EMERGING DEVELOPMENTS AND CHALLENGES IN COMPLYING WITH THE DATA PROTECTION ACT

Following the operationalisation of the Data Protection Act 2019 (**DPA**), many entities have spent substantial time and resources in attempting to comply with the new laws. The Office of the Data Protection Commissioner (**ODPC**) and Kenyan Courts have also issued numerous determinations, directions and penalties, some of which suggest that the journey to compliance can be a winding uphill struggle.

In this article, we will highlight some of the key developments in the area as well as some of the emerging challenges in light of the developments over the past year. These developments may force data controllers to rethink some of their strategies and outlook on compliance with the DPA.

Consent

In the past year alone, the ODPC has issued multiple penalty notices to various institutions for non-compliance with the DPA. Mulla Pride Ltd, a digital credit provider has recently had a penalty of KES 2,975,000 imposed on it for unlawful collection of contact information from third parties and subsequent use for debt collection purposes without the consent of the concerned individuals.

Similarly, Oppo Kenya and Casa Vera Lounge have been fined KES 5,000,000 and KES 1,850,000 respectively for sharing images of complainants on their social media pages without their consent as required under the data protection laws.

Roma School also received a substantial penalty of KES 4,550,000 for posting minors' pictures without parental consent. In the cases of *Wanjiru v Machakos University* [2022] and *Kamande v Nation Media Group* [2022], the High Court also awarded substantial damages to petitioners whose images had been published without their consent.

The upshot of these findings is that the object of the data protection laws is to empower data subjects and give them control over the use of their personal data. The DPA prohibits the processing of personal data for commercial purposes without the express consent of the data subject.

The DPA defines consent as "*any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of their personal data"*.

Any consent must meet the requirements of "express manifestation", "informed" and "clear affirmative action". Mere disclaimers of the possibility of processing personal data do not meet the threshold for consent under the DPA. Consent is also not a silver bullet and will not negate a data controller's obligation to comply with the other requirements under the DPA.

While consent is mandatory where a data controller or processor seeks to process personal data for commercial purposes, it is not the only basis for processing personal data. Based on the understanding of most data controllers, '**consent**' appears to be the most popular basis for

processing personal data. It is however not inherently the most suitable basis. In some cases, consent may be impractical and even undesirable owing to the requirements and obligations attached to consent as a legal basis for processing personal data. Consent can also be withdrawn by the data subject at any time, potentially leaving the data processor exposed.

Data controllers and data processors should carefully consider what the most appropriate legal basis would be for their intended processing activities. The DPA provides for eight other legal bases for processing personal data.

In some cases of personal data collection such as CCTV surveillance, it may be more practicable to rely on the data controller's legitimate interests such as security purposes as a legal basis for processing. Likewise, necessity for the conclusion or performance of an employment or supplier agreement could be a more suitable basis for processing employee or suppliers' personal information.

Notification of Processing Activities

Where there is a personal data breach and there is a real risk of harm to the data subject whose personal data is affected, a data controller is required to report details of such breach to the ODP within 72 hours of the detection. In the same breath, they are obligated to communicate this to the affected data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.

The ODPC is currently investigating Naivas Supermarkets for failure to adhere to these reporting requirements. The giant supermarket chain failed to report the unauthorised transfer of over 611 GB of customer personal data in time and potentially faces a fine of up to KES 5,000,000 if found culpable.

In order to be able to meet these stringent reporting requirements, it is necessary for a data controller to be able to identify any data breaches as soon as practically possible.

The use of Endpoint Detection Systems (EDS) is one solution that could play a crucial role in cybersecurity by safeguarding individual devices such as computers, laptops, and mobile devices, against malicious activities. These systems focus on identifying and mitigating threats at the endpoint, where users interact with the networks. They involve monitoring device behaviour, file activities, and network connections so as to detect anomalies indicative of potential security breaches. By providing real-time visibility into endpoint activities, these systems would enable organizations to proactively defend, identify and mitigate cyber threats such as data breaches, ensuring the overall security and integrity of their IT infrastructure as well as enabling data controllers meet the reporting requirements in the event of a data breach.

Data Subject Rights

The wide array of rights granted to data subjects is at the heart of the DPA. This includes the right to be informed of the use to which their personal data is to be put; to access their personal data in the custody of a data controller or data processor; to object to the processing of all or part of their personal data; to correction of false or misleading data; and to deletion of false or misleading data about them.

It is the onus of data controllers and data processors to ensure that they implement proper internal mechanisms to facilitate the exercise of these rights.

In the matter of *Harrison Kisaka v Faulu Microfinance Bank*, the ODPC affirmed the right of data subjects to access their personal data in the possession of a data controller or data processor upon request. In this case, the ODPC held that prospective employers are obligated to grant prospective employees access to their personal data gathered during background checks upon request.

For this reason, data controllers should ensure that they integrate data protection principles by default or by design into the entire process of designing and developing systems, products, or services. Embedding the data protection principles into the core architecture and functionality of all operations will facilitate the exercise of data subject's rights within the legally stipulated timelines. This includes data access requests, restriction of processing or deletion of personal data held by a data controller or processor.

Sector-specific Guidance Notes

The DPA empowers the data commissioner to develop sector-specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education and social protection. To this end, the ODPC issued four new guidance notes in December 2023.

The Guidance Note for the Communication Sector applies to all communication service providers processing personal data in either the public or private sector. This is intended to set the minimum standard which can be supplemented

by additional measures for the protection of privacy and individual rights, which may impact or be impacted by the processing of subscriber information, traffic information, location information or contents of a telecommunication.

The Guidance Note for Digital Credit Providers ("**DCP**") applies to persons who give loans over a digital platform. It sets out the compliance requirements that DCPs must implement in the processing of personal data in compliance with the DPA. The guidelines provided are aimed at upholding the right to privacy and ensuring data protection for individuals while encouraging responsible innovation and sound operations within the finance sector. This guidance note contains a checklist which may be used as a tool for monitoring compliance with the provisions of the DPA and the regulations thereunder by the DCPs.

The Guidance Note on the Processing of Health Data applies to all health institutions including digital health processing platforms such as Health Management Information System (HMIS), eHealth and mHealth applications. It includes separate sections tailored to different healthcare institutions and players in the health industry and considers the specific data protection issues relevant to each type of institution. It provides clear and practical guidance on various data protection principles and includes checklists to help healthcare institutions monitor their compliance with relevant legal requirements.

The Guidance Note for the Education Sector is intended to provide educational institutions with comprehensive insight into their responsibilities under data protection laws. This guidance note strives to address diverse facets of data protection spanning from collection, use, retention, disclosure and disposal. It applies to all educational institutions operating in Kenya including kindergartens, primary and secondary schools, higher education institutions and e-learning solutions and contains a checklist to help school administrations understand and monitor their compliance with relevant legal data protection requirements including guidance on the creation of privacy notices.

While guidance notes may not in themselves have the force of law, they give us a glimpse into the ODPC's mind when seeking to interpret the provisions of the DPA in light of the practical challenges faced by the data controllers in these sectors. They would also provide a level of certainty and a practical tool for data controllers when developing standard operating procedures.

Conclusion

As we celebrate the DPA and witness the surge in registration of data controllers and processors across the country along with the rush to draft and implement the various policies required under the DPA, it is critical to note that the practicalities of compliance go beyond these initial steps.

The requirements under the DPA and the regulations thereunder require entities to rethink and perhaps even redesign their processes, products and services in order to factor in data protection principles throughout the lifecycle of their operations.

It would therefore be prudent to undertake regular data protection compliance audits taking into account emerging case law, ODPC determinations, guidelines and compliance checklists issued from time to time in order to truly appreciate the height, width and breath of the data protection obligations under the DPA.

Looking forward, we are keen to see how the courts will interpret the provisions of the DPA and whether their decisions will align with the findings of the ODPC.

Please feel free to reach out to us with any questions or concerns.

SARAH KIARIE -MUIA
Partner
SKiarie@kapstrat.com

AUDREY SEUR
Associate
ASeur@kapstrat.com

VICTOR GATEI
Associate
VGatei@kapstrat.com