Legal Alert | **June 24, 2021**

The Draft Data Protection Regulations, 2021

Introduction

The Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs issued regulations under the Data Protection Act, 2019 (the "Act") for public participation and consultation. The regulations issued are the draft Data Protection (General) Regulations, 2021 (the "Draft General Regulations"); the draft Data Protection (Compliance and Enforcement) Regulations, 2021 (the "Draft Compliance Regulations"); and the draft Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 (the "Draft Registration Regulations") (collectively, the "Draft Regulations"). We analyse below the salient features of the Draft Regulations.

Registration of data controllers and processors

The Draft Registration Regulations provide for the procedure of registration of data controllers and data processors. Data controllers, who determine the purpose and means of data processing, will need to register with the Data Commissioner ("the Commissioner"). A data processor, who has a contractual relationship with a data controller and with no decision-making power, will also be required to register with the Commissioner. Data controllers and processors (together "Data Users") with annual turnover or revenue below KES 5 million and less than 10 employees will be exempted from registration. This exemption will not apply to Data Users who process personal data for purposes such as debt administration and factoring, insurance and retirement benefits administration.

On registration, a Data User will be issued with a certificate of registration, which is renewable annually. The renewal application should be filed at least thirty days before expiry. The Commissioner will communicate approval of an application within 30 days, and rejection within 21 days.

The Commissioner will be able to reject an application for insufficient information, lack of appropriate data protection safeguards, or the applicant being in violation of any provision of the Act. The Commissioner will be required to maintain a current register of data controllers and processors.

We note that processing data with an expired certificate is an offence. The Commissioner should review this section of the Draft Registration Regulations as data processing is continuous, and a delay in undertaking this core mandate due to an expired certificate could prove costly to a single business, and catastrophic to business sectors. The Commissioner should instead consider perpetual registration which will remain valid, subject to:

- payment of an annual renewal fee;
- annual self-certification of continuing compliance with the Act; and
- well-spaced compliance audits — three years would be a good interval.

This will ensure compliance and business continuity, while also enhancing the ease of doing business.

Data Subject Consent

The Draft General Regulations require a Data User to inform the data subject of the nature and scope of the data to be processed; the reasons for processing; whether the data will be shared with third parties; and the implications of providing, withholding, or withdrawing consent. This must be done in plain, clear and easy to understand language.

The Draft General Regulations seek to establish the parameters for valid consent. Valid consent is the consent given voluntarily by a person who can legally give and is able to communicate their consent.

Data Users cannot imply consent simply because the data subject did not object to the processing proposal. Similarly, there is no consent where the intention of the data subject is unclear, ambiguous, or subject to reasonable doubt. If the purposes for which data is to be processed change, the Data User must seek fresh consent from the data subject.

Collection of personal data

The Draft General Regulations recognize that personal data may be collected from various sources including directly, publications, databases, surveillance cameras, web browser cookies and biometric technology. Whatever the manner of collection, the Data Users will be responsible for: collecting data only with consent; ensuring the quality of the data; securing the data; and only collecting sensitive personal data directly from the data subject.

This will impact everyone including offices using closed-circuit television cameras (CCTVs) or biometric door locks who will be responsible for ensuring the protection of the data collected.

Data Subject Requests

The Draft General Regulations also allow the data subject to restrict processing; object to processing; access the data; rectify the data; transfer the data to another Data User; anonymize or pseudonymize the data; and erase the data. The data subject will do this by making a written request to the Data User with reasons for the request. The Data User may decline the request on certain grounds, for example, refuse access where it may result in a serious threat to life, health or safety of a data subject, or refuse erasure where carried out in exercise of official authority.

Commercial use of personal data

The Draft General Regulations seek to introduce practice guidelines for the commercial use of personal data. In addition to express consent for commercial use and direct marketing, a Data User will be required to give the data subject a simple opt-out mechanism.

The opt-out mechanism should enable the data subject to request not to receive direct marketing. This gives control of data back in the hands of the data subjects. Given global data protection trends, it is advisable for Data Users to provide both opt-in and opt-out mechanisms for direct marketing.

The Draft General Regulations require the opt-out mechanism to be as simple as possible and in a language the data subject understands. To ease compliance, Data Users should publish their data collection media in both English and Kiswahili. Within 7 days of receiving an opt-out request, the Data User shall cease using and shall not disclose the personal data for direct marketing. This request shall be free of charge to the data subject.

The Act emphasizes consumers' consent for processing of their personal data for purposes beyond what is needed for a contract. With people becoming more sensitive about data privacy, organizations will need to show they prioritise consent and protection. This can be done by using a dual opt-in and opt-out structure and asking for clear and affirmative action to signal consent as opposed to pre-checked boxes.

Obligations of Data Users

The Act allows a Data User to retain personal data for as long as is necessary for the processing purpose. Data Users will be required to maintain a retention schedule to ensure compliance. The schedule will outline the purpose and period of retention, provide for periodic audit and what should occur after the audit.

A Data User will also need to have a contract in place before sharing personal data with a third party. These 'data sharing agreements' will set out the roles of the parties in relation to processing of the personal data and sets standards with which the parties will comply. If the regulations are passed, processing of education, election, and national civil registration data will only be done through a server or data centre located in Kenya.

Notification of personal data breaches

The Act requires a Data User to notify the Commissioner of a data breach where there is real risk of harm. The Draft Regulations seek to clarify real risk of harm as where the data breach relates to:

- full name or identification number;
- income, investments, liabilities, or financial records;
- identifiers or access codes for the data subject's account with the Data User.
- adoption or a vulnerable child;
- health or mental well-being; and
- sexual or gender violence.

The Commissioner must be alerted of notifiable breaches within 72 hours, and the data subject within a reasonable time. When deciding what a reasonable time is, it will be useful to remember that liability increases where mitigation is made impossible.

Transfer of personal data outside Kenya

The Draft General Regulations establish the due diligence required of Data Users before they transfer personal data outside the country. The Data User must ascertain that the recipient is bound by legally enforceable data protection obligations comparable to the Act and regulations under it; the data subject has consented to the transfer; it has taken all reasonable steps to prevent unauthorized use or disclosure by the recipient; and the rights of the data subject are safeguarded.

The data subject should be informed of the risks of cross-border transfer and the safeguards in place. Obtaining consent deceptively or misleadingly is an offence which on conviction will attract a fine of up to KES 3 million or imprisonment for up to 10 years, or both.

A country or territory will be taken as having appropriate data protection safeguards if it has ratified the African Union Convention on Cyber Security and Personal Data Protection; or has a reciprocal data protection agreement with Kenya; or it has an adequate data protection law as determined by the Commissioner.

Complaint handling procedure

The Draft Compliance Regulations seek to provide the procedure for making a complaint. A complaint may be lodged by the complainant personally, through a representative, agent or attorney, or anonymously.

Before a complaint is admitted, it will be reviewed to confirm it lies within the Commissioner's mandate. Where it does not, the complainant will be advised in writing of the rejection and reasons.

Where a complaint is admitted, the accused party will be given a chance to respond. The Commissioner will conduct investigations, guided by the provisions of the Fair Administrative Action Act (No. 4 of 2015, Laws of Kenya). Upon the conclusion of investigations, the Commissioner will notify the parties, together with supporting reasons, of its decision. The Commissioner may issue an enforcement or penalty notice, dismiss for lack of merit, recommend prosecution, or order compensation.

The Draft Compliance Regulations allow for a complaint to be handled through negotiation, mediation, or conciliation. The Commissioner facilitates the alternative dispute resolution process and at its conclusion, the parties sign an agreement.