Deloitte.

Data privacy day
The road to compliance

January 2022

MAKING AN IMPACT THAT MATTERS since 1845

Africa has witnessed extensive economic development attributed to increased internet connectivity, access to broadband and digital trade. This has also come with its own set of concerns around data privacy; a discussion that has been propelled by the 2016 General Data Protection Regulation (GDPR) of the European Union (EU). Notably, few African countries have enacted data protection policies and legislation.

The 28th of January marks the annual global Data Privacy Day and this year it is particularly important in the East African data privacy landscape. With Kenya, Rwanda and Uganda having enacted specific data protection legislation, and other countries in the region having draft bills in motion, the data privacy discussion is coming to the forefront to drive enterprise-wide business initiatives.

Recently in Kenya, various regulations have been published to aid in the implementation of the Kenyan Data Protection Act. They include:

1. The Data Protection **(General) Regulations, 2021** – which give various provisions for Data Subject Rights, restrictions on the Commercial Use of Data, Obligations of Data Controllers and Data Processors, elements to implement Data Protection by Design and by Default, notification of personal data breaches, transfer of personal data outside Kenya, Data Protection Impact Assessment, and exemptions under the Data Protection Act.

2. The Data Protection **(Complaints Handling and Enforcement Procedures) Regulations, 2021** – which provide for the procedures related to lodging, admission, and response to complaints and enforcement provisions.

3. The Data Protection **(Registration of Data Controllers and Data Processors) Regulations, 2021** – which give the registration rates for various organisations as data processors and controllers, as well as indicates a two-year validity of the certificates. Exemptions are also provided for data controllers and processors whose annual turnover is below five million Kenya Shillings or have annual revenue of below five million shillings and less than ten employees.

What do you need to be thinking about?

On this day, five important privacy areas to focus on in the next few months, as we approach enforcement.

Data Privacy regulation, unlike various other regulations, cuts across the enterprise and requires a multi-disciplinary approach towards ensuring successful compliance. Multiple aspects of the business need to be taken into consideration as organisations prepare to be compliant with the regulation. Below is a summary of key considerations to apply across various business domains.

Data

Data Privacy regulation regulates the life cycle of personal information within an organisation. Therefore, it is imperative for organisations to have greater visibility over their data life cycle management; specifically touching on aspects around data governance, data quality, data minimization, data storage and disposal. The challenge is to provide clearer oversight on data storage, journeys, and lineage, with an understanding of what personal data is collected and where it is stored facilitating compliance of the data subjects' rights (rights to have data deleted and to have it ported to other organisations). Hence affecting data processing operations including the ones managed by third-party vendors.

A precursor to engaging in data related activities is the commissioning of data flow diagrams which explicitly maps the flow of personal information in the context of business processes, people and technology, through a particular business area within an organisation. Once an understanding is gained of where personal information resides and how it is being processed, data privacy regulation requires that specific measures be implemented in respect of collection, storage, retention and destruction to ensure that processing is based on the principles of fairness, transparency and good ethical governance to meet rights of data subjects. This will require organisations to strengthen their data governance and data quality management capabilities.

Given that data subjects can also request deletion of their data, organisations need to review their data management processes, system architecture, third party access, data archiving and deletion procedures to ensure compliance.

Legal and Compliance

Organisations that participate in various processing activities around personal data will have to appoint a Data Protection Officer (DPO) who will have a key role in ensuring compliance. In order to ensure that the DPO can comply with their obligations to monitor compliance by the organisation, the DPO must ensure that they able to aggregate compliance information from the organisation in respect of several key risks as it relates to privacy. As a result, determining and then defining key risk indicators as they relate to privacy, ensuring that the key risks remain within acceptable manageable levels of risk as determined by the organisation, and regularly providing this information to the relevant stakeholders within the organisation in terms of established reporting protocols and standards, is a key part of the DPO's role.

Furthermore, privacy policies, notices and consent management requirements also need to be considered carefully since, the regulations retain the notion of consent as one of the conditions for lawful processing as well as demonstrate that consent was 'freely given, specific, informed and unambiguous.' This, therefore, requires careful consideration of organisations public-facing privacy policies and consent notices.

Technology

Privacy regulation will change how technologies are designed and managed (protection by design/default), therefore Data Protection Impact Assessments will be a requirement before deploying any new technologies or making updates to systems that would likely result in a high risk to the rights and freedoms of data subjects. This requires coordination across the business in ensuring risk management, project management and system design and implementation procedures are aligned and enforced consistently.

There is also a need to assess minimum cyber security standards and posture that must be adopted to ensure that organisations can reasonably protect personal information, and that such protection is appropriate in the circumstances. While traditional cyber security frameworks are a good starting point to determine an organisation frame of reference, it is important to note that the security measures that are required to be implemented in the context of privacy are peculiar and specific. For example, consider technical aspects

around encryption, data loss prevention, or even pseudonymization. An example of these are the recently published ISO/IEC 27701:2019 and updated NIST privacy control catalogue, both of which have a focus on privacy requirements.

Third Party Risk Management

This is an important area for consideration, especially for those who outsource the processing of personal information to third parties. Perhaps the most important starting block is to prescribe the privacy obligations the third parties are required to adhere to. It is important to expressly highlight the physical security, cyber security, data management and breach notification protocols in third party agreements. The second important component that should be considered, is the ongoing monitoring and assessment against these requirements and the remediation of areas of non-compliance in third party environments. There are several ways in which this can be achieved, including assessments or audits and certain reporting or disclosure requirements by the third party. It is important to ensure that where areas of non-compliance are discovered, remediation plans are created and deployed to track progress against the findings to ensure that the areas of non-compliance are remediated in a timely manner.

Incident and Breach Management

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorized person, there is an automatic obligation to notify the Regulator. In most instances, save where notification to the affected data subjects would impede a criminal investigation, notification to the affected data subjects is also mandatory. The notification to the Regulator and the data subject must contain certain mandatory information, including a description of the possible consequences of the security compromise, the measures taken by the responsible party to address the security compromise and the measures the data subject can take to mitigate the adverse effects of the security compromise.

At the point of notification by the responsible party to the Regulator and/or the data subjects, several important consequences are triggered including exposure to legal, reputational and business risks and consequences. As a result, it is important to ensure that an organisation is correctly configured to respond to a material event such as a security compromise. Part of this configuration is to ensure that a task team is identified and mandated to respond to a security compromise which should consist of the DPO, legal representation, reputational management, the cyber security team and any other stakeholder that may be required.

In Summary

The implementation of privacy projects is as much about compliance as it is about the management of the risk of non-compliance. It is important for organisations to recognize where they will not be able to comply with the provisions of the regulations by the effective date and ensure that the risk of non-compliance is managed appropriately. This should include formally registering the risk within the organisation, having the appropriate visibility and proper acknowledgement of the consequences that arise as a result of the risk of non-compliance.

Of course, data privacy regulation is not only about compliance, but rather the value that it unlocks for organisations and all the stakeholders. Seen from the perspective of a value driver, data privacy regulation can significantly enhance cyber security, data discipline and quality, efficiency and standardization, and results in an increased data asset value. These in turn, reduce the impact of potential breaches on businesses and their adverse effects on data subjects, and fundamentally increases business insights through more meaningful data consumption and analytics. Indeed, compliance will undoubtedly deliver value across the business; and perhaps it will deliver it in some of the areas where it is needed most.

References

1. kenyalaw.org. [Online] 19 January 2022.
2. dataprotection.africa. [Online] 19 January 2022.
3. odpc.go.ke. [Online]

Contacts

Urvi Patel
Partner, Risk Advisory
ubpatel@deloitte.com

Rakesh Ravindran
Senior Manager, Risk Advisory
rravindran@deloitte.com

Contributors

Technical

Felix Achira
Manager,
Risk Advisory

Janet Silantoi
Consultant,
Risk Advisory

Creative & Design

Daniel Gitonga
Clients & Industries Analyst

Offices

Kenya
Deloitte Place
Waiyaki Way, Muthangari
Nairobi
Tel: +254 719 039 000

Tanzania
Aris House
3rd Floor, Plot 152, Haile
Selassie Road,
Oysterbay, Dar es Salaam
Tel: +255 22 2169000

Uganda
3rd Floor Rwenzori House
1 Lumumba Avenue
Kampala
Tel: +256 41 7 701000

Deloitte.