LEGAL TAKE

DATA PRIVACY LIABILITY OF FOREIGN WEBSITES

Lewis Ndonga
Associate

1. Introduction

There's been a huge uptake in the level of access to all sorts of websites over the last twenty years. Now, any person residing in Kenya can access a website selling products from overseas. Think of Amazon, you can now shop online and have the goods delivered from abroad to your door.

On the flipside, such access can require you to provide certain information about yourself. This can be as simple as a name, to as sensitive as your debit card details. Considering that these websites are hosted abroad and owned by companies that are not Kenyan, what kind of liability do these web hosts have to you regarding the safety of their data?

2. The Role of the ODPC in compliance by foreign bodies

In Kenya, the Office of the Data Protection Commissioner (the **ODPC**) acts as the regulator and enforcer of data privacy laws in Kenya. The ODPC is tasked with the mandate of ensuring compliance with the Data Protection Act, 2019 (the **Act**).

Part of this mandate is to:

1. investigate complaints made to the ODPC by aggrieved parties:

2. issue enforcement notices requiring certain data processors and controllers to comply with the requirements of the Act; and

3. issue penalty notices should data controllers/processors fail to comply with enforcement notices.

However, this is easy to do when data controllers and processors are registered and carry out business in Kenya. The ODPC can trace non-compliant bodies and issue the requisite notices. It becomes trickier where the non-compliant organization is a foreigner based abroad. In such a case, we turn to the provisions of the Act.

Section 4 of the Act provides that it applies to the processing of personal data by a data controller or data processor who is:

a. established in Kenya or ordinarily resident in Kenya and processes personal data while in Kenya; or

b. *not established in Kenya, nor ordinarily resident in Kenya but processes personal data of individuals located in Kenya.* [Emphasis added]

The language of the Act indicates that it (and by extension the powers of the ODPC) extends to data controller/processors operating outside of Kenya, such as Amazon. This means that the ODPC has the mandate under Kenyan law to investigate any complaints of misuse of any personal data being stored, used or otherwise processed in another country. The ODPC can also issue enforcement notices to such foreign organizations and even require them to pay any penalties in accordance with the Act.

Further, the protection given under the Act applies also to any other person **located** in Kenya. It is not limited to Kenyan citizens in Kenya.

3. The challenges of cross-border compliance

While the Act requires compliance by foreign organizations, this presents some practical challenges. Particularly, foreign controllers/processors do not have the same incentive to comply with the Act as local controllers/processors. Should the ODPC issue a foreign organization with an enforcement notice/penalty notice, the organization can easily choose to ignore such notice.

Failure to comply with an enforcement notice attracts a fine of K.Shs.5,000,000/= or an imprisonment term not exceeding two years. Such criminal culpability requires use of state power to arrest any person found in contravention of the Act and require them to stand trial. This is simple enough to do within Kenya but represents a tall order to enforce in a foreign country.

A legal challenge is presented where the Act in Kenya prevents the disclosure of information to a third party, yet the law in a foreign country allows for the disclosure or access of a subject's personal data. Unless terms of use or privacy policies are clear on the governing law, this creates a conflict of the applicable laws.

4. Addressing the challenges of cross-border compliance.

To address these challenges, the following steps need to be taken to protect the data collected by foreign controllers/processors:

i. *International co-operation*

The foreign country must have some level of co-operation with the Kenyan government to ensure that their resident businesses comply with the Act. This is usually achieved through bilateral and multilateral treaties, specifying the obligations of member states

with respect to enforcing legal and contractual obligations such as data privacy laws between them or within a larger region. In Europe, we have the convention for Protection of Individuals with Regard to Automatic Processing of Personal Data. In Africa, we have the Convention on Cybersecurity and Personal Data Protection. However, as of the date of this article, Kenya is yet to ratify the same.

ii. Robust action by local regulatory authorities

The ODPC must reflect the position of the Kenyan government regarding data protection and be firm on the protection of information located within Kenya. This means that the ODPC may have to liaise with regulatory bodies in other countries to ensure co-operation between the two. The ODPC should also liaise with other arms of government to ensure that their notices are complied with, which may include restricting or cautioning locals from accessing certain websites which are known for data misuse.

iii. Legal provision on transfer of data

In Kenya, the Act requires that any information transferred out of Kenya is done only where there is assurance of appropriate safeguards in place in the other country. Such safeguards can be confirmed if the country has:

- ratified the AU Convention on Cybersecurity and Personal Data Protection;
- a reciprocal data processing treaty with Kenya; or
- binding corporate rules legally enforceable against the foreign controller/processor such as rights of data subjects, complaint procedures, mechanisms of compliance.

Such legal provisions ensure that information is protected at the source, to prevent any transfer of data to countries well known for misusing personal data.

A great example of regional and international protection has been set in Europe, with a recent decision by the Court of Justice of the European Union, colloquially known as *Schrems II,* that determined that EU-US transfer of data did not comply with the General Data Protection Regulation, particularly on government surveillance. The US has since complied with this decision and adhered to the new standard contract clauses provided by the EU to be included in contracts governing EU-US data transfer.

5. Conclusion

Regulatory bodies have a vital role to play in the protection of subjects within their territory. However, the challenges of cross-border compliance make it difficult for regulators like the ODPC to ensure protection of the individuals within their mandate. Regionally and internationally, countries must begin ratifying conventions related to data protection, to provide recourse to any countries regarding enforcement of privacy laws. Further, countries need to consider entering bilateral arrangements, including binding corporate rules and standard contract clauses to better govern the exchange of data between countries.

In case you require further information on this topic, please get in touch with **Lewis Ndonga** at ndonga@fmcadvocates.com

PUBLISHED BY

FMC ADVOCATES

FMC ADVOCATES
2nd Floor, Left Wing
The Crescent, Off Parklands Road
Westlands
Nairobi - Kenya
www.fmcadvocates.com