Kenya Privacy and Data Protection Policy, 2018 and the Data Protection Bill, 2018 – Comments

Sector Name: Capital Markets

Regulated Entity: Allan Gray Kenya Limited

No.	Reference	Comment / Concern	Reason
Privacy and Data Protection Policy 2018			
1.	Paragraph 5	5.1 Fairness and lawfulness and Transparency 5.1.4 "the data subjects will be sufficiently informed regarding the processing of their personal data."	Clarity is required on what "Sufficiently informed" entails, and how this relates to the requirement in 8.2.5 that requires "specific, informed and freely given consent" Further to that where the burden of proof is placed on data processors/controllers in terms of section 28 of the Act. Is tacit consent sufficient or does the consent have to active?
2.	Paragraph 7.3.1	Exceptions " There may be limitations on data subject rights when required by the law or when there are competing rights and therefore it will require an assessment based on the facts and circumstances"	It seems clear that data subject rights may conflict in various circumstances with competing rights and legal obligations. Clarity is required on how a data controller/processor is mandated to weigh up these competing rights. Include perhaps "In case of a conflict of this Act with another law… the following shall prevail/be considered".
The Data Protection Bill 2018			
3.	Section 15	Registration of data controllers and data processors.	Refers to exemptions under the Act where registration of a data controller or processor is not required but it does not specify what these are? E.g. there is no registration required under GDPR or POPIA.

4.	Section 15	Registration of data controllers and data processors.	What do data controllers or processors do in the interim?
5.	Section 17	Duration of the registration certificate.	Prescribed period for renewal of the registration certificate is not specified. Will the Data Commissioner specify the period? And if so, how?
6.	Section 21(1)(b & c)	Compliance and Audit. Appointment of a DPO: There is no definition of what is meant by "large scale" in terms of processing of sensitive categories of data or monitoring of data subjects.	Clarity is required on what “large scale” would entail.
7.	Section 27(4)(1)	Lawful processing of data. Processing of sensitive data without falling under one of the exceptions provided for is punishable by KES 5 million imprisonment of a term of 5 years.	Is it a fine AND imprisonment, OR imprisonment (or both)? Clarity is required as to whether both or either one of the two penalties will be applied.
8.	Section 38(1)	Notification of breach of security on personal data. The prescribed period for notification of a personal data breach to the data Commissioner (and data subject) has not been specified.	Clarity is required on the period of reporting/notification to the Data Commissioner of data breaches. E.g. the GDPR provides for 72 hours.
9.	Section 44(3)	Rule as to data centres and servers. Cross-border processing of sensitive personal data is prohibited.	Does this still apply even if one of the grounds for exemption for processing is complied with? This seems like a pro-active measure on the part of the Data Commissioner.

			(We not aware of specific / similar provisions under the GDPR or POPIA though technically a data subject could complain to the Data Protection Authority directly the latter could act pro-actively in a similar manner).
10.	Section 53	Preservation Order. Data Commissioner may apply for a preservation order (where there is reasonable grounds to believe that data concerned is vulnerable to loss or modification).	A provision like this does not apply in the GDPR and POPIA: Cross-border processing is subject to countries with adequate levels of protection, appropriate safeguards or as exemptions under one of the derogations provided for.