African nations apply the gold standard of data protection: a round up

Krishna Jhala - Senior Associate - Digital & Data
k.jhala@tamimi.com - Abu Dhabi

Minal Sapra
m.sapra@tamimi.com - DIFC, UAE

The General Data Protection Regulation ('GDPR') which came into force in May 2018, which is primarily applicable to the European Union ('EU') and to businesses handling European citizens' data, has had a global impact and is viewed as the gold standard for protection of consumer data. Nations around the world have been adopting the 'EU-GDPR' approach to data protection, as also seen in UAE's financial free zones i.e. DIFC and ADGM. With a rapidly growing digital economy and increased use of technology for the delivery of remote services, the protection of data in Africa is assuming ever-increasing importance. Out of a total of 54 countries in Africa,[1] at least 50 per cent have either enacted their data protection legislation or have a draft law in place. This article focuses on the data protection laws of the four such countries: South Africa; Kenya; Ghana; and Egypt, and how they compare against the GDPR.

Core principles under the GDPR

For reasons of space it is not possible to provide a comprehensive overview of the GDPR. However, for the purposes of this article, the core principles under the GDPR are as follows:

- **Personal data** is defined *as data that identifies an individual directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Emphasis on the fact that personal data relates to natural persons and not to legal persons i.e. corporates/businesses having legal personality*; and
- **Special categories of personal data** means *processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.
- **Personal Data** should be: (i) processed lawfully, fairly and in a transparent manner in relation to individuals; (ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (i.e., purpose limitation); (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (i.e., data minimisation); (iv) accurate and, where necessary, kept up to date (i.e., accuracy); (v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (i.e., storage limitation); and (vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (i.e., integrity and confidentiality).
- **Data Controllers and Data Processors** should be able to demonstrate compliance with the principles mentioned above including by way of providing clear information to the data subjects, maintaining data processing records (i.e., accountability).
- **Data Protection Officers** ('DPO') are mandatory for organisations that meet one of the three conditions: (i) it is a public authority; (ii) it engages in systematic monitoring of people; or (iii) it

processes sensitive personal data on a large scale. A DPO's role is to advise and train the organisation on data processing and compliance, to monitor and conduct regular security audits, and co-operate with any supervisory authority that oversees activities related to Personal Data.

Data protection laws in Africa

South Africa

The Protection of Personal Information Act 2013 ('POPIA') came into effect on 1 July 2020 (save for certain provisions) and provides a one-year grace period for organisations to comply i.e. 1 July 2021. The "Information Regulator" is the data protection authority under the POPIA and has been in existence since December 2013.

Under the POPIA, the definition of ''Personal Information'' is much broader than under the GDPR and includes "*information relating to ethnicity or social origin, religion*; *information relating to the education or the medical, financial, criminal or employment history of the person; and biometric information."* The definition of "Special Personal Information" is similar to GDPR's definition of special categories of personal data, with the addition of 'criminal behaviour'.

The POPIA sets out eight conditions for lawful processing which include: accountability; process limitation; purpose specification; further processing limitations; information quality; openness; security safeguards; and data subject participation which are similar to the GDPR.

Before processing personal information, the relevant Information Officer (which is referred to as a "DPO" under GDPR), must register with the Information Regulator, and the Responsible Party (i.e., a data controller) should seek prior authorisation from the Information Regulator when processing certain personal and special personal information which includes personal information belonging to children.

Failure to comply with the POPIA may result in the Responsible Party being fined up to US$673,816 (approx.) or imprisoned for a term of between 12 months to 10 years, or both.

Kenya

On 25 November 2019, the Data Protection Act, 2019 ('DPA') came into force and is now the primary statute on data protection in Kenya.

The definitions of personal data and sensitive data under the DPA are aligned with the GDPR's definition of personal and special categories of personal data, although the DPA further expands the definitions of health data and biometric data.

The office of Data Protection Commissioner ('DPC') has been established as the regulator under the DPA and the Commissioner of the DPC was appointed on 16 November 2020. All data controllers and data processors must register with the DPC. The DPC may prescribe additional thresholds for mandatory registration based on: the nature of industry; the volumes of data processed; and whether sensitive personal data is being processed.

Similar to the GDPR, data controllers have an obligation under the DPA to notify the DPC of any breaches within 72 hours of becoming aware of such breach. Data processors are required to inform data controllers of any breach within 48 hours of becoming aware of such a breach.

Contravention of the DPA is subject to penalty up to US$45,641 (approx.) or 1 per cent of an undertaking's annual turnover the preceding year, whichever is lower.

Egypt

Egypt's Personal Data Protection Law ('PDPL') was published on 15 July 2020 and came into force on 14 October 2020. Regulations under the PDPL are expected to be issued by April 2021. Businesses have until April 2022 to comply with the PDPL. The definition of personal data is aligned with the GDPR. However, the definition of sensitive personal data also includes 'financial data' within its definition (which requires explicit consent for processing).

The Egyptian Data Protection Centre, which is proposed to act as the regulator under the PDPL, is yet to be established.

Entities that process personal data (controllers or processors) must obtain a licence permit from the Centre prior to undertaking any such processing or e-marketing activities. The maximum penalty for contraventions of the PDPL is a fine which may amount up to US$319,355 (approx.) or imprisonment for a period up to six months

For further information on the PDPL, please refer to our update that highlights the role and duties of a DPO and the rights of a data subject.

Ghana

In Ghana, the Data Protection Act, 2012 ('DPA 2012'), is the primary legislation governing data privacy and protection which came into effect on 16 October 2012. The DPA's definitions of personal data and sensitive personal data are aligned with the GDPR.

Data controllers must be registered with the Data Protection Commission ('Ghana DPC'), which maintains an online public search register of registered data controllers. Once registered, the data controller receives a Certificate of Registration that should be renewed every two years. A data controller that is not incorporated in Ghana must register as an external company. All data controllers should appoint a data protection officer

Unlike the GDPR, data controllers and processors have the duty to notify the Ghana DPC and all relevant data subjects as soon as reasonably practicable after any breach has been discovered. The maximum penalty under DPA 2012 is US$ 10,500 (approx.) or imprisonment to 10 years or both.

Mindful of the ongoing pandemic, the Ghana DPC has permitted data controllers to register online for the period from 1 October 2020 to 31 March 2021.

What's next?

In addition to the countries discussed above, Uganda has a Data Protection and Privacy Act 2019. However, the implementing regulations are yet to be published and the regulator is not operational. Nigeria has introduced a Data Protection Bill 2020 to enhance its existing Data Protection Regulation 2019. Similarly, Rwanda's Cabinet approved a draft bill on data protection on 27 October 2020.

Apart from country specific legislation, many African Union ('AU') members have adopted the African

Union Convention on Cyber Security and Personal Data Protection,[2] which aims at strengthening existing legislation on Information and Communication Technologies for its member states. A total of 14 countries are signatories to the Convention and it has been ratified by eight countries.[3]

With the growing digital economy and increased use of technology for the delivery of remote services in Africa, there is a pressing need for robust data protection laws to tackle cybersecurity attacks and data breaches. As may be seen, the existing data protections laws of the countries reviewed above are generally aligned with the "gold standard of data protection", the GDPR. It will be interesting to see how the regulators implement and enforce data protection laws, and the extent to which they are influenced by EU regulatory practices and decisions.

For further information, please contact Krishna Jhala (k.jhala@tamimi.com).

[1] Data available on: https://www.worldometers.info/population/countries-in-africa-by-population/ (last accessed on 2 February, 2021)

[2] See information on https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (last accessed on 2 February, 2021).

[3] See information on https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (last accessed on 2 February, 2021).