com

www.pwc.com/ke