BARIZI
DATA
PRIVACY
SERVICES

DATA PROTECTION HANDBOOK

INTRODUCTION

1. BACKGROUND

The information age has resulted in a tremendous growth of personal and sensitive information shared online through app and websites. While this trend has made certain services accessible to most of the population in a now globalized world, the risks related to such sharing continue to rise. From phishing attacks, ransomware, identity theft and sale of personal data companies and individuals are left vulnerable. Emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML) and Large Language Models (LLMs) also make it crucial for governments, individuals and companies to take data protection into consideration in their activities.

In Kenya, the foundation of data protection can be traced to Article 31 of the Constitution 2010 which guarantees the right to privacy. This right under the constitution include the right to privacy of self and possession, right not to have an individuals family details disclosed without their prior authorization and the protection of individuals communication devices from unauthorized access. This essentially prevents persons, groups, organizations, or unscrupulous persons from using an individual's personal data for their own use and without consent from the individual.

To facilitate respect to the right to privacy of an individual, the Data Protection Act 2019 was enacted. The Act breathes life into the provisions of Article 31 of the constitution by requiring all persons (Legal & Juristic) to process personal data as per the laid down principles and bases under the Act. The Act also establishes the Office of the Data Protection Commissioner which is responsible for implementation and enforcement of the Act.

2. OBJECTIVES OF THIS HANDBOOK

This handbook seeks to provide a quick and easy to read guide relating to compliance with the Data Protection Act 2019. It shall highlight the various obligations and requirements under the Act, as well as breakdown the main concepts and principles relating to data protection.

3. WHY IS THE DATA PROTECTION ACT IMPORTANT?

Data has been dubbed "the new oil" owing to the value it creates upon exploitation and analysis. Companies can now derive consumer insights and preferences through data analysis making personal data an essential commodity in the delivery of good and services. Although the use of personal data to inform business decisions is a welcome approach, available literature and decisions by Data Protection Authorities across the globe show there is evidence of the misuse of personal data by companies and the exposure of individuals to risks such as fraud and identity theft. The evolving threat landscape and the value of personal data to perform various tasks and functions in our day to day lives warrants its protection and security.

4. DEFINITION OF TERMS

Some key terms relating to data protection:

1

Data

Information which is processed by means of equipment operating automatically in response to instructions given for that purpose; or information that is recorded with intention that it should be processed by means of such equipment; or information that is recorded as part of a relevant filing system;

2

Data Controller

a person (natural or legal), public authority, agency or other body which determines the purpose and means of processing of personal data;

3

Data Processor

A person (natural or legal), public authority, agency or other body which processes personal data on behalf of the data controller;

4

Data Subject

An identified or identifiable natural person who is the subject of personal data. Essentially this refers to the person whose data you are collecting;

5

Data Controller

a person (natural or legal), public authority, agency or other body which determines the purpose and means of processing of personal data;

6

Processing

any operation or sets of operations which is performed on personal data, whether or not by automated means, including: -

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

7

Sensitive Personal Data

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.

5. SOME KEY ASPECTS OF THE ACT

5.1 PRINCIPLES OF DATA PROTECTION

The Act introduces the principles of data protection, which are reflected throughout the Act itself. These principles include:

- **Lawfulness, fairness, and transparency:** Data should be processed lawfully, fairly, and in a transparent manner. For instance, a valid explanation should be provided whenever information relating to family or private affairs is required, as well as the reason for processing. This can be achieved through the use of Privacy Notices/Policies, which must be displayed at a location that is visible and in simple language. The use of privacy notices allows individuals (data Subjects) to make informed decisions.

- **Purpose limitation:** When an organization intends to process personal data, it must determine the purpose of such processing prior to the processing. Additionally, that personal data must be collected for an explicit, specified and legitimate purpose. The second limb of this principle requires the personal data not to be further processed in a manner incompatible with the original purpose of collection. For example, if a customer pays for a service at your company using mobile money, it will be unlawful for you to use that data to send marketing or promotional messages to them.

- **Minimization:** The principle of minimization dictates that only necessary personal data should be collected for specific purposes. For example, when an online retailer collects a customer's name, address, and payment details for the purpose of processing and delivering an order, they should not request additional information that is unrelated to this specific transaction, such as the customer's medical history.

- **Accuracy:** This principle demands that collected personal data be accurate and, where necessary, regularly updated. For instance, a healthcare provider must ensure that a patient's medical records are kept up to date with accurate information about their allergies,

medical conditions, and current medications etc.

- **Storage limitation:** This principle stipulates that personal data should not be retained for longer than necessary for the purposes for which it was collected. An example is a financial institution storing a customer's transaction records for a legally mandated period and then securely disposing of the data once this retention period has expired.

- **Non-transferability:** This principle restricts the transfer of personal data beyond national borders, with few exceptions such as when adequate data protection safeguards are in place or when the data subject has provided explicit consent. An example is a multinational company obtaining explicit consent from its employees before transferring their personal data to its overseas subsidiaries.

- **Right to Privacy:** The principle of privacy mandates that personal data should be processed in a manner that respects and safeguards the privacy rights of the data subject. For instance, a social media platform must ensure that it complies with privacy regulations and user preferences regarding the collection, use, and disclosure of personal data.

5.2 RIGHTS OF DATA SUBJECTS.

The Data Protection Act Kenya 2019 provides a comprehensive framework to protect the personal data of individuals and grants specific rights to data subjects regarding the processing of their personal information. These rights are designed to empower individuals, enhance their control over the use of their personal data, and ensure that their privacy and data protection rights are upheld in accordance with the law. In this section, we examine the data protection rights granted to data subjects under the Data Protection Act Kenya 2019, providing detailed explanations and examples to elucidate the practical application of these rights in safeguarding individuals' personal information.

- **Right to be informed:** Data subjects have the right to be informed about how their personal data will be used. This includes the obligation for data controllers to provide individuals with clear and transparent information regarding the purposes for which their data will be processed, the legal basis for processing, the retention period of the data, and any third parties with whom the data may be shared.

- **Right of access:** Individuals have the right to access the personal data held about them by data controllers or processors. This right enables individuals to obtain confirmation of whether or not their data is being processed, access a copy of their personal data, and obtain information about the purposes of the processing.

- **Right to object:** Data subjects have the right to object to the processing of their personal data, including profiling and direct marketing. This right allows individuals to object to the processing of their data for specific purposes, such as marketing activities, and prohibits further processing of their personal data unless the data controller demonstrates compelling legitimate grounds for the processing.

- **Right to rectification:** Individuals have the right to have inaccurate or incomplete personal data corrected. This empowers individuals to request the rectification of any inaccurate or outdated information held about them by data controllers. Where such restrictions apply, the personal data shall only be processed with the data subject's consent or for the establishment, exercise or defense of a legal claim, the protection of the rights of another person or for reasons of public interest.

When does restriction apply?

Restriction applies where:

a. the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;

b. the personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defense of a legal claim;

c. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

d. the data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

Koros Kiprotich vs Higher Education Loans Board (ODPC Complaint No. 0781 of 2023)

The Complainant in this case alleged that the Respondent failed and/or neglected to update his loan repayment information yet he had cleared all his Higher Education Loan Board arrears and was issued a Credit Reference Bureau clearance certificate.

The Respondents having been registered as Data Controllers with the ODPC, have a responsibility of constantly ensuring that the personal data it processes is accurate and up to date.

In the instant case the Respondents aver that they failed to update their records even though the Complainant cleared his arrears, therefore, the ODPC found that they had violated the Complainant's right to correction and rectification of their personal data.

The ODPC issued a directive to the Respondent that within seven days they ought to have updated/rectified their records to ensure that the Complainant's personal data shared with third parties was accurate and failure to which an enforcement notice would be issued.

- **Right to erasure:** Data subjects also have the right to request the deletion or removal of their personal data

where there is no compelling reason for its continued processing. This right, also known as the "right to be forgotten," enables individuals to request the removal of their personal data from a company's systems, especially after terminating a service or contract, unless there are overriding legitimate grounds for the processing.

- **Right to data portability:** Data subjects have the right to obtain and reuse their personal data for their own purposes across different services. This right allows individuals to obtain, move, copy, or transfer personal data easily from one environment to another in a safe and secure way without hindrance to usability. When enabling this right, the data controller or processor should share this information in a machined readable format. The Act however, doe not define what such format encompasses. Additionally, it is important to note that this is the only right under the Act that could incur charges before it is enabled.

- **Right to restriction of processing:** Data subjects have the right to request the restriction of processing of their personal data. This means that an individual can request the temporary suspension of the processing of their personal data, for example, while they verify the accuracy of their data or if they object to the lawfulness of the processing. Restriction of personal data will apply to all places where this data is processed, including where a processor or third party is involved. This means that, once a data controller receives a request for the restriction of processing, they must notify all relevant parties to restrict or suspend the processing of that data.

- **Right to lodge a complaint:** Individuals have the right to lodge a complaint with the Data Protection Commission if they believe that their rights under the Data Protection Act have been infringed. This includes the right to seek compensation if their personal data has been processed unlawfully or in violation of their data protection rights.

6. LAWFUL BASES FOR PROCESSING PERSONAL DATA

Any form of processing of personal data is required to be undertaking in accordance with the Act. Some of the conditions that are required to be met prior to processing personal data, include that:

a. there is consent to the processing; or
b. the processing is necessary for;

1. the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
2. compliance with any legal obligation to which the data controller is subject;
3. in order to protect the vital interests of the data subject or another natural person;
4. the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
5. the performance of any task carried out by a public authority;
6. the exercise, by any person in the public interest, of any other functions of a public nature;
7. the legitimate interests pursued by the data controller or processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
8. the purpose of historical, statistical, journalistic, literature and art or scientific research.

In the following section, we will look at the lawful bases in-depth.

6.1 CONSENT

Consent is a crucial element in the processing of personal data under the Data Protection Act. To be considered valid, consent must meet specific criteria, namely being express, unequivocal, freely given, and informed. This means that individuals must clearly and explicitly agree to the processing of their personal data, understanding the implications and freely choosing to provide consent without any form of coercion.

Valid consent can be provided through either a statement or a clear affirmative action signifying agreement to the processing of one's personal data. The Act does not prescribe a specific method for obtaining consent, allowing for various means that meet the necessary requirements, such as providing a signature or using a check-box to indicate consent.

What is a clear affirmative action?

A clear affirmative action, as outlined in the context of the Data Protection Act, refers to an unmistakable and positive indication from an individual signaling their agreement to the processing of their personal data. This action should leave no room for ambiguity and should unambiguously demonstrate the individual's consent.

Examples of clear affirmative actions may include:

1. Checking a box on a website to indicate consent to the processing of personal data.
2. Selecting particular settings or options in an online account or application to signify agreement to data processing activities.
3. Actively signing a consent form or document either physically or electronically.
4. Verbal confirmation in a recorded phone conversation or in person.
5. Taking specific steps such as pressing a button or clicking on an option to indicate consent.

It is also important to note that individuals always retain the right to withdraw consent previously given at any time. The withdrawal of consent should not affect the lawfulness of processing based on prior consent. The ability of the individual to withdraw their consent at any time emphasizes the ongoing control that individuals have over the use of their personal data as anticipated by the Act.

As a data controller or processor, the Data Protection Act places the burden of proof to demonstrate that consent was obtained. This underscores the importance of documenting all consents received as such a record will be crucial where a compliant is made against you.

Eric Migwi and Scholastica Onon vs f Company Limited (ODPC Complaint No. 0646 of 2023 as consolidated with ODPC Complaint No. 0719 of 2023)

The Complainant in this case alleged that they had been receiving incessant messages from the Respondents demanding payment from them as guarantors of loans which they knew nothing of. The Complainants alleged that they had not given their consent to being guarantors of loan applicants by the Respondent.

The Respondent did not adduce any evidence to show that the Complainants consented to the processing of their personal data by the Respondent.

In its determination the ODPC relied on Section 2 of the Data Protection Act which defines consent to mean, '*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.*' The ODPC found that the Respondent had not discharged the burden of proof of consent as required under section 2 of the Data Protection Act.

Therefore, having established that there is no proof of consent to the processing of the personal data by the Respondent, the ODPC found the Respondent liable for

unlawful processing and issued an enforcement notice against the Respondent.

6.2 PERFORMANCE OF A CONTRACT.

This lawful basis is applicable when the processing of personal data is necessary for the performance of a contract to which the data subject is a party or when taking pre-contractual steps at the request of the data subject. For example, a company processing personal data to fulfill an order made by a customer or to carry out the necessary obligations under a service agreement.

6.3 LEGAL OBLIGATION

This lawful basis applies when the processing of personal data is necessary for the data controller to comply with a legal obligation. For example, a financial institution processing customer data to fulfill its legal obligations under anti-money laundering regulations.

6.4 VITAL INTERESTS

This lawful basis is relevant when processing personal data is necessary to protect the vital interests of the data subject or another individual, particularly in urgent or life-threatening situations. For instance, a healthcare provider processing a patient's medical information in an emergency situation to ensure the individual receives appropriate medical care.

6.5 PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR IN THE EXERCISE OF OFFICIAL AUTHORITY VESTED IN THE CONTROLLER.

This basis is applicable when personal data processing is required for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. Such as a government agency processing personal data for the administration of public benefits or for law enforcement purposes.

6.6 THE PERFORMANCE OF ANY TASK CARRIED OUT BY A PUBLIC AUTHORITY.

When a task is carried out by a public authority and involves the processing of personal data, this lawful basis is

applicable.

6.7 PUBLIC INTEREST OR ANY OTHER FUNCTIONS OF A PUBLIC NATURE.

This applies when personal data processing is necessary for the public interest and relates to specific functions of a public nature.

6.8 LEGITIMATE INTERESTS.

This basis allows for processing personal data based on the legitimate interests pursued by the data controller, processor, or a third party to whom the data is disclosed, unless such processing would result in unwarranted harm or prejudice to the rights and freedoms of the data subject.

6.9 PURPOSES OF HISTORICAL, STATISTICAL, JOURNALISTIC, LITERATURE AND ART OR SCIENTIFIC RESEARCH.

This basis is relevant for the processing of personal data for the purpose of historical, statistical, journalistic, literary, artistic, or scientific research. For example, a research institution processing personal data for conducting academic or scientific research while ensuring appropriate safeguards for the data subjects' rights and freedoms.

Each of these lawful bases serves as a foundation for the lawful and ethical processing of personal data, ensuring that individuals' privacy and data protection rights are respected and upheld.

7. PROCESSING PERSONAL DATA RELATING TO A CHILD

The law assumes that 'consent' can only be provided by persons above the majority age (i.e. 18 years and above). As such, the Act provides that personal data relating to a child shall only be processed where:

a. consent is given by the child's parent or guardian; and
b. the processing is in such a manner that protects and advances the rights and best interests of the child.

Christine Wairimu Muturi vs Roma School Uthiru (ODPC Complaint No. 0841 Of 2023)

The Complainant alleged that the Respondent sought to process images of minors on their social media platforms, particularly TikTok without the express consent of their parents or guardians. The Complainant requested from the Respondent to be given/shown measures that they would take to ensure that the processing of the minors' personal data would be done in accordance with the Act, and the Respondent failed to provide such measures.

The Respondent rebutted the Complainants claim and stated that they did not have a pupil neither was the Complainant a parent in their school. They also averred that they did not have any minor's data on Tik Tok or any of their social media platforms.

The ODPC upon investigations found that the Respondent did have a Tik Tok page that posts images and videos of minors in the school. Furthermore, their Facebook page operated as a means of advertising the school by use of images and videos of minors. The ODPC found that the Respondent had violated the rights and best interests of the minors in their school by not obtaining express consent from the minor's parents or guardians before posting their images and videos on social media. The Respondent were issued with an enforcement notice from the ODPC.

Abdinur Kassim & Luqman Hussein Kassim (minor suing through his father & next friend) vs Joyce Njoki Ngugu T/A Kora Spa. (ODPC COMPLAINT NO. 0660 OF 2023)

The complainant in this case alleged that the Respondent processed personal information of a minor for commercial purposes without the consent of the minor's guardian.

On or about 11th September, 2021 the Complainant visited the Respondent's place of business for obtaining barber services. While receiving the said services the Respondents took the Complainant's photographs which were published on the social media handles of the Respondent's under the caption *"Barbers are culturally significant @spa.kora @juan"*

The Respondent did not deny nor did they provide evidence of having sought consent to process the personal data of the 2nd Complainant. The ODPC found that the publication of the said pictures on the social media platforms of the Respondent was aimed at advertising the Respondent's business and thus the images were being used for commercial purposes.

The ODPC found the Respondent to have violated the rights and best interests of the child, having not obtained consent from the parent/guardian to process the personal data (publish the pictures) of the 2nd Complainant. An enforcement notice was then issued against the Respondent.

8. PROCESSING OF 'SENSITIVE' PERSONAL DATA

Being of a heightened nature, there are specific instances laid down in the Act where sensitive personal data may be processed, such as where:

a. the processing is carried out in the course of undertaking legitimate activities with appropriate safeguards by a non-profit body (such as a foundation or association) with a political, philosophical, religious or trade union aim. This is on condition that;

i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and

ii) the personal data is not disclosed outside that body without consent,

b. the processing relates to personal data which is manifestly made public by the data subject; or

c. processing is necessary for—

i) the establishment, exercise or defense of a legal claim;

ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or

iii) protecting the vital interests of the data subject or another person where the data subject is physicall or legally incapable of giving consent.

Likewise, personal data relating to the health of a data subject may only be processed:

a. by or under the responsibility of a health care provider; or

by a person subject to the obligation of professional secrecy under any law.

9. DATA RETENTION

While there's no specific timelines prescribed under the Act for the retention of personal data, a data controller or processor may only retain personal data as long as may be reasonably necessary ***to satisfy the purpose for which it is processed***. This means that retention period will be determined on a case-to-case basis depending to the needs of the controller or processor at the time.

However, personal data may be retained beyond the purpose it was intended for as:

a. required or authorized by law;
b. reasonably necessary for a lawful purpose;
c. authorized or consented by the data subject; or
d. for historical, statistical, journalistic literature and art or research purposes.

All persons and organizations should therefore be aware of this requirement and ensure that they do not hold personal data collected for any longer as they may require, so as to ensure their compliance with the Act.

Victory Owino vs Wananchi Group (K) Ltd (ODPC Complaint No. 1992 of 2023)

The Complainant alleged that despite requesting the Respondent to stop calling, sending her messages and emails and delete her details from the system, the Respondent persisted on calling her and sending her the said promotional messages.

The Respondent stated that their terms and conditions for provision of their services acted as a contract between themselves and their customers. The terms provided that the customer premise equipment remained their property until termination of services and that they would recover the same.

Therefore, having received an email from the Complainant requesting the deletion of her data, she was to return the equipment to any of the Respondent's office or inform them of a day they could recover the equipment from her premises. The Respondent received no further communication from the Complainant and were therefore unable to proceed with the request.

The ODPC found that the Respondent had violated the Complainant's right to erasure pursuant to Section 40(1)(b) of the Data Protection Act as she had withdrawn her consent and requested the Respondent to delete her personal details, but the Respondent refused citing their terms and conditions as lawful basis for retention.

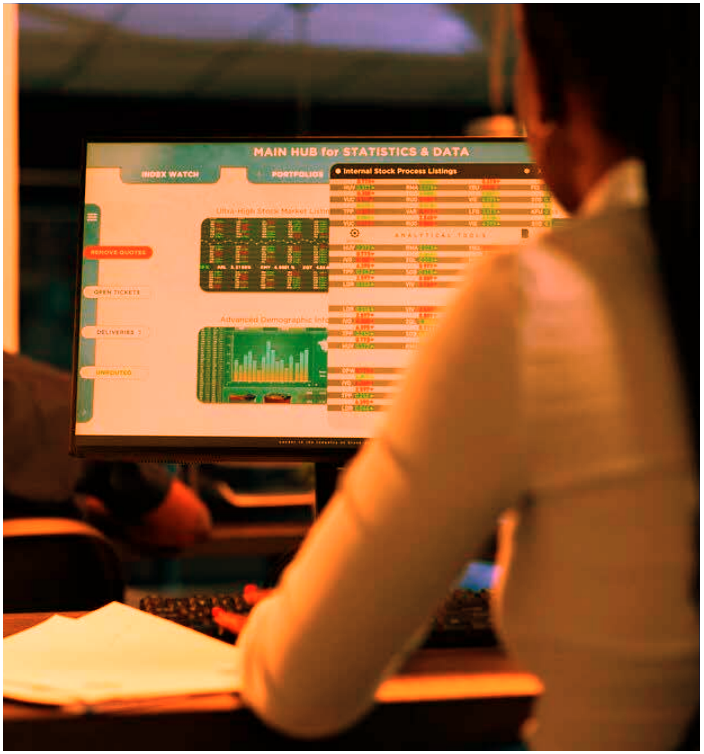
The ODPC also found the Respondent to be in contravention of Section 41 of the Data Protection Act, as they had not implemented technical and organizational measures that would enable them to remove and/or delete a customer's personal details once they cease being a customer.

10. OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS

A) DUTY TO REGISTER WITH THE OFFICE OF THE DATA PROTECTION COMMISSIONER

The Act requires that persons who handle personal data to register as Data Controllers and Data Processors under the Act. They are to provide accurate information when making such application. The application should contain the following;

a. A description of the personal data being processed;
b. A description of the purpose of processing the personal information;
c. Category of data subjects with whom the personal data relates;
d. Contact details of the data controller or processor, depending on the application;
e. Risks and Safeguards that ensure protection of the personal data;
f. Any measures of indemnification of the data subject by the controller or processor for unlawful processing.



It is an offence to provide false or misleading information during the application process and it attracts a general penalty of a fine not exceeding three million or imprisonment of a term not exceeding ten years or both.

After satisfactorily meeting all the requirements, the Data Commissioner will issue a certificate for either the data controller or data processor, with a validity period of two years and shall be renewable subject to expiry.

The terms and conditions of the certificate of registration may be varied or the certificate may be canceled as a whole if it is established that the information that was given at the time of registration was false or misleading or where the holder fails to comply with any requirement under the Data Protection Act.

B) DUTY TO DEVELOP A DATA PROTECTION POLICY

A data controller or processor has a duty to develop, publish and update a data protection policy that indicates how they handle personal data, the rights of a data subject, the purpose of collection and processing of such data, data transfer measures, retention periods, and complaint handling mechanisms.

C) DUTY TO DIRECTLY COLLECT PERSONAL DATA AND TO NOTIFY DATA SUBJECTS OF COLLECTION.

Data Controllers and Data Processors have a duty to collect personal data directly from the data subjects unless in the following instances;

a. Where the data is of public record;
b. Where the data subject has made such data public;
c. Where the data subject has given consent of such collection from another source;
d. Where the data subject lacks capacity and the guardian appointed has given consent to such collection from another source;
e. Where the data subject would not be prejudiced from collection from another source;
f. Where the collection of data from another source is necessary for the following;

i. Prevention, detection, investigation, prosecution and punishment of crime;
ii. Enforcement of the law for purposes of imposing a pecuniary penalty; and
iii. Protection of interests of the data subject or any other person.

It is also the duty of the Data Controller and the Data Processor to notify its data subjects prior to collecting their personal data of the following;

a. The fact they are collecting their personal data;
b. Their rights during collection and processing;
c. Whether any 3rd parties will have access to their data and if they do what measures they have put in place to safeguard the said data;
d. A description of the technical and organizational measures used by the organizations to prevent and/or mitigate any privacy risk and/or breach;
e. If their personal data is collected pursuant to any law, and whether the collection is voluntary or mandatory; and
f. Consequences of failing to provide all or any data that has been requested.

A data subject can be notified of the collection of their personal data through the following methods;

i. Written Notice, which can either be through a letter or an email.
ii. Privacy Policy on a website or app.
iii. In -App Notification, this can be by a pop-up notification explaining data collection from third parties.

An Enforcement Notice will be issued to Data Controllers or Data Processors for failure to comply with any provision of the Act. The Notice requires such person to take reasonable steps so as to remedy that which they have contravened. Such period will not be less than twenty-one days from the date of the Notice. Failure to comply with the notice, the person shall be liable for a fine not exceeding five million or

imprisonment for a term not exceeding two years or both.

Annsalome Wangari and Jaytie Sichiri vs Kerox Technology Company Limited (ODPC Complaint No. 0988 of 2023 & 0974 of 2023 as Consolidated with ODPC Complaint No.1006 of 2023)

The 1st Complainant in this case alleged that she was being called by AsapKash, a product of the Respondent, demanding her to repay a loan which she alleged she never took. The Respondent informed her that she was being held accountable for a third party's loan.

The 2nd Complainant in this case alleged that she was incessantly contacted by AsapKash, a product of the Respondent, telling her that she had been listed as a guarantor by a third party.

The Respondents confirmed that the 1st and 2nd Complainant were never their clients and that Asap Kash had contacted them on the basis that the company contract mandated that a borrower provides alternative numbers during registration and requisition of a loan.

The Respondents averred that they were truly sorry for the nature of messages and calls that both the 1st and 2nd Complainant had received and that they were to write an apology to them and a copy to be shared to the ODPC. However, no such copy was received by the ODPC.

The ODPC in its determination relied on Section 29 of the Act, which provides that a Data Controller or Data Processor has a duty to inform data subjects of their rights under Section 26 of the Act, before collecting their personal information. Furthermore, Section 28 provides that collection of personal data shall be directly from the data subject.

The ODPC found that the Respondent having not obtained prior consent from both Complainants and having not notified them of being enlisted as guarantors by third parties to be in breach of Section 28 and 29 of the Act.

Further, the ODPC found the Respondents to have violated the rights of the Complainants, guaranteed under Section 26, by failing to inform them of the collection and use of their personal data. The Respondents were then issued with an Enforcement Notice.

D) DUTY TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment is a type of assessment that is conducted when the processing of personal data is likely infringe on the rights and freedoms of a persons. Article 29 of the Working Party underscores the instance in which a DPIA should be conducted;

i. When the processing of the data will result in profiling and predicting a person's health, location, economic position, work performance and interests or preferences.
ii. When processing of that is aimed at making decisions on behalf of individuals
iii. When processing of that data will be used in observation or monitoring of persons, including data that is collected in public spaces.
iv. When processing sensitive data, this included, a person's race, health status, ethnicity, belief, conscience, genetic data, biometric data, property details, family details, sex or sexual orientation.
v. When processing data on a large scale.
vi. When combining or matching data sets. This could mean the combination of two datasets which were being used for processing data for different purposes.
vii. When processing data of vulnerable persons. Vulnerable persons include, children, persons of marginalized groups, employees, elderly.
viii. When creating or using new technology or organization solutions.
ix. When the processing would infringe on a person's rights and freedoms

The Data Protection Act places an obligation on the Data Controller or Processor to consult with the Data Commis-

sioner and also to conduct a DPIA before processing personal data that would infringe on a persons' rights and freedoms. Further, a DPIA report should be prepared and submitted to the Office of the Data Protection Commissioner sixty (60) days before the processing of such data.

A well-structured DPIA report requires incorporating the following essential features;

i. A description of the processing, including the purpose, and the legitimate interests.
ii. A description of the necessity, and its proportionality.
iii. Risks on the rights and freedoms of the individuals.
iv. Safeguards to address the risks which are identified.
v. Individuals who are to monitor and review the DPIA

ODPC Complaint No.1394 of 2023 (World coin Case)

Tools for Humanity GmbH (TFH) began collecting and processing personal data of Kenyan citizens for the purpose of developing a machine learning algorithm to establish a "Proof of Personhood" protocol. They submitted a DPIA report to the ODPC, which stipulated that the aim was to develop an algorithm that can differentiate a real human and fake irises as well as differentiate one real human iris from those of people who have signed up to the protocol.

The ODPC found TFH to have violated section 31 of the Act, by failing to show how they implemented technical and organizational measures to uphold the data protection principles and how they integrated necessary safeguards for processing.

E) DUTY TO RETAIN PERSONAL DATA FOR AS REASONABLY NECESSARY.

A Data Controller or Data Processor has a duty to retain personal data of a data subject only for as reasonably necessary unless the retention period is;

i. Specified in law;
ii. Necessary for a lawful purpose;

iii. Consented by a data subject; and
iv. For historic, statistical, journalistic literature and art or research purposes.

It is important to note that upon expiry of the retention period a data controller or processor should either delete, erase, anonymize or pseudonymize personal data that is not necessary to be retained.

F) DUTY TO ANONYMIZE OR PSEUDONYMIZE PERSONAL DATA

A Data Controller or Processor has the duty to anonymize or pseudonymize personal data at the request of the data subject. This increases a data subjects' privacy and reduces their risk of harm.

G) DUTY TO RECTIFY AND ERASE

At the request of the data subject, a data controller or processor and any third party contracted by a data controller or processor, has a duty to rectify and erase, without delay, personal data that is inaccurate or erase that which is irrelevant.

Jeff Nduko vs One Acre Fund (ODPC Complaint No.0574 of 2023)

The Respondent in this case admitted to have erroneously entered the Complainant's number into their database instead of their client's. The Complainant kept on receiving unwarranted messages and calls requiring him to pay back a loan which he took. As a mitigation measure, the Respondent upon notification updated its records.

Section 25(vi) provides that data controllers or processors should ensure that personal data should accurate and kept up-to-date and any inaccurate data should be erased or rectified without unreasonable delay. The ODPC in this case assisted the Respondent to take reasonable steps to erase or rectify the mistake they made, as the Complainant stopped receiving the unwarranted messages.

H) DUTY TO IMPLEMENT PRIVACY BY DESIGN AND DEFAULT

The term privacy by default means that privacy controls are embedded into products and services from their deployment until they are either disposed of or destroyed and that no action is required by individuals to maintain their privacy as it is already pre-installed.

The Data Protection Act,2019 provides that a data controller or processor has the duty to implement organizational safeguards before and during processing of personal data. Such safeguards identify the risks that are likely to face an individual and what measures the organization has or ought to put in place to prevent or mitigate such risk.

For organizations to prevent or mitigate risk, they should consider embedding privacy safeguards throughout the entire lifecycle of any product or service by taking into account the seven principles of Privacy by Design which are;

i. **Proactive not Reactive:** Organizations should anticipate any privacy issues that may arise in the course of processing personal data and prevent them from happening.
ii. **Privacy as the Default:** Organizations should ensure that privacy protections are automatically enabled for users and that users do not have go out of their way to find and activate them.
iii. **Privacy embedded into design:** Organizations should ensure that user privacy is promoted at every stage of product development and not considered as an afterthought. This will ensure a more secure, trustworthy and user-friendly experience.
iv. **Full functionality-positive sum, zero-sum:** Organizations should note that in accommodating privacy in their product development, there are not trading off its core functionality. The two can co-exist.
v. **End-to end security-full life cycle protection:** Security measures are essential to privacy. Having measures such as encryption, anonymization and pseudonymization are paramount in safeguarding

data through its entire lifecycle.

vi. **Visibility and transparency:** Organizations should be clear on why they are collecting data, how it is being used and with whom the data is being shared with. This establishes trust between the organization and their clientele.

vii. **Respect for user privacy:** Organizations should ensure that users have control over their data and are empowered to make informed choices on their data is being handled.

In the case of ***Pauline Muhanda T/A Mudeshi Muhanda and Co. Advocates vs Safaricom PLC (ODPC Complaint No. 1212 of 2023)***

The Complainant allegedly discovered that her and her law firm had been under private investigations, which led to her and her law firm's MPESA statements being accessed without her consent or knowledge. The Respondent confirmed that there had been a breach of personal data by its employee.

In guiding its determination, the ODPC was guided by section 41 (3) where it urged the Respondent, being a large data handler, to implement appropriate technical and organizational measures to ensure privacy by default is integrated into their systems.

The Respondent demonstrated that it had put in place policies and procedures to ensure the protection of personal data, therefore the ODPC found the complaint made against the Respondent to have been resolved.

I) DUTY OF NOTIFICATION OF DATA BREACH

A personal data breach is a breach of security that leads to unlawful access of personal information by an unauthorized person. This can occur through among others, theft, fraud, hacking, phishing, malware, A data controller is to notify the ODPC and the data subject of the same. In particular, that data controller shall:

a. Within seventy-two (72) hours of becoming aware of such breach, notify the ODPC.

b. As soon as reasonably possible, inform the data subjects in writing of such breach, unless their identity cannot be established.

Where a data processor becomes aware of such breach, the data processor shall notify the data controller within forty-eight (48) hours, without delay.

Where the notification to the ODPC is not made within the above timelines, such notification shall be accompanied by reasons for the delay above the specified duration.

The data controller has the right to delay or restrict communication as may be necessary and proportionate only for the purposes of prevention, detection or investigation of an offence by the concerned relevant body.

The Data Protection (General) Regulations, 2021 provide for the categories of notifiable data breaches under the Second schedule to include but not limited to;

i. The amount of wages, salary, fee, commission, bonus, gratuity, allowance or other remuneration paid or payable to the data subject by any person, whether under a contract of service or a contract for services;
ii. Income from the sale of goods or property;
iii. Networth of a data subject;
iv. Deposit or withdrawal of monies by a data subject;
v. Investment in any capital market products;
vi. Any other as provided under the Regulations.

When submitting a data breach notification report to the ODPC, the following should be included;

i. A description of the data breach;
ii. Measures that have been taken by either the data controller or processor in addressing the breach;
iii. Recommendations to the data subject to mitigate the effects of the security compromise;
iv. Identity of the unauthorized person who accessed the personal data; and
v. Contact details of the organizations data protection

officer

J) NON-TRANSFERABILITY OUTSIDE KENYA

Generally, the Act restricts the transfer of personal data outside the country. However, it provides for certain conditions to be met if any such transfer is to happen, such as ensuring that:

a. Adequate data protection safeguards are provided;

Where transfer of personal data is on the basis of appropriate safeguards, the transfer should be documented and the document should be provided to the Commissioner on request.

The document should include the following;

i. Date and time of the transfer;
ii. Name of the recipient;
iii. Reason for the transfer; and
iv. Description of the data being transferred.

b. Appropriate safeguards with respect to the security and protection of personal data are put in place, including confirming that the countries to transfer data to have commensurate data protection laws in place;

The list of countries/territories may be published on the website of the ODPC by the Commissioner if the Commissioner deems them to have adequate safeguards.

c. The transfer is of necessity;

When the transfer is on the basis of necessity, an organization should ensure that the transfer is strictly for the following reasons and that the rights and freedoms of individuals would not be violated;

i. The performance of a contract
ii. The conclusion of a contract
iii. For public interest;
iv. For a legal claim;
v. For the vital interests of the data subject or other persons; or
vi. For any legitimate interest.

d. The data subject has consented.
Such a transfer would only happen where the data subject has explicitly consented to it and has been informed of any risk that may arise from such a transfer.

K) EXEMPTIONS

The Act is applicable to all person (both natural and legal persons) equally. However, there are very specific instances where processing of personal data is exempt from the obligations under the Act, as follows:

a. where the processing is undertaken purely in the course of a personal or household activity;
b. if it is necessary for national security or public interest; or
c. disclosure is required by or under any written law or by an order of the court.

L) GENERAL OFFENCES

Offences committed in the following ways attract liability upon conviction of a fine not exceeding KES 3 million or to an imprisonment term not exceeding ten (10) years, or both;

a. A data controller unlawfully disclosing personal data in contravention with its purpose;
b. A data processor unlawfully disclosing personal data without prior authorization by the data controller;
c. obtains access to personal data, or obtains any information constituting such data, without prior authority of the data controller or processor by whom the data is kept;
d. discloses personal data to third party, commit an offence; or
e. Sells personal data that has been unlawfully disclosed by a data controller

In addition, a court may further:

a. order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence; or
b. order or prohibit the doing of any act to stop a continuing contravention.

The Act and subsequent Regulations also provide for other specific offences relating to data protection, with specific offences attached to them.

11. ENFORCEMENT AND PENALTIES

The Act provides for the following for contravention of any its provisions;

i. Enforcement Notice.
ii. Penalty Notice for failure to comply with the enforcement notice of a fine not exceeding five million shillings or imprisonment for a term not exceeding two years or both.
iii. General Penalty where there is no specific penalty provided of a fine of three million shillings or an imprisonment term not exceeding ten years or both.
iv. Specific penalty of a fine not exceeding five million shillings or imprisonment for a term not exceeding two years or both.
v. Compensation to a person who suffers damage by reason of contravention of a requirement by the Act. The damage suffered includes financial loss and damage that does not involve financial loss e.g distress.
vi. Forfeiture of equipment or articles connected with the carrying out the offence.

12. REGULATIONS

To assist in the enforcement of the Act itself, the subsequent regulations where published to provide clarity in the application of the Act. They include: -

a. *the Data Protection (General) Regulations, 2021* – these set out to provide further detail on the implementation of the Act. It provides clarity on the procedures involved.
b. *the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021* – these provide detail on the mechanisms of bringing forth a compliant to the ODPC. It provides for the procedures

for hearing and determination of complaints, as well as detailing the enforcement procedure.

c. *the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021* – these regulations provide for the requirements and process of registration of data controllers and data processors. It provides further details on the requirements for registration or persons are data controllers and data processors.

13. GUIDELINES

The Office of the Data Protection Commissioner in 2023 released guidelines for the Education, Hospital, Communications and Digital Credit Providers sectors. These guidelines have specific requirements on what each sector must consider whenever they are processing personal data.

14. CONCLUSION

Data protection has become a critical element in our day-to-day activities, thereby requiring due regard to our procedures and systems that we interact with. It is almost impossible to separate aspects data as discussed herein with our business activities.

As Barizi Data Privacy Services, we are happy to support the needs of your business through our data protection compliance services. Please do not hesitate to contact us if you have any queries.

CONTRIBUTORS

WINNIE WAMBUI NGIGE
Data Protection Officer

+254 714 974 056
wngige@bdps.co.ke

JOYCE MWAURA
Data Protection Assistant

+254 797 209 963
mwaura@bdps.co.ke

BARIZI
DATA
PRIVACY
SERVICES

I&M Bank House, 5th Floor,
2nd Ngong Ave

info@bdps.co.ke

+254 112 77 42 27

www.bdps.co.ke