Client Alert

TRIPLEOKLAW ADVOCATES

August 2019

AN ANALYSIS OF THE KENYA DATA PROTECTION BILL, 2019

Article 31 of the Constitution of Kenya 2010 provides for the Right to Privacy. The Draft Data Protection Bill is aimed at realizing this right. This Bill is herein discussed in detail.

DEFINITION OF 'PERSONAL DATA'

Personal data has been defined as any information relating to an identified or identifiable person. However, we must consider that in an ever-changing technological sphere, what seems non personal information now has the potential to be personal data if distinct data elements are joined together. That definition should therefore be expanded to include information which, if not by itself, makes it possible to identify a person if combined with other information. This will seal a loophole which is otherwise bound to assist data breaches.

DEFINITION OF 'DATA SUBJECT'

We recognize that the Bill is majorly designed towards protecting personal information belonging to natural persons. However, an assumption that data which requires statutory protection is only that relating to natural persons is a misconstruction. Article 260 of the Constitution of Kenya 2010 while interpreting a person under provides

Contacts

For more information please contact:

Catherine Kariuki
Ckariuki@tripleoklaw.com

Janet Othero
jothero@tripleoklaw.com

Joyanne Njau
Jwanjiru@tripleoklaw.com

that a person includes a company, association or other body of persons whether incorporated or unincorporated. As such, the applicability of Article 31 on Privacy includes the above referenced definition.

The Bill's definition of a data subject as an identified or identifiable natural person who is the subject of personal data is therefore incomplete when weighed upon the threshold set by the Constitution. Data goes beyond personal details. Given that the legislation is a data regulation, the Bill should contemplate business information such as financial information, trade secrets, intellectual property among other vital business data. The term data subject should therefore be expanded to reflect this.

DATA COMMISSIONER, PART II

Part II establishes the Office of the Data Protection Commissioner and the appointment of a Data Commissioner who is tasked with among other things, overseeing the implementation of the Act. The Act makes further provisions in different sections which empower the Data Commissioner to make regulations pertaining different data privacy variables. For instance, Section 54 which allows him to make provisions for other instances where compliance with certain provisions of the Act may be exempted.

There are no proper checks and balances set in the Bill to ensure that his powers do not end up crippling the key players within the data privacy ecosystem.

Whereas we recognize the indispensable role played by the Data Commissioner in ensuring compliance, it is our considered view that the Data Commissioner, as an individual, is too powerful. Much has been left to his discretion. There are no proper checks and balances set in the Bill to ensure that his powers do not end up crippling the key players within the data privacy ecosystem. Major decisions such as exemptions should be agreed upon in consultation with other valued opinion makers in the sector such as the Cabinet Secretary to ensure that there is objectivity in decisions made.

REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS, PART III

Part III of the Bill requires that data controllers and data processors be registered with the Data Commissioner. From the onset, this requirement is cumbersome, laying a hurdle for compliance for many data controllers and data processors. Moreover, it is a costly venture especially for those data controllers and data processors who handle very minimal data. The expectation laid upon a public agency acting as either a data controller or processor is the same expectation laid upon. small and medium sized enterprises which will ultimately face a challenge in complying with this provision practically. In our view, the Act should have set minimums on this

requirement. For instance, the Bill can require all data controllers and data processors to have privacy policies that are in line with the provisions of the Bill while registration would only be for data controllers and data processors who handle a huge amount of data like government agencies. The threshold for what amounts to huge amounts should also be set out to avoid ambiguity.

LAWFUL PROCESSING OF PERSONAL DATA, SECTION 30

The Act at Section 30 allows the carrying out of a data protection impact assessment where a processing is likely to result in high risk. This provision however fails to mention what the threshold for high risk is. It is worth noting that the statute, being the primary statute in the area of data privacy, is the major provision which stakeholders will refer to in justifying their actions. The lack of precision therefore in outlining what the threshold for high risk is, creates opportunity for data breaches. This could result in potentially terming as non-risky what is otherwise extremely perilous to the privacy rights of a data subject.

AUTOMATED PROCESSES IN PROFILING, SECTION 35

Recent technological advancement has seen the use of Artificial intelligence (hereinafter AI) and automated processes in profiling of persons. Although Section 35 of the Bill makes provision for automated processes in profiling, a lot has been left unregulated in this sphere.

Most AI applications require huge volumes of data in order to learn and make intelligent decisions. This overrides the principle set out at Section 25(c) which requires personal data to be collected for explicit and specified purposes. AI also requires information over time to make correct valued judgements. This may override the principle 25(f) which requires that data be kept for no longer than is necessary for the purposes which it was collected.

"Whereas the Bill aims at protecting sensitive data and similar variables, AI may need to include such data in the analysis to ensure accurate and fair results in ultimate profiling"

Whereas the Bill aims at protecting sensitive data and similar variables, AI may need to include such data in the analysis to ensure accurate and fair results in ultimate profiling. It is also worth noting that AI has advanced computational capabilities to infer identity of a person on non-personal data. Should there exist exemptions to AI given its complex nature and the 'black box problem'?

Consequently, the Bill must contemplate setting out specific laws on technologies, applications, contexts and consequences of use of such advancements as AI and any probable technological advancements that revolve around it. There should also be a discussion as to whether the existing principles apply in their entirety to AI and if not, what are the ethical requirements to be put in

place to ensure that application of such advancements in profiling do not end up breaching data subjects privacy rights.

RIGHT TO RECTIFICATION AND ERASURE, SECTION 40

This is a vital right that is also guaranteed in the European Union General Data Protection Regulation (hereinafter 'the GDPR') and is provided at Section 40 of the Act. This provision however lacks precision especially as to the data controller's or data processor's time limitations in rectifying or erasing erroneous data. The Act mentions that erasure should be without undue delay. What qualifies that? What is the limit to that?

Also, the Act in this Section provides that the data controller should take reasonable steps to ensure that it updates third party processors of such erasure or rectification. Once again, the lack of precision is evident. 'Reasonable steps' is not a threshold against which a data controller would be held accountable. This opens room for potential data breaches.

DATA PROTECTION BY DESIGN OR BY DEFAULT, SECTION 41

Such aforementioned ambiguity spills over to Section 41 which requires data controllers or data processors to implement appropriate technical and organizational measures to implement the data protection principles. The drafters should be intentional in contemplating the standard technical measures to be incorporated on a minimum basis. The provision should lay out the necessary safeguards that an organization should set out to ensure implementation.

PROCESSING OF PERSONAL SENSITIVE DATA, SECTION 44

The Bill prohibits processing of sensitive personal data unless Section 25 which makes provision for the Principles is set out. However, many entities, especially employers possess this sensitive data and may process it to the disadvantage of the data subject. With the Bill ultimately becoming law, the question arises as to how such information should be handled. What safeguards are to

be put in place by such entities with particular attention to sensitive personal data held by them and how will compliance be measured?

CLOUD COMPUTING FOR BUSINESS

An important data aspect that has totally been unregulated in the Bill is that of cloud computing. Many businesses around the world have settled on cloud as an important business solution. Technological advancements such as cloud expose data to potential security breaches which, in this case, is on an international sphere.

As resourceful as cloud computing is. It adds to the already existing data privacy and security risks. Cloud providers are an attractive target for hackers to attack as massive data is stored on cloud services. Protection of such data is vital to encourage flexibility and a greater uptake of cloud services.

Mexico is the only country that has adopted cloud specific provisions in relation to data protection to address transparency about the layered nature of the cloud supply chain; the treatment of user data following service termination, and law enforcement access. Our legislation should perhaps reflect the above variables.

ETHICAL ISSUES

It is not lost to us that the Bill does not cover certain ethical issues already existing within the data privacy ecosystem. For instance, entry into most buildings in Kenya requires persons to leave their personal information at the entry points. Does the Bill eliminate this practice? Will such entities be required to dispose such information held by them? If not, what minimum safeguards exist to ensure that data breaches do not occur based on this information?

Given the nature of technology to act as an enabler of human desires and therefore human thoughts, should entities be allowed to treat non-identifiable information as tools for personalized marketing considering that this would be targeted to specific individuals, therefore creating an identifiable individual which would result in a breach of the Bill?

Mexico is the only country that has adopted cloud specific provisions in relation to data protection to address transparency about the layered nature of the cloud supply chain; the treatment of user data following service termination, and law enforcement access. Our legislation should perhaps reflect the above variables

GENERAL APPLICABILITY OF THE ACT.

We recognize that the Bill has borrowed heavily from the GDPR which set a global standard for data privacy rights. As such, it is a Bill that mirrors international best practice in the data privacy

ecosystem. Granted, it is a reasonable expectation that with such great likeness to the GDPR, the weaknesses to be experienced by our Bill both in its drafting and its implementation would, in many respects, resemble the weaknesses of the GDPR.

Consequently, the Bill has major drawbacks such as the cost to reach compliance. For instance, the courts are exempt from having a data officer at Section 24(a) which is similar to the GDPR. This is unfortunate as the judiciary handles substantive personal data. The effect of such exemption would be data privacy breaches which will be impossible to prove as there is no officer confirming compliance. Similarly, the GDPR sets hefty penalties for non-compliance which reflects in the Bill. At Section 63, the penalty set out for breach of the provisions of the Bill includes up to two per centum of the organization's annual turnover for the preceding year which could result in huge losses for data controllers and data processors.