Do you want to transfer personal data out of Kenya? If so, you've come to the right place.
Through its Data Protection Act, 2019 and subsequent regulations, Kenya has established a framework to safeguard the privacy rights of its citizens and ensure compliance with global data protection standards. This article delves into the complexities of cross-border data transfers from Kenya, offering insights and practical guidance on navigating the intricacies of the Data Protection Act.

Key requirements for lawful data transfers

Before embarking on any cross-border data transfer, data controllers and processors in Kenya must diligently adhere to the stringent requirements outlined in the Data Protection Act, 2019.
These requirements form the foundation for lawful and ethical data transfers:

- Proof of adequate safeguards (Section 63): The cornerstone of lawful data transfers is the provision of adequate safeguards. Before transferring personal data outside Kenya, data controllers and processors must furnish the Office of the Data Protection Commissioner (ODPC) with evidence of the protective measures in place. These safeguards encompass a range of technical and organisational measures, including:
    - Technical security measures: Encryption protocols, access controls, and other technological safeguards that prevent unauthorised access, data and data breachesnsure the confidentiality, integrity, and availability of personal data.
    - Data handling policies: Clear, transparent, and readily available policies outlining data retention periods, data deletion procedures, and anonymisation practices.
- Legal framework of the recipient country: A demonstration that the recipient country boasts adequate data protection laws or has implemented suitable safeguards through binding agreements like SCCs or BCRs. These mechanisms ensure that personal data remains

protected even when transferred to jurisdictions with potentially less stringent privacy regulations.

- Explicit consent for sensitive data (Section 35): Sensitive personal data, which encompasses a broad spectrum of information related to race, health, religion, political opinions, sexual orientation, and more, requires explicit and informed consent from the data subject before being transferred outside Kenya. This underscores the significance of transparency and obtaining clear, unambiguous and explicit consent from individuals, empowering them to make informed decisions about their personal data.

Navigating diverse transfer scenarios

Kenya's data protection framework recognises the diversity of data protection regimes across different countries, necessitating nuanced approaches for various transfer scenarios as outlined in the Data Protection (General) Regulations, 2021.

Transfers to countries with adequate data protection (Regulation 21)

Data transfers to countries deemed by the ODPC to have data protection laws equivalent to Kenya's are generally permissible, subject to providing proof of adequate safeguards. This provision streamlines the process for transfers to jurisdictions with robust privacy protections, facilitating seamless data flows while upholding individuals' privacy rights.

Transfers to other countries (Regulation 22)

For transfers to countries without adequate data protection laws, additional measures must be implemented to ensure the continued protection of personal data. These measures include utilising SCCs or BCRs approved by the ODPC, which provide contractual or organisational safeguards, or obtaining explicit consent from the data subject along with evidence of robust data protection measures.

Special protection for civil registration data (Data Protection (Civil Registration) Regulations, 2020)

Civil registration data, encompassing vital information about births, deaths, marriages, and adoptions enjoys heightened protection under Kenyan law. Transferring this sensitive data outside Kenya is strictly prohibited without explicit written approval from the ODPC, underscoring its critical role in establishing legal identity and facilitating access to essential services.

Additional considerations for cross-border data transfers

Beyond the core requirements and specific transfer scenarios, several additional considerations warrant attention when navigating the complexities of cross-border data transfers from Kenya:

1. Data localisation: While Kenya does not impose a blanket data localisation requirement, certain sectors, such as financial institutions, may have specific data residency mandates. Organisations must stay abreast of sector-specific regulations to ensure compliance when planning cross-border data transfers.
2. Cross-border transfer agreements: We recommend establishing a meticulously drafted cross-border transfer agreement with the recipient entity. The agreement should clearly delineate the responsibilities of both parties, outline the specific data protection measures

implemented, and provide mechanisms for addressing potential disputes or breaches.

3. DPIA: When data processing activities involve high risks to individuals' rights and freedoms, including certain cross-border transfers, conducting a DPIA may be mandatory as per Section 52 of the Data Protection Act. A DPIA is a systematic process that helps organisations proactively identify and mitigate potential privacy risks before commencing any data processing activities.

High-risk data transfers: A closer look

Certain cross-border data transfers are classified as "high-risk" due to the inherent sensitivity of the data, the scale of processing, the utilisation of new or emerging technologies, or the potential impact on vulnerable individuals. These transfers warrant heightened scrutiny and often necessitate explicit approval from the ODPC, even if the destination country has adequate data protection laws.

Factors that elevate risk

Several factors can elevate a data transfer to the high-risk category:

- Sensitive personal data: Transfers involving sensitive personal data, such as health records, biometric information, or details about an individual's race, religion, or sexual orientation, inherently carry a higher risk due to the potential for significant harm if mishandled or misused.
- Large-scale processing: Transfers involving vast volumes of personal data or processing activities that affect a substantial number of individuals are also considered high-risk. The potential for widespread impact in case of a data breach or privacy violation necessitates additional safeguards.
- Innovative technologies: Using new or emerging technologies, such as artificial intelligence or machine learning, in data processing or transfer can introduce unforeseen privacy implications, thereby increasing the risk profile.

- Profiling and automated decision-making: Transfers that involve profiling or automated decision-making processes that could have significant legal or similarly substantial effects on individuals also warrant heightened scrutiny due to the potential for discriminatory outcomes or unfair treatment.
- Vulnerable individuals: Transfers involving data relating to children, older citizens, or other vulnerable groups require special care and attention due to the increased need for protection and the potential for exploitation.

Requirements for high-risk data transfers

In addition to the general requirements for cross-border data transfers, high-risk transfers necessitate additional measures to mitigate potential risks:

- DPIA: Conducting a DPIA is essential to:
    - thoroughly assess the necessity and proportionality of the transfer,
    - identify and evaluate potential risks to individuals' privacy, and
    - implement appropriate safeguards to address those risks.
- Prior consultation with the ODPC: In certain cases, the ODPC may require some instantiation before proceeding with a high-risk data transfer. This allows them to evaluate the proposed transfer, provide guidance on ensuring compliance, and suggest additional safeguards if necessary.
- Explicit ODPC approval: In many instances, high-risk data transfers require explicit approval from the ODPC, even if the destination country has adequate data protection laws. This serves as an additional layer of scrutiny to ensure the protection of individuals' privacy rights.

Consequences of non-compliance

Failure to comply with the requirements for high-risk data transfers can result in severe consequences, including:

1. Administrative fines: The ODPC has the authority to impose substantial fines for non-compliance with data protection laws, which can significantly impact an organisation's financial standing.
2. Reputational damage: Data breaches or privacy violations resulting from unauthorised or non-compliant data transfers can severely tarnish an organisation's reputation, leading to a loss of trust among customers and stakeholders.
3. Legal action: Individuals whose data is mishandled or transferred without proper authorisation can take legal action against the data controller or processor, potentially resulting in costly litigation and further damage to reputation.

Seeking ODPC approval: Practical examples and why it matters

Engaging with the ODPC is a crucial step in ensuring compliance with Kenya's data protection framework, particularly when undertaking cross-border data transfers. Understanding when and why ODPC approval is necessary, along with practical examples, is vital for organisations to avoid legal repercussions and uphold the privacy rights of individuals.

When is ODPC approval mandatory?

The Data Protection Act and its associated regulations stipulate specific scenarios where obtaining explicit approval from the ODPC is mandatory before initiating a cross-border data transfer:

Transfers to countries lacking adequate protection

Example: A Kenyan company wants to transfer customer data to a cloud service provider based in a country that hasn't been recognised by the ODPC as having adequate data protection laws. In this case, the company must seek ODPC approval and demonstrate how they will implement appropriate safeguards, such as SCCs or BCRs, to protect the data.

Transferring civil registration data

Example: A research institution wants to share anonymised birth records with a foreign university for a demographic study. Even though the data is anonymised, it falls under the category of civil registration data, and thus, requires written approval from the ODPC before any transfer can occur.

High-risk data transfers

Example: A healthcare provider in Kenya plans to share patient data with a medical research organisation overseas. Due to the sensitive nature of health data and the potential impact on individuals' rights and freedoms, the ODPC may deem this a high-risk transfer and require a DPIA and their explicit approval, even if the recipient country has adequate data protection laws.

The importance of proactive engagement

Beyond these mandatory scenarios, proactive engagement with the ODPC is highly recommended whenever uncertainties arise regarding the need for approval.
Example: A Kenyan e-commerce platform is considering using a third-party analytics service based outside Kenya. While the data being transferred might not be inherently sensitive, the platform is unsure whether the transfer qualifies as high-risk. In such cases, it is prudent to consult with the ODPC to clarify any ambiguities and ensure full compliance.

The ODPC plays a vital role in upholding data protection standards in Kenya. By seeking their guidance and obtaining necessary approvals,

organisations demonstrate their commitment to responsible data handling and contribute to a secure and trustworthy digital ecosystem.