Activity supported by the
Canada Fund for Local Initiatives
Activité réalisée avec l'appui du
Fonds canadien d'initiatives locales

Canada

ELGIA
ELECTORAL LAW AND GOVERNANCE
INSTITUTE FOR AFRICA

DATA PROTECTION ACT 2019

ABRIDGED VERSION

Primary legislation governing data privacy in Kenya

Contents

Introduction

Kenya's Data Protection Act came into effect in November 2019, ushered the country into a new data privacy dispensation that aimed at ensuring Kenyans were empowered with enforceable privacy rights over their personal information, while providing clear guidelines for private and public institutions to handle their users' data with care.

The Kenyan Data Protection Act (DPA) applies to data controllers and processors and provides data subjects with certain rights and safeguards.

Why the Act?

Objective of the Data Protection Act 2019

The main objective of the Data Protection Act 2019 is to protect your rights as a data subject over the usage of your personal information which is collected, stored or used by a company, app or website.

The Act sets out the rights of data subjects and obligations of data controllers and processors to safeguard individual privacy through establishment of institutional mechanisms and enforcement.

Key Definitions

Who is a data subject?

As per Section 2 of the Kenyan Data Protection Act, 2019, a data subject is "an identified or identifiable natural person who is the subject of personal data." In simpler terms, the data subject is the individual person to whom the personal data collected relates to.

If a piece of information can be linked back to you, you are the data subject. The entire Act is built around protecting the rights of the data subject.

What is personal data?

Any information relating to an identified or identifiable natural person. For example, a person's full name, identity card number, date of birth, gender, physical and postal address, phone number, location data, an online identifier.

Personal data doesn't have to be in written form, it can also be information about what a data subject looks or sounds like, for example biometrics, genetic data, photos, audio or video recordings.

What is sensitive data?

Under the Data Protection Act, 2019 (DPA), this means data revealing a person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of a person's children, parents, spouse or spouses, sex, or sexual orientation.

It is personal data that requires additional protection due to the high risk an individual is likely to face if it is accessed by unauthorized persons/ entities.

What is a data controller

A data controller is a person or organization that collects personal information from others for a specific purpose. A data controller decides on the nature of information collected, its usage, and protection thereof.

An example of a data controller is an NGO collecting project beneficiaries' names and contacts during the implementation of its program

Who is a data processor?

A data processor, on the other hand, is a person or organization that handles or uses the collected data on behalf of the controller.

Processes the data in accordance with the instructions of the data controller, for example, a telecom company disbursing funds to the beneficiaries of the NGO program, processing payments using the collected contacts from the NGO.

The Office of the Data Protection Commissioner (ODPC)

What is the role of the Office of the Data Protection Commissioner?

The Office of the Data Protection Commissioner (ODPC) is established in accordance with Article 260 (q) of the constitution. The office is headed by a Data Commissioner. The purpose of this office is to oversee implementation and enforcement of the Data Protection Act.

What are the functions of the Data Protection Commissioner?

1. Establishment and maintenance of data controllers and data processors register.
2. Exercise oversight on data processing operations, either of own motion or at the request of a data subject.
3. Promote self-regulation among data controllers and data processors
4. Conduct assessments/checks to ensure organizations handle information legally and correctly.
5. Receive and investigate any complaint by any person on infringements of the rights under this Act
6. Educate the public on their data rights and how to stay safe online
7. Carry out inspections of public and private entities with a view to evaluating the processing of personal data.
8. Promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements.
9. Perform such other functions as may be prescribed by any other law or as necessary for the promotion of objects of this Act.

Data Controllers and Processors

What is expected of the Data Controller or Processor?

Registration

Data controllers and processors must register with the Data Commissioner.

Duty to Notify

Data subjects must be informed about the collection and processing of their data.

Data Protection Impact Assessment

Required for processing operations likely to result in a high risk to the rights and freedoms of data subjects.

Data Protection by Design and by Default:

Data controllers must implement appropriate technical and organizational measures to ensure data protection is integrated into the processing system from the outset.

Breach Notification

The Data Commissioner and the affected data subjects must be notified without undue delay upon becoming aware of a personal data breach.

How do you register to be a data controller or processor?

- Applications are submitted electronically through the ODPC's website *(https://www.odpc.go.ke/)* in the prescribed form and payment of registration fees. The required organisational details must be submitted as well as a description of the processing activities.
- Where the Data Commissioner is satisfied that the applicant has fulfilled the requirements, a certificate of registration will be issued within 14 days and an entry of the details of the applicant will be made in the register of data controllers and data processors.
- The certificate of registration will be valid for a period of 24 months from the date of issuance. A certificate of registration is renewable every 24 months and an application for renewal will need to be made at the appropriate time.
- Where the data commissioner is dissatisfied and rejects the registration application, the Data Commissioner shall notify the applicant within 21 days and provide reasons. Where the application had been declined, the applicant may make a fresh application.

How much is the registration fee?

The registration fees depend on the category within which the data controller or data processor falls. The Registration Regulations classifies profit-making or private sector data controllers and data processors for purposes of registration into three tiers:

- Micro and small data controllers /processors, (those with an annual turnover/revenue of Kshs. 5 million and 1 to 50 employees);
- Medium data controllers /processors (those with an annual turnover/revenue of above Kshs. 5 million but less than Kshs. 50 million and 51 to 99 employees);
- Large data controllers and processors (those with an annual turnover/revenue of more than Kshs. 50 million and more than 99 employees);

Public entities and non-profit making entities such as charities; and religious entities (regardless of revenue/turnover) are also required to register.

What are the fines and penalties for non compliance?

Fines:

Person who obstructs or impedes the Data Commissioner in the exercise of powers e.g. fails to provide assistance or information requested, refuses to allow the Data Commissioner to enter any premises or gives information which is false or misleading in any material aspect, 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 both.

Penalty Notice:

If the Data Commissioner is satisfied that a person has failed or is failing as described in section 58, the Data Commissioner may issue a penalty notice requiring the person to pay to the Office of the Data Commissioner an amount specified in the notice.

Administrative Fines

In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

General Penalty

A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.

Right of Appeal

Any person aggrieved by a decision of the Data Commissioner has the right to appeal to the High Court.

You as the Data Subject

What are your rights as a data subject?

The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects them.

The right to be notified about the collection and use of their personal data.

The right to obtain confirmation as to whether their personal data is being processed and to access that data.

The right to have inaccurate data corrected and the right to have their personal data erased (the “right to be forgotten”) under certain conditions.

The right to object to the processing of their personal data, including processing for direct marketing.

The right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller.

What is my "right to be forgotten" and how can I use it to have old or embarrassing posts, photos, or data deleted from a platform?

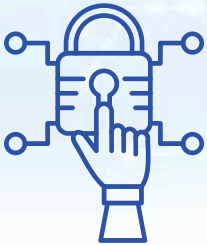
Under the Kenya Data Protection Act (2019), you have the right to be forgotten. This means you can ask for your personal data to be deleted when it should no longer be online or used. You can ask a platform (like a social media site, app, or website) to remove your posts, photos, videos, or personal information if:

- The data is no longer needed for the reason it was collected
- The data was used unfairly or illegally
- Keeping it online violates your privacy rights
- The information is old, embarrassing, misleading, or harmful
- You decide to withdraw your consent
- The data was posted when you were a child or minor

However, this right is not absolute — data may stay online if needed for legal reasons, public interest, or freedom of expression. Screenshots or re-shares by other people may still exist, but platforms must remove what they control.

Does the Act prevent companies from using my personal data like my location, browsing history, or social media activity to create a "profile" of me that could lead to discrimination e.g., being denied a service or charged a higher price?

The Kenya Data Protection Act (2019), prohibits companies from freely using your personal data like location, browsing history, or social media activity to profile you in a way that is unfair, harmful, or discriminatory.



Can a data controller e.g., a dating app or a mental health service process my sensitive personal data without my explicit consent?

Can a data controller e.g., a dating app or a mental health service process my sensitive personal data without my explicit consent?

If my data rights are violated, how do I file a complaint with the Data Commissioner, and is there a cost involved?

If a company or organization misuses your personal data or ignores your data rights, you can lodge an online complaint on the Office of the Data Protection Commissioner (ODPC) portal. Filing a complaint is free

How do you file a Complaint?

- Before complaining with the ODPC, try to ask the company to fix the issue
- Keep screenshots, emails, or messages as evidence
- Prepare your information e.g., name, contact details, details of the offending app or company, clear explanation of the offence, evidence, and what action want taken.
- Submit a complaint to the ODPC online portal, email or physical submission to the ODPC offices
- You don't need a lawyer or legal language

What are the penalties for data handlers who misuse my data, can I receive compensation if I suffer harm due to a data breach?

If a data controller or processor breaks the rules of the Data Protection Act, the Data Protection Commissioner (ODPC) can;

- Impose administrative fines for non-compliance.
- Impose general penalties for unlawful disclosure of personal data and other offenses
- Award compensation for damages
- An aggrieved person by a decision of the Data Commissioner has the right to appeal to the High Court.

Cross-Border Data Transfer

- Data Controllers are only allowed to transfer data outside Kenya if they can prove to the Data Commissioner that the data will be safe and protected through evidence of strong safeguards and especially if the recipient country has similar data protection laws to Kenya.
  Necessary transfer of cross-board data transfer may be permitted in case of; fulfilment of contract, to protect the safety and life of a subject, public interest reasons, legal cases or legitimate reasons that the transfer does not harm the rights of the subject.

- Sensitive personal data needs extra care. It can only be transferred outside Kenya if the person gives consent and strong security measures are in place.

- The Data Commissioner can ask for proof that the data is well protected and can stop or limit the transfer if people's rights are at risk.

- The government can require certain types of data to be processed only on servers located in Kenya to protect national interests or revenue.

Contacts

Drop us a line
info@elgia.org

Give us a call
+254 (020) 367-3903

Office Location
CVS Plaza, Lenana Rd.

WITH SUPPORT FROM

Activity supported by the
Canada Fund for Local Initiatives

Activité réalisée avec l'appui du
Fonds canadien d'initiatives locales

Canada