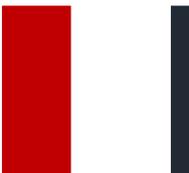


ONG'ANYA OMBO
ADVOCATES

Data Protection Act, 2019



About Us

Ong'anya Ombo Advocates specialises in proffering Strategic Legal Services to both natural and juristic persons in the Republic of Kenya, and beyond.

Our Contacts

Ong'anya Ombo Advocates
Windsor House, 4th Floor,
University Way/ Muindi Mbingu Street,
P.O. Box 15598 – 00400
Nairobi

e: hello@onganyaombo.com

w: www.onganyaombo.com

m: +254 703 672515

Ong'anya Ombo Advocates © 2019

Images: Pixabay

DISCLAIMER: Take note that the information herein is not intended to serve as a legal opinion or advise, and should you need any clarity or understanding of what this information is about, you are advised to seek professional advice from your legal advisor, lawyer, or the professional person that you deem fit in reference to the questions that you have. In addition, you, inclusive of your representatives, agents, assigns, or whosoever, agree that, should you rely on this information, you shall not hold us liable, be it directly or indirectly.

Data Protection Act, 2019

Introduction

Information Communication Technology is a result of continuous innovation that has resulted in a need to access immense data for purposes of companies or individuals conducting both legal and illegal activities.

All over the world, there has been an intensive focus on how data is being harvested and used, which has resulted in various laws, directives, or regulations. Recently, the European Union implemented the General Data Protection Regulations (GDPR); California, USA, has the California Consumer Privacy Act; the Republic of Kenya has Data Protection Act, 2019, among others.

In this discussion, the content will be about the Data Protection Act, 2019 (DPA) that was assented to law by President Uhuru Muigai Kenyatta on November 08, 2019.

The DPA actualises Article 31 (c) and (d) of the Constitution for purposes of protecting the data of the persons whom the laws of Kenya apply. The DPA adopts an immense character from the GDPR, which has had tremendous traction since it was approved on April 27, 2016, and came to effect on May 25, 2018, and the repealed Data Protection Directive 95/46/EC.

It is imperative to note the DPA stretches to adopt practices based on Commission Decision 2000/520/EC (popularly known as the Safe Harbour Regulations) that was succeeded by the Privacy Shield before being rendered nugatory by the GDPR.

For purposes of this Question & Answer, focus will be towards the Functions of the Data Commissioner, Part II; Registration of Data Controllers and Data Processors, Part III; Principles and Obligations of Personal Data Protection, Part IV; Grounds for Processing of Sensitive Personal Data, Part V; Transfer of Personal Data, Part VI; Exemptions, Part VII; and Enforcement Provisions, Part VIII.

“One cannot step twice in the same river.”

Heraclitus (ca. 540 – ca. 480 BCE)

Data Protection Act, 2019

What are the functions of the Data Commissioner?

The Data Commissioner (the Officer) will oversee the implementation and enforcement of the DPA – the enforcement and assessment will either as requested or on its own motion. To do so, the Officer will ensure that there is a register entailing details of Data Controllers and Processors. Therefore, the Officer must make sure that the public is well informed about the DPA.

Enhance the idea of Self-Regulations among Data Controllers and Data Processors. It is quite similar to the defunct Safe Harbour Regulations and Privacy Shield that applied between the US and EU - tainted by scandals over Data Breach under the Safe Harbour Regulations.

Data Commissioner will always be open to receive complaints and investigate. Further, it will have the power to conduct inspections towards Government and Private entities on how the DPA is being applied. It reflects the fact that the Constitution of Kenya applies vertically and horizontally.

The Officer will ensure that there is international cooperation on matters Data Protection. It will be with regards to the international conventions and agreements and enhance Research and Development (R&D).

The Data Commissioner's office is independent. However, where the need is, it will collaborate with the National Security Organs.

What are the Powers of the Data Commissioner?

Initiate investigation after a complaint being filed or on its own motion, seek professional assistance, provide room for Alternative Dispute Resolution, issue summons to a witness, seek information as per the DPA, impose fines, effect any power as per the DPA and any law that provides the Officer with specific capabilities.

To enhance its purpose, the Officer will enter into various associations with various entities in and outside Kenya.

You are wondering what will be factored by the Data Commissioner?

To be registered as a Data Controller or Processor, the Data Commissioner will consider the industry, the volume of data, any sensitive data, and among other factors, the Data Commissioner may deem fit.



What will you provide as an intended Data Controller or Processor?

The Data Commissioner will be interested in the description of the personal data to be processed by the Data Controller or Processor, purpose of processing, category of data subjects, contact details of the Data Controller or Processor, general information on security factors and mechanism put in place, measures to compensate in the event of data breach, and any information as requested by the Data Commissioner.

The Data Controller or Processor that meet the requirements will be issued with a certificate. In the event of any developments that require notifying the Data Commissioner, the Data Controller or Processor should notify immediately – the register will be amended to meet the new developments.

Considering the changes that occur during data controlling or processing, it might result in the cancellation or variation of the certificate.

Anyone who knowingly provides false, misleading information or fails to comply will be considered to have committed an offence.

Will the Register be Private or Public?

The Register will be public and open for updating as per the request of the relevant Data Controller or Processor. In the event a person needs a certified copy of any entry of the Register, such an application may be made to the Data Commissioner.

Will it be appropriate to appoint Data Protection Officer by Data Controller or Processor?

Save where the Courts are acting in their Judicial capacity, a Data Controller or Processor may appoint or designate a Data Protection Officer (DPO) on covenants as the Data Controller or Processor may determine. It applies where the Data Controller or Processor is handling sensitive data, or its core activity entails require regular and systematic monitoring data subjects.

Data Controller or Processor may appoint staff as a DPO and may conduct other duties as long as there is no conflict of interest. A group of entities may appoint one DPO. In the event it is a Public body, there can be one DPO for more Public authorities.

A person may attain the status of a DPO if the person has the relevant academic background or professional skills.

The information about the DPO will be provided under the website and communicate to the Data Commissioner. The current practice is that the DPO contacts are always under the Privacy Policy on the site of the entity.



As a DPO, what are my duties?

Advise on matters on data laws to the Data Controller or Processor and its employees; the DPA is complied with, facilitate capacity building of staff on data laws, and cooperate with the Data Commissioner.

What are the Principles of data protection?

It is the duty of the Data Controller or Processor to ensure that personal data is processed in consideration to right to privacy; lawfully, fairly and transparent; collection is specific to the

purpose; adequate, relevant and limited to its use; valid explanation issued to collect private or family information; accurate and up to date while inaccurate is erased; with identifies but for a specific period; not transferable outside Kenya save where there is adequate protection or consent of the data subject is acquired.

What are the Rights or ways to exercise the Rights of the data subject?

The Data Subject must be informed how the personal data is to be used, right to access the data under the Data Controller or Processor, object to the processing of part or all of their data, correction of data, and deletion of false or misleading data.

A minor will have his or her rights realised through the parent or guardian; a person experiencing mental challenges or such will exercise through a guardian or administrator; or a person duly authorised by the Data Subject.

How can one collect personal data?

Personal data will be collected directly from the Data Subject or indirectly from a public record, deliberately made public, where consent is issued, the data subject has incapacity, if where collected from it will not prejudice Data Subject and necessary to enhance law or public protection.

What kind of notification does a Data Controller or Processor need to give to a Data Subject?

In the event of the need to collect personal data, it is essential that – if practical – inform the Data Subject of the rights as per s 26 of the DPA, data is being collected, purpose, third parties that will or has receive(d) the data, safeguards in place, contacts of the Data Controller or Processor, the organisation technological infrastructure on matters data protection, whether the collection is as per law and voluntary or mandatory, and consequences of failure to comply.

What amounts to the lawful processing of personal data?

The Data Subject consents for a specific purpose; or the processing is necessary to the performance of a contract, legal compliance, protection of Data Subjects interest, performance of a task by

a Public Authority, public interest, legitimate interest, and acceptable research.

It is an offence to contravene these provisions.

What happens if the model of data control or processing has high chances of a data breach?

The Data Controller or Processor is required to conduct a thorough data protection impact assessment, which will address operation and purpose, proportionality test, assessment of the risks, measurements to address the risks.

The Data Controller or Processor should consult the Data Commissioner and present the report sixty days before the intended processing of data.

What are the conditions of consent?

It is upon the Data Controller or Processor to prove that consent was acquired, importantly, as per the law – freely given. Also, it is imperative to note that regardless of giving consent, it can be withdrawn.

The withdrawal of consent will not affect the lawfulness of processing information based on initial consent.

What about processing personal data concerning a child?

The parent or guardian issues the consent, and the processing must be done in a manner that protects and advances the interests of the child. Therefore, it is required that there be age verification and consent to process the data of a child.

Can there be restrictions on processing data?

In the event a data subject requests to restrict processing of their data if the accuracy of the data is contested, the information is no longer required for the processing, the processing is unlawful, the data subject has objected to the processing.

Once a restriction is in place, the data will only be processed upon meeting the set legal requirements, and in the event of lifting the restriction by the Data Controller must inform the Data Subject.

Does the law restrict the commercial use of data?

A person will not utilise any data for a commercial purpose unless it secures express consent from the data subject, or allowed as per a specific law and the data subject is informed of the use when collecting.

A Data Controller or Processor that utilises data for commercial purposes will have to remove all identifiers about the data subject.



What does it mean by the Right to data portability?

The Data Subject has the right to ask for its personal data, which must be provided in a manner that a person can read – and understand. The Data Subject can share the information with another Data Controller or Processor, or have one Data Controller or Processor send it to another similar entity. If the initial Data Controller or Processor declines, the Data Commissioner may be involved to address the situation at hand.

What are the limitations on retention and right of rectification and erasure?

The Data Controller or Processor will hold the information as long as it is reasonably necessary for its intended purpose unless authorised by law, lawful purpose, authorised or consented by Data Subject, or for historical, statistical, journalistic literature and art or research purpose.

Any data that is not necessary for retention will be deleted, erased, anonymised, or pseudonymised.

The Data Subject may request that information held about oneself be rectified or erased without delay. The Data Controller or Processor will be

required to contact any third party to have all information rectified or erased as proposed.

What amounts to data protection by design or by default?

Data Controller or Processor must effect appropriate measures that will enable the enhancing the protection principles and integrate safeguards to strengthen the purpose of the DPA.

These will involve organisational and technical factors like credible technological infrastructure.

What types of notifications must be issued in the event of a breach?

If there is a data breach that can result in risk or harm of the Data Subject personal data, the Data Controller is required to notify the Data Commissioner within 72 hours and proffer more details to make it clear to the Data Commissioner. In the event of any delay, the Data Controller must give reasons for the delay.

The Data Controller ought to inform the Data Subject within a reasonable time unless it is hard to establish the Data Subject. However, the Data Commissioner may restrict the issuance of notice to the Data Subject.



What are the permitted grounds for processing sensitive personal data?

The processing of sensitive data is restricted unless s 25. Sensitive data as per s 2 of the DPA 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.

Sensitive Data can be processed in the course of legitimate activities by non-profit organisations with a political, philosophical, religious or trade union as long as it focuses on members of that organisation or has regular contact with the organisation and it is not disclosed without the consent of that person.

The Data Subject's sensitive data will be collected or processed for purposes of legal claims, exercising specific rights, or realising vital interest.

Further, sensitive data can be collected and processed by a health facility.

What are the conditions for the transfer of data out of Kenya?

Once the Data Controller or Processor provides proof to the Data Commissioner on the appropriate data safeguards that have been put in place and the jurisdiction to be transferred as similar or better data protection safeguards and that the transfer is necessary.

What exemptions are available?

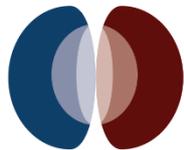
The DPA applies on all matters pertaining to data; however, data collection based on purely personal household activity, national security or public interest, or disclosure as per the law (written or Court order).

The DPA will not apply to certain aspects of journalism, literature, and arts; and on research, history, and statistics. However, the Data Commissioner will provide the required regulations to guide on such matters. Besides, for purposes of Data-Sharing, the Data Commissioner will be required to prepare the Data-Sharing Code.

What are the enforcement mechanisms?

A Data Subject or person who finds a specific Data Controller or Processor's conduct infringing his/her rights, may lodge a complaint with the Data Commissioner. It will be investigated, and if there is a case, notices will be issued for purposes, and, if found in violation, there will be penalties and compensation to Data Subject.

An aggrieved party by the decision of the Data Commissioner can appeal to the High Court.



ONG'ANYA OMBO
ADVOCATES

4th, Windsor House,
The junction at University Way and Muindi Mbingu Street,
P.O. Box 15598 – 00400
Nairobi, KENYA.
Office: +254 703 672 515

e: hello@onganyaombo.com
w: www.onganyaombo.com