Grant Thornton

Data Protection Act, 2019

Enacted by The Parliament of Kenya

Data Privacy and Advisory Services

2021

Audit | Tax | Advisory

Data Protection Act, 2019

Introduction

The Data protection Act, 2019 ("the Act") came into force on 25th November, 2019 and is now the primary statute on data protection in Kenya. It is an act of Parliament that establishes the Office of the Data Protection Commissioner.

Objectives and purposes of this Act

- Regulate the processing of personal data;
- Ensure that the processing of personal data of a data subject is guided by the principles
- Protect the privacy of individuals;
- Establish the legal and institutional mechanism to protect personal data; and
- Provide Data Subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

Grant Thornton Team has the deep experience and international reach to help your business develop and implement practical compliance solutions to the Act.

Importance of Compliance with the Act

- **Section 56** states that; A complaint made to the Data Commissioner shall be investigated and concluded in **ninety days**.
- **Section 58** of the act states that: Where the Data Commissioner is satisfied that a person has failed, or is failing to comply with any provision of this Act, the Data Commissioner may serve an enforcement notice on that person requiring that person to take such steps and within such period as may be specified in the notice. Any person who fails to comply with an enforcement notice commits an offence and is liable on conviction to a **fine** not exceeding **five million shillings** or to **imprisonment** for a term **not exceeding two years**, or to both.

Data Protection Act, 2019

What Is Personal Data?

"personal data" means any information relating to an identified or identifiable natural person.

What is Sensitive Personal Data?

"sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

What is Personal Data Breach?

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal Data Processing

"processing" means any operation or sets of operations which are performed on personal data or on sets of personal data whether or not by automated means, such as

- collection, recording, organization, structuring;
- storage, adaptation or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination, or otherwise making available;
- alignment or combination, restriction, erasure or destruction.

Data Processor

The natural or legal person, public authority, agency or other body which processes the data for and on behalf of the Data Controller.

Data Subject

Any person whose personal data is being collected, held or processed.
e.g. Clients, Prospects, Employees, Job Candidates, Third parties, and Subsidiaries.

Data Controller

A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

Data Protection Commissioner (DPC)

The DPC mandate includes overseeing the implementation and enforcement of the provisions of the Act. The DPC is tasked with the maintenance of the register of Data Controllers and Data Processors, receiving and investigation of complaints under the Act and carrying out inspections of public and private entities to evaluate the processing of personal data.

Data Protection Officers (DPOs)

The Act makes provisions for the designation of DPOs but this obligation is not mandatory. DPOs can be members of staff and may perform other roles in addition to their roles. A group of entities can share a DPO and the contact details of the DPO must be published on the organization's website and communicated to the DPC. The DPO has the following roles:

- Provide advise on data processing requirements, data protection impact assessment and ensure compliance with the Act
- Facilitating capacity building of staff involved in data processing operations
- Cooperating with the DPC

Data Protection Act, 2019

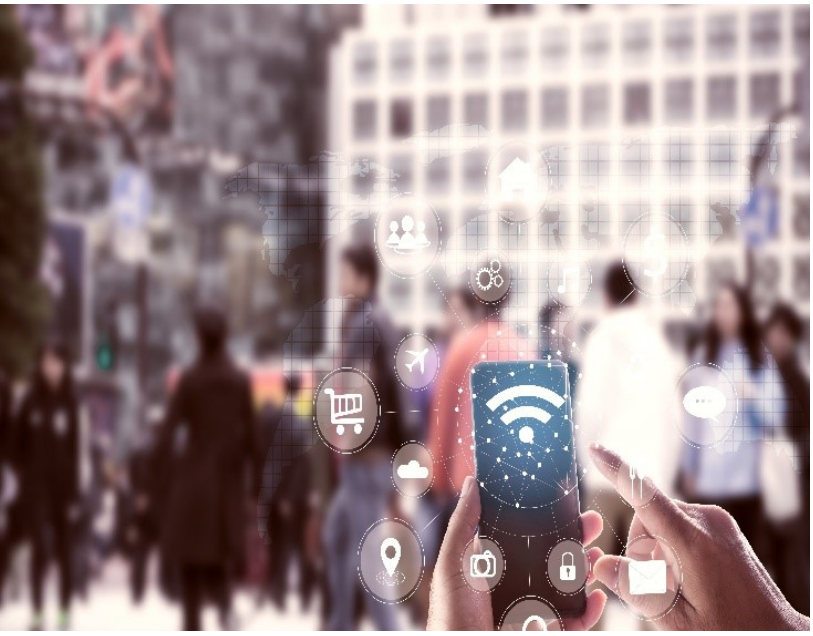
Registration as a Data Controller or Processor

Data Controllers and Data Processors are required to be registered with the DPC. The DPC, however, has discretion to prescribe the thresholds for mandatory registration considering:

- The nature of industry
- The volumes of data processed
- Whether sensitive personal data is being processed
- Any other criteria the DPC may specify

A Data Subject has the right to

- Be informed of the use to which their personal data is to be put
- Access their personal data in custody of Data Controller or Data Processor
- Object to the processing of all or part of their personal data
- Correction of false or misleading data
- Deletion of false or misleading data about them.



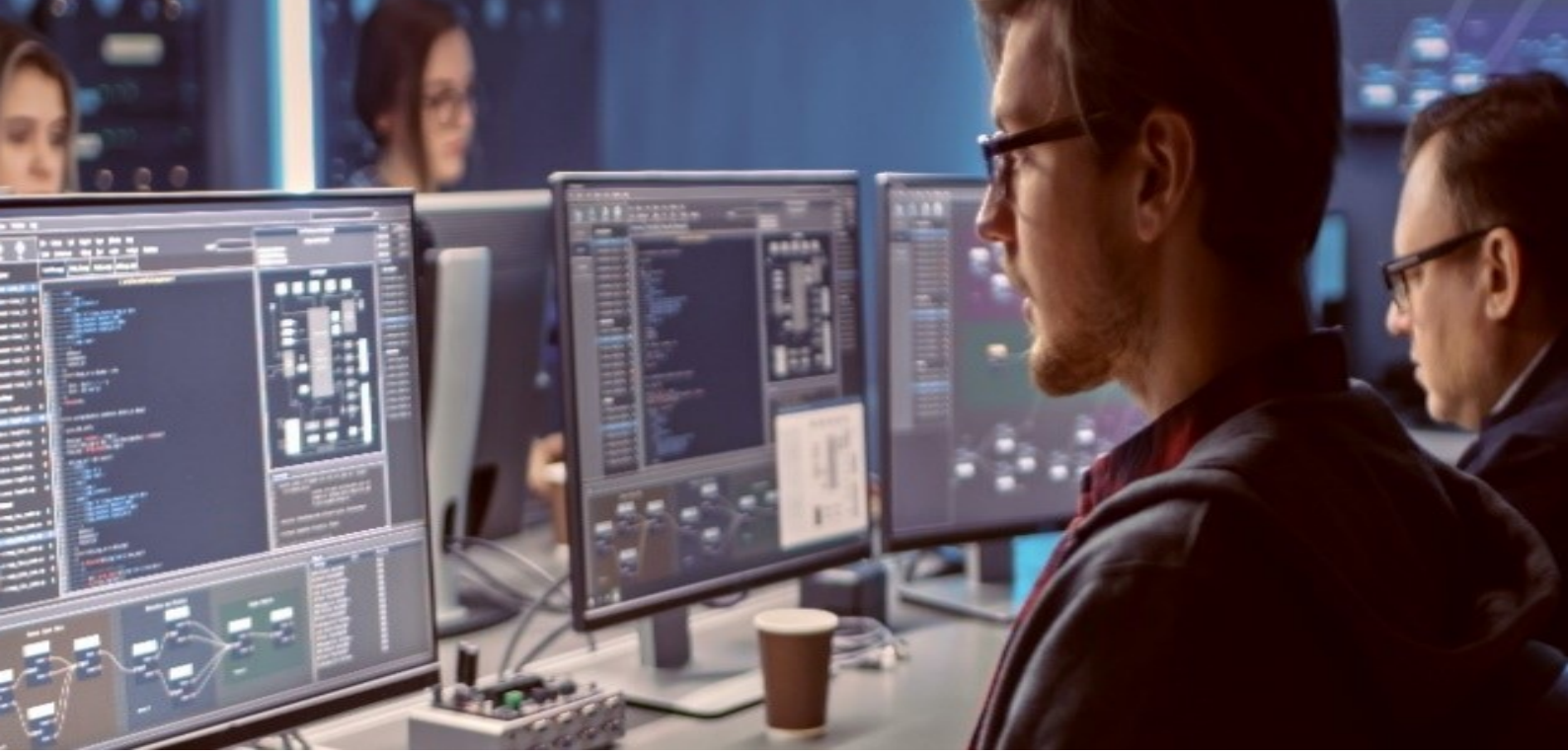
Personal Data Protection Principles

Every Data Controller or Data Processor shall ensure that personal data is:

- Processed in accordance with the right to privacy of the Data Subject
- Processed lawfully, fairly and in a transparent manner in relation to any Data Subject
- Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed
- Collected only where a valid explanation is provided whenever information relating to family or private affairs is required
- Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay
- Kept in a form which identifies the Data Subjects for no longer than is necessary for the purposes which it was collected
- Not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the Data Subject.

What does Consent means?

Consent is 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 personal data relating to the Data Subject.



Data Protection Act, 2019

What Grant Thornton will do?

Grant Thornton can help you to assess, analyse, identify, develop and deliver the required governance framework, policies, procedures and detailed implementation plan for achieving compliance with Kenya's Data Protection Act. Services offered by Grant Thornton include:

1. **Legal and Regulatory Advice.** We can provide you with legal and regulatory advice on how to comply with the Data Protection Act.

2. **Record of Personal Data processes activities.** We can help you develop a record detailing all processes and systems which collect or process personal data for your organization. This may include departments such as Finance, Human Resources & Administration, Information Technology, Compliance, Operations, Risk Management, etc.

3. **Gap Assessment and Implementation Roadmap.** We can help you assess your current data policies and practices against the requirements of the act resulting in GAP Assessment Report and an implementation roadmap.

4. **Data Protection Framework.** We can help you develop a data protection framework that will include the data protection policies and procedures and the data protection governance structures defining the roles and responsibilities.

5. **Privacy Notices and Third-Party Contracts**. We can help you develop privacy notices for the Data Subjects, Employees, Job Candidates, Third-Parties, Customers and the organizations Website.

6. **Data Protection Impact Assessment.** We can help you to identify and assess high risk personal data processing activities.

7. **Awareness and Training.** We can provide training to staff and stakeholders to create awareness of the Data Protection Act.

Contact us

Parag Shah
Partner
T: +254 722 742 026
E: parag.shah@ke.gt.com

Vivek Patel
Associate Director – Advisory
E. vivek.patel@ke.gt.com
T: +254 723 897 782

Address:

Nairobi
5th Floor
Avocado Towers
75 Muthithi Road, Westlands
P.O. Box 46986 – 00100
Nairobi, Kenya

T +254 20 3747681
T +254 20 699539
T +254 728 960963

W www.grantthornton.co.ke
E info@ke.gt.com

Kampala
2nd Floor, Wing B&C
Lugogo House
42, Lugogo Bypass
P.O. Box 7158
Kampala, Uganda

T +256 200 907333
T +256 414 535145
T +256 312 266850

W www.gtuganda.co.ug
E info@ug.gt.com

Dar es Salaam
207 Viva Towers
Ali Hassan Mwinyi Road
P.O. Box 443
Dar es Salaam, Tanzania

T +255 784 936888

Grant Thornton

grantthornton.co.ke