Data Protection Issues Arising from Blockchain

1. INTRODUCTION

Blockchain technology (**BCT**) is founded on a digital system based on the concept of distributed technologies. This digital system operates as a shared digital ledger which is used for recording data in blocks and each of these blocks represents a unique and identifiable transaction.

The main innovation behind BCT lies in the fact that blockchain (**BC**) lacks a central point of data administration and instead the digital ledger is decentralised. This, among other key features of BCT discussed below, pose some interesting challenges in the context of the data protection principles and framework in Kenya, articulated in the Data Protection Act, 2019 (**DPA** or **the Act**).

2. APPLICATION OF THE DPA TO BLOCKCHAIN TECHNOLOGY

The DPA applies to the processing of personal data by any data processor or data controller who is ordinarily resident in Kenya or not ordinarily resident in Kenya but processing personal data of data subjects located in Kenya.

The DPA widely defines processing to mean any operation performed on personal data. Briefly therefore - any handling of personal data constitutes processing within the meaning of the DPA.

Specifically, within the context of BCT, the initial upload of personal data (to the extent that it constitutes personally identifiable information) onto the distributed ledger as well as the subsequent storage amounts to processing.

3. DATA PROTECTION AND BLOCKCHAIN – POSSIBLE AREAS OF CONFLICT

3.1 Data Controllers

Data controllers (being the person or entity that determines the means and processing of personal data) are at the heart of the data protection regime in Kenya. Given the decentralised nature of BCT, being that a BC network is a distributed ledger intended to be operated by several independent parties, it is not possible to determine whether or not there is a single or several persons/entities who should be considered the controller in a particular data processing transaction. This is because the means of processing of data are determined by various parties including developers, operators, and miners and therefore indicate more of a push towards the concept of "joint controllers" (which is recognised under the DPA).

This specifically poses a challenge in the context of the data protection regime as it is not possible to pinpoint the entity that bears the responsibility of compliance with the data protection obligations under the DPA. This particularly is an issue in public blockchains which lack a central operator and therefore no single person or entity can be deemed to be the controller.

3.2 Principles of data protection

Section 25 of the DPA lists the principles of data protection. The application of BCT might cause compliance issues with the following specific principles of data protection.

Transparency – The DPA provides that personal data should be processed in a transparent manner. In the case of public blockchains, where no central operator exists and no clear designation of a controller or data processor, transparency requirements would not be met.

Data minimisation – the DPA provides that the processing of personal data should be limited to what is necessary in relation to the purposes for which it is processed. Thus, only the data necessary for the controller's purpose should be obtained and processed. One of the key features of BCT is that each node replicates and stores a full copy the data processed by the previous node for the success of the subsequent transaction. This means that data would be processed (stored) for a purpose other than that for which the data was obtained and conflicts with the principle of minimisation.

3.3 Rights of a data subject

Section 26 of the DPA lists the rights of a data subject. However, in a distributed ledger system, the data subject may encounter some hurdles in the exercise of their rights including:

Right to correction of false or misleading data – Most BC networks are designed such that deletion and modification of data is difficult in a bid to secure the integrity of the data and maintain trust in the network.

Right of erasure – Similar to the above, the utility of BCT would render this right difficult to enforce as most BC networks are designed to limit the instances of deletion and modification of data.

Right to object to the automated processing of personal data – BCT employs automated processing technology which in turn makes it burdensome to accommodate unilateral intervention of data processing as a means to increase the integrity and trust of the network.

3.4 Cross border transfers

Section 48 of the DPA provides for the instances where personal data may be transferred outside Kenya and the grounds that must be met prior to such transfer to ensure the security and integrity of the transferred personal data outside of the Kenyan borders. As the design of BCT is not limited or restricted by geography, not only is data easily transferable outside Kenya without meeting any of the pre-requisite conditions for such transfer but additionally, individuals around the world can access and handle all data blocks within the chain at any time.

4. BLOCKCHAIN AS A TOOL TO GIVE EFFECT TO THE DPA

The focus now shifts to the various ways in which BCT could be used to give effect to the DPA.

Control over personal data – It could be argued that all the rights and obligations under the DPA are generally geared towards one goal – providing a data subject with control over their personal data. Through the application of BCT, a data subject could dictate who has access to their personal data as well as decide what happens to their personal data.

Privacy by design – Privacy by design mandates a data controller to consider privacy and data protection principles at the design phase of any system, service, product or process and then later throughout its lifecycle. With the application of BCT, a data controller not only has in place technical measures designed to implement data protection principles in line with the DPA, but a data subject can also monitor the processing of their personal data.

Anonymity/Encryption – To give effect to data protection by design or by default under the DPA, a data controller may employ measures such as pseudonymisation and encryption of personal data. By its very nature, data stored on a BC ledger is encrypted and consisting mostly of hashed values and is therefore highly secure.

Monitoring compliance with the DPA including auditing – At present, inasmuch as safeguards for personal data exist, the data subject has no control over how their personal data is used by a data controller. As discussed above, with BCT, a data subject could dictate how their data is processed as well as to whom such data is transferred. Through BCT thus, a data subject could in essence, ensure that a data controller is in compliance with the DPA.

5. WAY FORWARD

Having established the pros and cons of BCT, organisations looking to utilise BCT in their operations should not shy away from such use. BCT is a technology that can enable DPA compliance as long as a clear understanding of the data flows is mapped out as well as private network limitations.