Client Alert

TRIPLEOKLAW ADVOCATES

September 2019

Contacts

For more information please contact:

Catherine Kariuki
Ckariuki@tripleoklaw.com

Janet Othero
jothero@tripleoklaw.com

Joyanne Njau
Jwanjiru@tripleoklaw.com

THE HUDUMA BILL, 2019

DEFINITION OF 'PERSONAL DATA'

Personal Data has been defined as foundational and functional data collected under the Act as specified in the first schedule. Firstly, the Schedule sets out what foundational data is but fails to expound what amounts to functional data. The lack of that definition thereof creates ambiguity and a possible loophole that creates opportunity for breach of the right to Privacy.

Further, the Data Protection Bill, which if assented to will be law also defines personal data. This Bill defines it as any information relating to an identified or identifiable person. Given that this will be the primary law guaranteeing the right to privacy as enshrined in Article 31, there is need to harmonize these definitions to ensure that the protection offered in the law for data privacy is guaranteed in this Bill as well.

INITIAL ENROLMENT, SECTION 11

The Bill requires that individual residents make a personal appearance before a designated National Integrated Identity Management System (hereinafter 'NIIMS') registration officer to enroll into the NIIMS. As an exception to this,

section 11 (4) provides for the different categories where the Principal Secretary can make arrangements to ensure that enrolment is obtained e.g. elderly people.

However, the Bill fails to contemplate persons with deformities, for instance, one who lacks fingers. With the requirement set out on biometric information, such persons would be locked out of the NIIMS. There is therefore need for expansion of the special groups persons to reflect such issues as deformities.

REPLACEMENT OF HUDUMA CARD, SECTION 15

Section 15 of the Bill provides that where the Huduma card is lost, worn out, tampered with or otherwise rendered unserviceable, the application for replacement will be subject to a prescribed fee. This is an unreasonable provision as it lays a financial burden on the individuals. This ultimately limits individuals accessibility to services outlined in the Section 8 of the Act as a Huduma card is mandatory in the said instances. In our view, there should be no fee for replacement of a Huduma card. The said provision should therefore be deleted.

SUPPLY OF FUNTIONAL DATA INTO NIIMS, SECTION 17.

The Bill at Section 17(2) provides that every government agency delivering a public service shall be linked to the NIIMS database. This means that every government agency will have unlimited and unrestricted access to the personal details of enrolled individuals.

"The law does not set any controls in ensuring that agencies only access the adequate and relevant information necessary for the particular service delivery"

The law does not set any controls in ensuring that agencies only access the adequate and relevant information necessary for the particular service delivery. The European Union General Data Protection Regulation (hereinafter 'the GDPR') sets out principles of data protection amongst which is the principle on data minimization, which restricts collection or access of data to the relevant necessary data required as well as the principle on purpose limitation which requires that data controllers and data processors restrict themselves to the specific purpose of the information obtained.

Client Alert

Consequently, the unlimited access by government agencies creates a loophole for data breaches. In our view, the provision should reflect the principles of data protection.

ACCESS TO INFORMATION, SECTION 37

The Bill allows an individual to obtain a copy of the particulars of their personal data in the NIIMS database. The Bill fails to provide the process an individual should follow to access this information. Is the application oral or written, what processes shall be followed? This ambiguity goes into denying the individuals the right of access to their information.

Also, this provision on access fails to tie in all other agencies that would potentially have access to the NIIMS database. Given that the NIIMS is poised to be the single source of personal identification, private entities would definitely rely on its database as the source for validation and verification of individuals information. The Bill should therefore clearly dictate how private entities shall access such data and the controls set therein. What processes are to be followed and the bare minimums that an entity should meet in order to access information. This includes matters such as the cybersecurity polices in place in order to indemnify the data subject in case of breach.

Further, this provision as read with section 39 on technical security measures does not instill confidence in individuals as to the controls set in the Bill to ward off unauthorized access to the NIIMS database. This needs to be addressed.

RIGHT TO RECTIFICATION, SECTION 40

The right to rectification is a vital right that is also guaranteed in the GDPR and is provided at Section 40 of the Bill. This provision however lacks precision especially as to the agency's time limitations in rectifying erroneous data. The Bill mentions that rectification should be without undue delay. What qualifies that? What is the limit to that?

This section does not have a threshold against which an agency would be held accountable. This opens room for potential data privacy breaches.

A closely associated right to this one is the right to deletion. In the Data Protection Bill, the right to rectification and deletion has been set out in the same provision. This is also reflected in the GDPR Principle on storage limitation which requires that information be deleted when no longer required. In this Bill however, the drafters fail to provide for this very important right. In the event that information held in these databases is erroneous and rectified, can an individual have the former information deleted? What happens to information on a foreigner who no longer resides in Kenya? How does the agency holding such information deal with it? Do the drafters envision a situation where such information would be archived? Such questions need to be addressed by having clearly spelt out provisions that touch on all these variables and protect privacy rights associated with the NIIMS.

CONFIDENTIALITY, SECTION 41

We recognize that the Bill has provided for confidentiality by requiring that a NIIMS registration officer or any other person who processes information under NIIMS to treat the information that comes to their knowledge as confidential.

"personal data is sensitive to the individual and the sharing of such information therefore amounts to a serious breach of their Constitutional right to privacy"

However, the Bill does not expand this provision to reflect the consequences of such officer breaching this provision. It is worth noting that personal data is sensitive to the individual and the sharing of such information therefore amounts to a serious breach of their Constitutional right to privacy. Further the Bill fails to bind such officer to confidentiality even after the termination of employment or service relationship. This oversight will eventually open doors for serious breach with no recourse to an enrolled individual.

COMMUNICATION OF BREACH, SECTION 43

The Bill provides that where the NIIMS database has been accessed by an unauthorized person and there is real risk of harm to the enrolled person, the Principal Secretary shall communicate to the enrolled person in writing within reasonably practicable period. This provision is ambiguous. There is no specificity as to the period within which communication to the enrolled person should be done. The discretion is left to the Principal Secretary to decide this. With the bureaucratic systems in government offices, this period could well be months. This discretion left to the Principal Secretary could potentially result in the enrolled person suffering harm. Statutorily binding the PS or whatever agency responsible thereof will expedite the process and possibly allow the enrolled person the opportunity to avoid the risk that comes with such access.

> ***"the requirement that the communication of breach is to be made only when the access is likely to result in serious risk is unacceptable. There is no threshold of what amounts to serious risk set in the Bill. This could result in the PS terming as non-risky access that is actually very risky. The communication should therefore be made to the enrolled person every time there is unauthorized access and breach of the individual's privacy"***

Further, the requirement that the communication of breach is to be made only when the access is likely to result in serious risk is unacceptable. There is no threshold of what amounts to serious risk set in the Bill. This could result in the PS terming as non-risky access that is actually very risky. The communication should therefore be made to the enrolled person every time there is unauthorized access and breach of the individual's privacy rights.

LOCATION OF DATA SERVERS, SECTION 44

The Bill provides that any processing of data under NIIMS shall be done through a server or a data center located in Kenya.

The are no further provisions on this data center. What are the security standards and mechanisms to be met to ensure cyber security? Will audits be carried out? What agency shall be responsible for auditing the equipment at the data center? What will be the frequency of such audits? Will there be any adoption of cloud services? What informs entry of contract with the service provider? What deliverables should be

met? These specifics need to be addressed to ensure protection of data located in these servers and to ensure accountability.

PENALTIES UNDER NO. 5 OF 2018, SECTION 47

The Bill at Section 47 provides that NIIMS is a protected computer system within the meaning of Computer Misuse and Cyber Crimes Act. Consequently, this section proceeds to set out penalties under the afore legislation which are applicable in this Bill. However, the Bill refers to sections which have been contested under Petition 2016 of 2018, such as Section 17, due to issues raised on infringement of fundamental rights guaranteed under the Constitution. Such provisions are currently not operational.

The question therefore arises as to the legality and applicability of this section in the event of breach and what safeguards will exist in the event that these sections are rendered unconstitutional. The Bill must contemplate this situation.

ADMINISTRATION OF THE ACT, PART VI

This part provides for a NIIMS Coordination Committee whose role is purely administrative. We note with concern that whereas the Committee is expected to have representatives from different core ministries relating to NIIMS, the Bill fails to include in the Committee stakeholders who would add expertise and value to the output of the committee. For instance, legal advisers to ensure that there is compliance with data protection laws, cybersecurity experts to ensure technical maintenance of the database and analysis of the NIIMS system itself.

In our view, this part should have established an agency that will be tasked with collection, validation, updating and maintenance of the database.

GENERAL APPLICABILITY OF THE ACT.

In the Memorandum of reasons and objects, the Cabinet Secretary states that Part V adopts international best principles of data protections including those provided under the GDPR. However, it is our opinion that the Bill hardly reflects these principles. There is no goodwill expressed in the Bill to adhere to principles of purpose limitation, data minimization, accuracy and confidentiality as expounded within this commentary.

Further, the willingness to ensure compliance to data privacy rights and data protection is not clear. There are no provisions requiring data protection impact assessment or provision for Data Officer given that NIIMS will hold database of every individual within Kenya.

Consequently, the Bill if implemented as it is will in many ways greatly contribute to infringement of the right to privacy enshrined in Article 31 of the Constitution.

Further, given that all individuals, including foreigners, are expected to update their information on the database, there is great possibility of conflict of laws especially where the individual is from the EU. The chances of infringing on one's data privacy rights are high. The Bill must contemplate and mitigate this.