OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes on Biometric Data

2025

TABLE OF CONTENTS

FOREWORD

The right to privacy is a constitutional guarantee under Article 31 of the Constitution of Kenya, 2010. Within this framework, the Data Protection Act, 2019 establishes the Office of the Data Protection Commissioner (Office) as the statutory regulator responsible for ensuring that personal data is processed lawfully, fairly, and transparently. Among the categories of personal data, biometric data is particularly sensitive due to its inherent connection to an individual's identity and the increased risks associated with its collection, storage, and use.

As Kenya accelerates its transition into a digital economy under the Bottom-Up Economic Transformation Agenda and the Digital Superhighway, the use of biometric technologies has become increasingly prevalent across various sectors, including national registration, elections, health, education, financial services, and workplace management. While biometrics offer undeniable benefits in authentication, efficiency, and inclusion, their misuse or unregulated processing can result in irrevocable harm to individuals' rights and freedoms, including discrimination, surveillance, profiling, and exposure to security breaches.

This Guidance Note has been developed to provide clarity on the legal and compliance obligations of data controllers and data processors—both in the public and private sectors—when processing biometric data. It interprets the requirements of the Data Protection Act 2019, subsidiary regulations, and international best practice, and emphasises the need for safeguards such as data minimisation, privacy by design and default, informed consent, data localisation, Data Protection Impact Assessments, and timely breach notification.

The Office underscores that biometric data processing must be approached with caution, necessity, and proportionality. Our hope as an office is that this Guidance Note will provide guidance on the compliance requirements of the law, enhance public trust, strengthen institutional accountability, and safeguard the dignity of individuals whose biometric attributes are processed.

The ODPC remains committed to providing regulatory guidance, engaging stakeholders, and enforcing regulations to ensure that Kenya's adoption of biometric technologies advances innovation while upholding fundamental rights. I hope that this Guidance Note will serve as a critical reference for entities entrusted with biometric data, guiding them to act responsibly, lawfully, and transparently in all their processing activities.

Immaculate Kassait**, MBS**
Data Commissioner

DEFINITIONS

"Act" means the Data Protection Act, No. 24 of 2019;

"Anonymization" means the permanent and irreversible removal of personal identifiers from personal data so that the data subject is no longer identifiable.

"Biometric" means unique identifiers or attributes such as fingerprints, facial geometry, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA.

"Biometric Data" means personal data resulting from specific technical processing based on physical, physiological or behavioral characterization including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

"Data" means information which –

a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
b) is recorded with the intention that it should be processed by means of such equipment.
c) is recorded as part of a relevant filing system.
d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or
e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

"Data Commissioner" means the person appointed under section 6 of the Act.

"Data Controller" means 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 Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.

"Data Subject" means an identified or identifiable natural person who is the subject of personal data.

"Encryption" means the process of converting the content of any readable data using technical means into coded form.

"Entity" or **"Entities"** means a natural person (individual) or legal person, public authority, agency or other body that processes (handles) personal data.

"Office" means the Office of the Data Protection Commissioner as established in section 5 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Privacy framework" is a set of guidelines, principles, and standards that organisations can use to protect the personal information of individuals.

"Processing" means any operation or sets of operations which is performed on Personal Data or on sets of personal data, whether by automated means, such as:

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

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements.

"Pseudonymisation " means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"Regulations" means the Data Protection (General) Regulations, 2021; the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021; and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

"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.

THE OFFICE

The Office of the Data Protection Commissioner is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It has the responsibility of enforcing data protection laws and policies to safeguard the privacy, dignity, and fundamental rights of individuals. The Office is mandated to oversee the implementation and enforcement of the Data Protection Act, 2019, which regulates the processing of personal data by both private and public organisations in Kenya.

The Office plays a vital role in ensuring that individuals control their personal data and that organisations respect their privacy rights. The Office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches, and imposing sanctions on entities that violate data protection laws. In addition, the Office is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the office of the data protection commissioner is a critical institution in maintaining trust and confidence in our data-driven society.

The Office is positioned to facilitate both the government and private sector entities in achieving the government's strategic goals under the "Bottom-Up Economic Transformation Agenda" and its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, with its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation. Kenya remains at the cutting edge of digital transformation while maintaining stringent data protection standards. The Office serves as a key stakeholder and regulator in guiding the nation's digital superhighway journey by ensuring that as we advance technologically, the rights and privacy of individuals remain safeguarded.

INTRODUCTION

This guidance note is intended to assist data controllers and data processors who process biometric data in complying with the provisions of the Act and its subsidiary regulations. It should be reviewed prior to determining whether biometric data will be processed and, where such processing occurs, it should be regularly consulted to ensure ongoing compliance.

Biometric data includes the physical and/or physiological data which individuals are born with and the behavioural data developed by an individual after birth. Biometric data is, therefore, data directly related to an individual, enabling or confirming someone's unique identification. While it may not be reasonably practicable for a layperson to ascertain the identity of an individual by merely looking at the individual's fingerprint images or their numeric representations, when specific technologies are applied or the biometric data is linked with personal data in another database, a data subject can be identified. Further, due to the sensitivity, incorrectly processed data can have far-reaching privacy implications, especially in our highly digital world.

For the reasons above, biometric data is considered sensitive personal data under the Act and due to its highly sensitive nature, biometric data is subject to stringent data protection requirements under the law. Its use has a significant impact on the rights and freedoms of data subjects, particularly their right to privacy. When designing and implementing biometric systems, it is imperative to ensure that data subjects maintain control over the ongoing processing of their personal data; have access to their data; clearly understand how their data is being used; and are adequately informed about all aspects of the data processing.

While biometrics serve as a tool for managing identities rather than defining them, they offer significant advantages, such as improved accessibility, eligibility, and inclusion across society. They streamline processes, replace vulnerable paper-based systems, and reduce the risk of security breaches and human error.

However, like any technology, biometric systems come with privacy risks and concerns which significantly impact data subjects' rights. Ensuring responsible use of biometrics by implementing data protection by design and default can make biometrics an effective tool for enhancing proper data management.

This guidance note sets out recommended good practices in processing and using biometric data.

PRIVACY CONCERNS

Biometric data, classified as sensitive personal data under Section 2 of the Act, requires the implementation of stringent safeguards to ensure its lawful and ethical processing. Any processing of such data must adhere to the principles of data protection by design and by default, thereby minimizing unnecessary intrusion into individuals' privacy.

While biometric technologies can significantly enhance operational efficiency and security, they also present unique privacy risks. The extent to which biometric systems protect or infringe upon privacy depends largely on how these systems are designed, deployed, and managed.

As reliance on biometric technology increases, so too do concerns about privacy and potential misuse. It is therefore essential that privacy considerations are embedded at every stage of biometric system development and operation, ensuring that individual rights are respected and upheld. Here are some of the key privacy concerns in this sector:

1.1. Accuracy

Although the accuracy of biometric recognition technology has increased significantly in recent years, differences in performance exist for certain demographic groups. Biometric technology often has lower accuracy for certain demographic groups, including but not limited to children, the elderly, and persons with disabilities. These differences could result in more frequent misidentification for certain demographics, such as misidentifying a data subject.

1.2. Surveillance & tracking:

Data controllers and/or data processors may use biometric recognition technology to monitor data subjects. This surveillance can be done with or without data subjects' consent, and it can be difficult to know when it is happening. For instance, facial recognition technology may process or store facial images, posing varying levels of risk. Some of these concerns include, among other things, the technology's potential to identify individuals in public without their knowledge or consent and track their locations, movements, and companions. Misuse of surveillance, lack of transparency in data processing and usage, integration with other datasets, and risks of intrusive profiling exacerbate these concerns.

1.3. Data security:

This concern revolves around protecting sensitive biometric data throughout the data lifecycle process, from processing to storage and transmission. Risks include unauthorized access to encrypted data, potential privacy breaches during decryption, and impacts on individuals' privacy rights. To address these concerns, data controllers and/or processors should implement strong encryption protocols, secure key management practices, controlled decryption processes, and transparency in data usage and consent.

1.4. Biometric data breaches:

Data controllers and/or processors who handle biometric data face a heightened risk of data breaches due to the inherently sensitive nature of such data. This risk is further compounded by

the variable and often dynamic retention periods associated with the storage of biometric data, which can increase the complexity of ensuring ongoing security and compliance.

4.5 How Biometric Recognition Systems Work

Biometric recognition systems process biometric data through capture, feature extraction, template creation, and comparison. A biometric sample (e.g., a facial image) is captured, and algorithms extract features (e.g., numerical representations of facial landmarks) to create a template. During comparison, a new sample (probe) is matched against stored templates to verify or identify an individual, using thresholds to determine similarity. These systems rely on statistical probabilities, introducing risks of false acceptance or rejection.

1.5. Misuse of personal data:

This concerns the processing, use, and sale of personal information by data brokers and companies. For instance, facial image datasets could be sold or shared by various parties, which can lead to unwanted disclosure of personal data and violations of rights of data subjects.

SCOPE AND PURPOSE OF THE GUIDANCE NOTE

In exercise of the powers of the Office pursuant to the Act and the Regulations, this Guidance Note provides detailed considerations that must be taken into account when processing biometric data.

This guidance note considers:

i. The Data Protection Act, 2019;
ii. The Data Protection General Regulations, 2021;
iii. The Data Protection and Privacy Policy, 2018;
iv. Other applicable laws and regulations and
v. International Best Practice.

The Guidance Note applies to the biometric processing of personal data in either the public or private sectors and should be regarded as a minimum standard which can be supplemented by additional measures for the protection of privacy and individual rights, which may impact or be impacted by the processing of personal data.

LEGISLATIVE FRAMEWORK

Processing personal data in Kenya is governed by the Constitution and other legislation, which include but are not limited to the following:

The Constitution of Kenya, 2010

Article 31 (c) and (d) guarantee the right to privacy with regard to individuals information or information relating to their family or private affairs unnecessarily being required, revealed or infringed.

Article 35 states that every citizen has a right to access information held by the state and any other person that is necessary for the exercise or protection of a right or fundamental freedom.

The Data Protection Act, 2019

It identifies certain types of personal information as more sensitive and offers them additional protection, establishes the Office of the Data Protection Commissioner and further provides for the protection of personal data and privacy of individuals in Kenya, including the data processed across jurisdictional borders.

The Computer Misuse and Cybercrime Act, No. 5 of 2018

The Computer Misuse and Cybercrimes Act safeguards the confidentiality, integrity, and availability of computer systems, programs, and data. It establishes legal protections against cyber threats by criminalizing malicious activities targeting individuals using computer systems, as well as attacks directed at computer systems themselves.

The Elections (Technology) regulations of 2017

The Elections (Technology) regulations of 2017 define biometrics as unique identifiers or attributes, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, and DNA.

The Children Act of 2022

This act reinforces in **Section 8(1)** that in all actions concerning children, the best interests of the child shall be a primary consideration.
Additionally, **Section 27** enshrines the children's right to privacy by stating that a child shall not be subjected to arbitrary or unlawful interference with their privacy, family or private affairs, or correspondence, or to attacks upon his or her honour or reputation.

APPLICATION OF DATA PROTECTION PRINCIPLES DURING BIOMETRIC PROCESSING

The principles and/or elements of data protection as listed under Section 25 of the Act and Regulations 28 to 34 of the Data Protection (General) Regulations 2021 include the following:

1.6. Lawfulness

The principle of lawfulness requires that data controllers and/or data processors must establish a specific legal basis for processing biometric data, as provided under Section 30 of the Act. In addition, because biometric data is classified as sensitive personal data, its processing must be subject to additional safeguards, including those outlined under Part V of the Act.

Example

The National Registration Bureau uses finger impressions when issuing National Identity cards. Section 5(1) of the Registration of Persons Act further requires the principal registrar to maintain a register of all persons in Kenya, which includes their particulars, such as finger and thumb impressions; however, if individuals are missing fingers or thumbs, palm or toe impressions, or both, may be used instead. The National Registration in processing biometric data relies on the fulfilment of their legal obligation under the Registration of Persons Act.

1.7. Fairness and Transparency

This principle emphasizes the importance of transparency and the protection of data subjects' privacy. Data controllers and/or processors are required to provide clear, accessible, and comprehensive information about the processing of personal data; grant data subjects access to their data and allow them to exercise control over how it is used; and ensure that data processing is carried out in a manner that is fair, non-discriminatory, and free from bias.

Example

A company is using facial recognition technology to track employee attendance. Before deploying the system, the company informs employees about the use of biometric data, how it will be processed, stored, and used solely for attendance monitoring purposes. Employees can choose to opt-in or opt-out of the system. The consequences of opting out are clearly outlined, and alternative mechanisms are available. If employees opt in, they have sufficient control over their data and provide informed consent. Additionally, the

company regularly reviews the technology to ensure it does not exhibit bias or discriminate against any individuals based on factors like race or gender.

1.8. Purpose limitation

The processing of biometric data must be limited to the explicit, specified, and legitimate purposes for which the data was processed. For example, if fingerprint data was processed for security and access control, it should not be used for performance evaluations.

Example:

KaziSafi & Sons employs Mali. His employer requests for all employees, including Mali, to enroll their fingerprint biometrics for the purpose of office access. Before collecting the fingerprints, the Human Resource department at Kazisafi & Sons informs Mali of the purpose for which the data is being collected. In this case, the data should not be used for any other purpose, like monitoring employee timekeeping and office activity.

1.9. Data minimization

This principle dictates that only the personal data necessary to achieve a clearly defined and lawful purpose should be collected and processed. In the context of biometric data, data minimization requires a demonstration of both necessity and proportionality in the processing activities.

The privacy risks associated with biometric processing increase with the volume and granularity of the data collected for example, the number of biometric features extracted from a sample or image. Therefore, data controllers and/or processors must carefully assess the minimum amount of biometric data required to fulfill the intended purpose, and avoid excessive or unnecessary data collection.

Example

A financial institution uses fingerprint biometrics to control access to a secure server room containing sensitive customer data. To minimise data, only two fingerprints are collected instead of all ten, and only authorized IT staff are enrolled. The system stores non-reversible fingerprint templates rather than full images, with the data encrypted and access strictly limited.

1.10. Accuracy

Data controllers and processors are required to take all reasonably practicable steps to ensure that personal data held is accurate. As biometric data processed can be used to take adverse action against a data subject, accuracy of the data is of particular importance to the data subject. For instance, where an employee supplies biometric data on each working day to prove work attendance, any inaccuracy of the data processed may result in salary deduction or even termination of employment. To ensure the accuracy of biometric recognition systems, data controllers and/or processors must ascertain and be satisfied that the false positive rate and false negative rate of the biometric recognition systems are within reasonable limits, having regard to the size of the population monitored by the systems. Data controllers and/or data processors should query the irregularity within their systems and procedures and provide an avenue for affected individuals to provide an explanation, where appropriate.

Example:

An insurance company, which deals with the issuance of medical insurance cover must ensure that they have accurate records of their clients' biometric data, such as fingerprints and facial recognition. This is essential to ensure that only their clients benefit from the insurance cover. By validating biometric data during onboarding and registration of their clients, Anguka Nayo Insurance Company can prevent unauthorized use of the insurance cover and ensure accurate client identification. Inaccurate biometric records could lead to errors in patient identification, misuse of the insurance cover, lack of service provision to the insured, and losses to Anguka Nayo Insurance.

1.11. Storage Limitation

This principle emphasizes retaining biometric data only for the duration necessary to fulfill its intended purpose. Clear policies and procedures for data retention and deletion must be established, defining specific purposes and retention periods. Prompt deletion or anonymization should occur once the purpose is fulfilled to mitigate privacy risks from unjustified retention periods and ensure compliance with the Act and Regulations. Retaining personal data for a period beyond what is necessary would create a burden on the data user in safeguarding data security and assuming the unnecessary risk of a data breach.

Example:

Employees at Watuwetu Ltd use fingerprint scans to access secure areas. Watuwetu Ltd processes and stores only fingerprint templates, not the full images, ensuring minimal data storage. These templates are encrypted and stored on a secure server with access controls. Watuwetu Ltd also implements a data retention policy with a clear retention period, purpose and reason for retention. Furthermore, procedures to delete biometric data immediately upon an employee's departure ensure that data is retained only as long as necessary for security purposes. By adhering to these practices, Watuwetu Ltd effectively minimises the

storage of biometric data, aligning with data protection principles and safeguarding employee privacy.

Guidance:

For the purposes of research or statistical analysis, data users who wish to retain personal data for longer than is necessary for the original purpose of collection may apply delinking mechanisms to achieve permanent anonymisation. Once data is effectively anonymized—such that individuals are no longer identifiable—it is no longer considered personal data and, therefore, falls outside the scope of the Act.

However, data users must carefully assess the feasibility and reliability of anonymizing biometric data, given its uniquely identifiable and often immutable nature. Particular caution should be exercised when processing data types such as DNA samples or genetic sequences, which—even when stripped of names or direct identifiers—may still reveal sensitive characteristics such as race, disability status, or familial relationships, potentially allowing reidentification under certain conditions.

1.12. Integrity and confidentiality

This principle mandates organisations to secure and maintain the integrity of biometric data, safeguarding it from unauthorized access, alteration, or disclosure. This involves implementing strong security measures and ensuring data is accurately recorded and stored to minimise errors and tampering.

Example:

ManiMoney, a financial technology company, launches a new product that allows their customers to approve high-value withdrawals and transfers through the alternative use of fingerprint recognition instead of in-person approval and wet signature. The institution implements strict security protocols to safeguard biometric data, such as encryption during transmission and storage, access controls, and regular security audits. Additionally, they ensure the accuracy and integrity of the data by regularly updating their biometric systems and monitoring any unauthorized access or tampering attempts.

LAWFUL BASIS FOR PROCESSING OF BIOMETRIC PERSONAL DATA

Section 30 of the Act provides eight lawful bases for processing personal data. However, given that biometric data constitutes sensitive personal data, its processing is subject to the additional and more stringent conditions outlined in Part V of the Act. Therefore, in addition to the general lawful bases under Section 30, data controllers must also identify and meet one of the specific conditions for processing sensitive personal data under Section 45 of the Act. In general, the acceptable lawful bases for processing biometric data are as follows:

8.1. Consent

Part V of the Act greatly restricts the instances where sensitive personal data, such as biometric data, may be processed. Consent is one of the lawful bases provided for in section 30 of the Act. Where a data handler relies on consent as a lawful basis to process biometric data, the data subject ought to have given free, unequivocal, and informed consent to the processing of their data. Consent of a data subject may be obtained through opt-in features that indicate the nature of data processing, with clear details of the biometric data collected from the data subject, with options to opt-out at will. Additionally, where biometric data is essential to the operation of a particular feature or service, the data subject must be provided with an option to withdraw such consent. The data subject must also be provided with alternative means of accessing the feature/service without having to provide consent again in order to use the service.

Consent for processing biometric data must be verifiable, and mechanisms must be in place for the data subject to access, modify, or withdraw consent at any time. This consent can be withdrawn at any time, and the data subject retains the right to object to their data being processed as well as the right to be forgotten.

Section 2 of the Act defines the meaning of consent as being:

a) **Specific**: The data subject must be informed about the specific purpose for which their data will be processed.
b) **Informed**: The data subject must be provided with sufficient information to make an informed decision about whether or not to give consent. This includes information about the types of personal data that will be processed, how it will be used, who will have access to it, and how long it will be retained.
c) **Freely given**: The data subject must have a genuine choice to grant or withhold consent. Consent cannot be coerced or forced, and there must be no negative consequences for the data subject if they refuse to give consent.

For example, when enrolling fingerprints as the chosen form of biometric data, explicit consent must be obtained through a clear and affirmative action. This consent must be specific to each individual processing activity and must not be bundled with general terms and conditions. The data controller or processor is required to provide the data subject with clear, concise, and accessible information outlining the purpose and legal basis for processing the biometric data; the nature and scope of the processing; the retention period for the data; and the rights of the data subject, including the right to withdraw consent at

any time.

Generally, where processing is based on consent, a data controller and/or processor are required to meet the conditions of consent as set out in Section 32 of the Act and Regulation 4 of the General Regulations. A data controller and/or data processor is required to inform the data subject of the following before seeking consent:

- the identity of the data controller or data processor;
- the purpose of each of the processing operations for which consent is sought;
- the type of the biometric data that is collected and used;
- information about the use of the biometric data for automated decision-making, where relevant;
- whether the personal data processed shall be shared with third parties;
- the right to withdraw consent; and
- the implications of providing, withholding, or withdrawing consent.

Consent of a data subject may be obtained through opt-in features that indicate the nature of data processing, with clear details of the nature of biometric processing, with options to opt-out at will. Additionally, where biometric data is essential to the operation of a particular feature or service, the data subject must be provided with an option to withdraw such consent. The data subject must also be provided with alternative means of accessing the feature/service, without having to provide consent again in order to use the service.

For instance, where biometric features are embedded in optional platform functionalities (such as facial recognition in photos, voice assistants, or device unlocking features), consent may be obtained through feature-specific opt-ins that clearly communicate the nature and purpose of the biometric processing. In such cases, activation of a specific feature may constitute valid consent, provided the data subject is presented with clear, concise, and accessible information at the time of activation, and is able to opt out or deactivate the feature at any time.

In addition, where biometric processing is integral to the functioning of a selected device setting or user feature, the bundling of consent with feature activation shall be permitted, provided that transparency is ensured and users retain the ability to withdraw consent without loss of access to unrelated services. In addition, the provision of this consent must not be marred by any illusion of choice, nor should there be adverse consequences for individuals who choose not to provide their consent.

Example 1:

Damu Researchers wish to carry out research on the relationship between malaria infections and the type of blood group. Before taking blood samples, they must seek consent from participants. For the consent to be valid, Damu researchers will inform the data subject the following: -

i. the identity of the data controller and/or data processor;
ii. the purpose of each of the processing operations for which
iii. consent is sought;
iv. the type of personal data that is collected and used, which in this case will be blood samples;
v. possibility of transfer of the personal data;
vi. the possible risks associated with the data transfer;
vii. whether the personal data processed shall be shared with third parties;
viii. the right to withdraw consent; and
ix. the implications of providing, withholding or withdrawing consent.

Parental Consent:

Parental or guardian consent must accompany any processing of children's biometric data in accordance with Section 33 of the Act and the Children Act, 2022

The Children Act of 2022 defines a child as anyone under the age of 18 years. Consequently, the age of consent is 18 years. Processing of data relating to a child is prohibited under the Act unless **informed consent** is given by the child's parent or legal guardian.

Section 33 of the Act further stipulates that the processing should be in a manner that protects and advances the rights and best interests of the child and a data controller or data processor shall incorporate appropriate mechanisms for age verification and consent to process personal data of a child.

Example

A school implements fingerprint scanning for cafeteria purchases. Before enrolling a student in the program, the school obtains explicit individual consent from the parent(s) or guardian(s). They provide clear information about how the biometric data will be processed, stored, and used solely for cafeteria transactions. Additionally, they offer alternative payment methods for students whose parents do not consent to their children's participation, ensuring that consent is voluntary and informed.

8.2. Performance of a Contract

When biometric data processing is necessary to fulfill the terms of a contract between the entity processing the biometric data and the data subject, the entity processing the biometric data should not process more personal data than is necessary to fulfill its contractual obligations. Further, it must not use biometric data for any other purposes that are not related to the performance of the contract. The data subject must also be notified of the processing and the purpose for the same.

Example

Witu Ltd pays its employees based on the number of hours worked. To make it easy to track the number of hours for each employee, Witu has a fingerprint system where employees use to clock into work and leave. When recruiting employees, Witu Ltd makes this clear to the employees and also includes it in the employment contract.

8.3. Compliance with Legal Obligations

Data controllers and processors are permitted to process biometric data if it's necessary to comply with a legal requirement imposed by law.

Example 1

For purposes of executing its mandate under the Constitution of Kenya, that is, conducting elections in Kenya as per Articles 83 and 86, an electoral body is mandated by law to process biometric data, including fingerprints and facial images, from eligible voters to ensure accurate voter registration and prevent fraud during elections. This legal obligation ensures the integrity and fairness of the electoral process in Kenya.

Example 2

For purposes of executing its mandate, the National Registration Bureau is mandated under section 5(1) of the Registration of Persons Act to process biometric data, including fingerprints from eligible persons resident in Kenya for purposes of issuing national identification cards. This legal obligation ensures national security and prevents identity fraud in Kenya.

8.4. Legitimate Interest Pursued by Data Controller or Processor

A data controller's and/or processor's reliance on legitimate interest in processing biometric data should not outweigh the rights and freedoms of data subjects at large. The data controller and/or processor should conduct a Legitimate Interest Assessment to ensure that the data controller and/or processor interests do not outweigh or prejudice the rights of a data subject

According to Section 45 of the Act, which governs the circumstances under which sensitive personal data may be processed, legitimate interest cannot serve as a standalone lawful basis for the processing of biometric data, due to its inherently sensitive nature. However, legitimate interest may be considered as a supporting or secondary basis, provided that a primary lawful basis such as explicit consent or a clear legal obligation is already established.

In such cases, the data controller must conduct a legitimate interest assessment (LIA) to demonstrate that the controller's interests are not overridden by the data subject's fundamental rights and freedoms. Additionally, any reliance on this basis must be necessary and strictly guided by the principles of purpose limitation, fairness, and transparency. Data subjects must be clearly informed of the intended processing, including the purpose, the lawful basis relied upon, and their rights under the Act.

Example 1:

AZ Company Ltd, which was making a lot of losses due to workers absconding duties, decided to use fingerprint recognition for employee timekeeping purposes. The company's legitimate interest lies in accurately tracking employees' working hours to ensure fair compensation and efficient workforce management. However, it's crucial for the company to balance its interest with employees' privacy rights and implement appropriate safeguards to protect their biometric data.

Example 2:

Vitu Ltd, a forensic lab, might require biometric data like fingerprints or palm scans to grant access to its facilities as part of its operations terms and conditions. Because of the nature of data held at the forensic lab, Vitu Ltd requires a secure and convenient access control system where biometric data might be the most appropriate solution. The data controller must ensure transparency by informing the data subject (employees) and any other person with access about the processing and purpose and necessity of this biometric data as part of the contractual agreement. This includes explaining how the data will be used, who will have access to it, and how long it will be retained. These data subjects must voluntarily agree to the processing of their biometric data as a condition of entering into the contract. This means they should have the option to opt-out or choose an alternative method if they do not wish to provide biometric data and further without suffering adverse effects because of their choice not to share their biometric data. Vitu Ltd, as the data controller, is further responsible for implementing appropriate security measures to protect the biometric data from unauthorized access, disclosure, or misuse. This includes encryption, access controls, regular security audits, and employee training on data protection best practices.

RIGHTS OF A DATA SUBJECTS

These are rights of a data subject exercisable with respect to the processing of their data. The Act provides data subjects with certain enforceable rights regarding their personal data with the aim of empowering data subjects to exercise their rights in a world increasingly dominated by technology and other players that process vast amounts of data. It is the duty of the data controller and/or processor to provide data subjects with modalities and avenues where the data subject can exercise their rights.

9.1. Right to be Informed

This right allows a data subject to know what personal data is being processed about them, why, and who is processing the data; how long it will be kept, how they can exercise their rights, guarantee on the integrity and confidentiality of their data, whether the processing is voluntary or mandatory and the consequences of failure to provide all or part of their biometric data and with whom the data controllers and/or processors may share the data with. Entities must ensure that this information is accessible to data subjects, including vulnerable persons. This may include providing information in alternative formats and the use of assistive technologies.

Example 1

Matu Ltd is implementing fingerprint access technology for the workplace and employee attendance. Before enrolling the employees to the biometric system, Matu Ltd informs the employees of the following to ensure the data subject right to be informed is upheld: -

i. their rights of data specified under the Act;
ii. the fact that biometric data which is fingerprints is being collected;
iii. that purpose for which their fingerprints are being collected is to ensure access to the workplace and track their attendance;
iv. that their biometric data will be accessed by the heads of ICT and Human resources only;
v. That their data shall be stored as long as they are employees of Matu Ltd;
vi. a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of their data;
vii. whether such collection is voluntary or mandatory; and
viii. the consequences, if any, where any employee fails to provide the requested data.

9.2. Right to access Personal Data

Data subjects have the right to access personal data in the custody of the data controller and/or processor, that is, whether or not personal data concerning them is being processed, the purpose of processing, categories of personal data, recipients of the personal data, the period for which the personal data will be stored and if the source of processing of the data is processed from a third party.

Due to the sensitive nature of biometric data, the data controller and/or processor has to develop a mechanism to verify the request, which may include the submission of

documents that support the request.

To exercise this right, data subjects must make a written request to the controller and/or processor, who shall respond by granting access to the biometrics in their custody. As biometric data is not identifiable merely by looking at it, the data controller and/or processor shall accompany the said biometrics with personal metadata. The request shall be complied with within 7 days and shall be free of charge.

Example 1:

Sarah works for a multinational corporation, GlobalTech, which uses biometric data such as fingerprint scans and facial recognition to secure its facilities. Concerned about the extent of biometric data processing, Sarah exercises her right as a data subject to access her biometric data held by GlobalTech. She submits a written request to the entity, asking for details on whether her biometric data is being processed, the purposes of such processing, the categories of biometric data processed, recipients of this data, the duration for which it is stored, and the source if the data was obtained from a third party. Within seven days, GlobalTech responds by providing Sarah with an electronic copy of her biometric data and relevant information, ensuring clarity and accessibility. This response empowers Sarah to understand the biometric data held by GlobalTech, enabling her to make informed decisions regarding her privacy and data security.

9.3. Right to Rectification of Personal Data

This means that data subjects can request corrections to untrue, inaccurate, outdated, incomplete or misleading information held about them. Due to the sensitive nature of biometric data, the data controller and/or processor has to develop a mechanism to verify the request and maybe be accompanied by documents that support the request. Once satisfied that the request is necessary, the data controller and/or processor are obligated to rectify the entry within 14 days and, where the request is declined to communicate the reasons for refusal in writing within 7 days.

Example 2:

John, a frequent traveler, uses a biometric authentication system provided by AeroSafe Airport Services for expedited security checks. Recently, John underwent facial reconstructive surgery, which altered his facial features. AeroSafe Airport Services allows John to rectify his biometric data to reflect his new appearance, ensuring that his information remains accurate and up to date.

John submits a request to update his facial recognition data, accompanied by medical documentation from his surgeon. AeroSafe Airport Services verifies the request and updates John's biometric data within the stipulated 14 days. Additionally, they inform John of the update and ensure that all third parties who previously had access to his outdated biometric data receive the corrected information. If the request had been declined, AeroSafe Airport Services would have communicated the reasons for refusal in writing within 7 days.

This process ensures the accuracy and completeness of John's biometric data, upholding his right to rectification and maintaining the integrity of the biometric authentication system.

9.4. Right not to be subject to automated decision- making

Automated decision-making occurs when an electronic system uses personal data, including biometric data, to make decisions without human intervention. Automated processing of biometric data may be used for various purposes such as access control, timekeeping, security verification, and predictive analytics. This right ensures that significant decisions involving sensitive biometric data are made with human intervention who can consider individual circumstances, biases, and context.

Data subjects have the right not to be subjected to an automated decision when it is based on automated processing that produces an adverse legal effect or significantly affects the individual. Data Controllers and/or processors must ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it where applicable.

To qualify as human intervention, data controllers and/or processors must ensure that they carefully analyze the decision and consider all the available input and output data, rather than just an output review. This should be carried out by someone who has the authority and competence to change the decision. This right does not specifically refer to profiling or when a decision does not have an adverse legal or similarly significant effect on a data subject.

Example 1:

Vitu Poa Insurance Company decided to use facial recognition to gauge the age of its clients and to set the amount of premiums to be paid by each client. Vitu Poa informed its client of its intention, the rights the clients had, and the possible consequences of relying on automated decision-making. Mtoto Mzuri, their client aged 25 years, was erroneously placed into a band of clients aged 32 years based on facial recognition using automated decision-making, and as a result, he filed a complaint with Vitu Poa Insurance Company. Vitu Poa Insurance Company designated a capable authority to evaluate the biometric data and make choices. To guarantee that decisions made in the future are reliable, the inaccuracies were fixed, and Mtoto Mzuri's data updated. Through this procedure, Mtoto Mzuri's rights were upheld, and equitable treatment was guaranteed by ensuring that important choices involving his biometric data were made with human scrutiny.

9.5. Right to Erasure

This right is also known as the right to be forgotten. It allows data subjects to request the deletion or removal of their personal data in custody of the data controller and/or processor. Further, this right only applies to data held at the time the request is received and does not apply to data that may be created in the future. The right is not absolute right, however when granted, the same should be complied with within 14 days of the request.

Data subjects have the right to have their personal data erased if the personal data is no longer necessary for the purpose within which it was originally processed, where consent was the lawful basis for processing of the personal data has been withdrawn, where the data subject objects to further processing of part or all of their personal data, where the processing becomes unlawful and where erasure is necessary to comply with a legal obligation.

If a valid erasure request is received and no exemption applies then the data controller and/or processor will have to take steps to ensure erasure from backup systems, live systems as well as third parties with whom the personal data has been shared. These steps will depend on the data controller's and/or processor's particular circumstances, their retention schedule (particularly in backups), and the technical mechanisms that are available to the data controller and/or processor.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defense of legal claims.

Example 1:

After quitting BioGuard Security Services, Alex, a former employee, exercised his right to be forgotten by requesting that his biometric data including his fingerprint and facial images be deleted. Alex's identification was confirmed, and his request was validated by BioGuard after confirming that no law required the retention of his biometric data, as such they had no lawful basis for continued retention of Alex's data. BioGuard ensured erasure and deletion of all of his biometric data from their live systems, backup systems, and third parties with whom his biometric data had been shared.

BioGuard notified Alex that his biometric data will no longer be kept, utilized or handled in accordance with this request in the future. By guaranteeing that Alex's personal data was completely deleted and not used for any other purposes, this procedure respected his right to be forgotten and complied with data protection laws**.**

Example 2:

Mary, a registered voter in Kenya, wishes to have her fingerprints and biometric data erased by the oversight electoral body. Mary is informed that the purpose of processing her biometric data was for the sole execution of a legal obligation and that the body is mandated by law to maintain a register of such biometrics, thus holding and retaining the data is a legal requirement. The electoral body communicates the refusal to Mary in writing within 7 days.

9.6. Right to Data Portability

Data subjects have the right to receive their biometric data in a structured, commonly used, and machine-readable format from the data controller and/or processor. This will allow them to transfer their biometric data easily to another controller if they wish to switch service providers or platforms. However, it's crucial to ensure that such transfers are done securely and with respect to privacy and security concerns associated with biometric data.

This right is provided for under Section 38 of the Act wherein a data subject may apply to port or copy their personal data from one data controller or data processor to another. However, the right to data portability shall not apply where;

i. Data that is not processed based on consent of the individual or a contract.
ii. Data processed based on other legal bases such as legitimate interest, public interest, or legal obligation.

Additionally, the service provider may need to verify the identity of the requesting customer before providing access to the personal data to ensure the data is only disclosed to authorized persons.

Example:
Alex uses a fitness app, FitTrack, which processes his biometric data, including heart rate and activity levels, to provide personalized health insights. After deciding to switch to a new app, HealthSync, Alex wants to transfer his biometric data to avoid losing his historical health records. Exercising his right to data portability, Alex requests FitTrack to provide his biometric data in a structured, commonly used, and machine-readable format. FitTrack, having obtained Alex's biometric data based on his consent, complies with the request, verifying Alex's identity to ensure security. Once the data is transferred to HealthSync, Alex seamlessly continues to track his health metrics without any disruption, benefiting from the continuity and usability of his personal biometric information across different service providers. This example demonstrates how the right to data portability empowers individuals to maintain control over their biometric data, ensuring ease of transfer and continued use across various platforms.

COMPLIANCE OBLIGATIONS IN THE BIOMETRIC PROCESSING

10.1. Registration with the ODPC

All entities processing biometric data are supposed to register with the Office and must thus register as Data controllers and/or data processors.

The Office has published a guidance note on registration of Data Controllers and Data Processors which is accessible through *www.odpc.go.ke*. The guidance note includes a step-by-step guide on how to complete the registration and the information required during the registration process.

10.2. Duty to Notify

One of the key principles of data protection is transparency. The biometric data processed by service providers shall be processed fairly and in a transparent manner. Privacy notices or policies must explicitly include processing of biometric data where applicable and be updated in real-time to reflect any changes in processing practices, data sharing arrangements, or technologies used.

Therefore, at the time of processing, entities must comply with the obligations under Section 29 of the Act. This provision requires that data controllers and data processors notify data subjects of their rights specified in the Act; inform them that personal biometric data is being processed, state the purpose of the processing; disclose any third parties who may receive the data and the safeguards adopted; provide the contacts of the data controller or data processor and the safeguards adopted; provide the contacts of the data controller or data processor and disclose whether any other entity may receive the data; describe the technical and organizational security measures taken to ensure data confidentiality and integrity; state if the data is being processed pursuant to any law and if it is voluntary or mandatory; and outline the consequences if data subjects fail to provide all or part of the requested data.

The above information should be provided to data subjects to enable them to understand how their personal data is used. The duty to notify should be contained in a data protection policy or a privacy statement. The Data Protection Policy acts as a notice to the subscribers whose data is to be processed or otherwise processed. This policy must be brought to the attention of all data subjects prior to the processing of their personal data or as soon as possible soon after where information is not processed directly. The data protection policy should also be provided to subscribers upon request.

When drafting a privacy policy, there are several practical tips and considerations that should be considered to ensure it effectively communicates to data subjects how their personal data will be used, these include:

1. The policy should be **written in clear and plain language** that is easy to understand. Technical or legal jargon should be avoided as much as possible to ensure that data subjects can easily comprehend what the policy says.
2. The policy should be **transparent and comprehensive**, covering all the relevant information that data subjects need to know about the processing

of their personal data. This includes information about the rights of data subjects under the Act, the fact that personal data is being processed, the purpose for which the personal data is being processed, the third parties to whom the data may be transferred, and any safeguards in place to protect the data.

3. The policy should be **accessible to data subjects**. This can be achieved by making it available on the data controller's or data processor's website, or by providing a copy upon request.
4. The policy should be reviewed and updated regularly to reflect any changes in data processing practices or in relevant laws and regulations.

To make privacy policies easy for data subjects to understand, it is important to use plain language and avoid technical jargon. Visual aids such as infographics and diagrams can also be used to help convey complex information. In addition, using a question-and-answer format or breaking down the policy into shorter sections with clear headings can make it more digestible for data subjects. Providing examples of how personal data may be used in practice can also help data subjects to understand the policy and the implications of sharing their personal information.

Example of a clear and concise Privacy Policy

Transparency in the processing of biometric data is a value upheld by biometric security system vendor Maji Ltd. Maji Ltd conforms with Section 29 of the Act when gathering biometric information, such as fingerprints and facial recognition, for access control.

The procedure consists of:

1. letting data subjects know about their rights and the processing of their biometric data.
2. stating the reason for the gathering (for example, access control).
3. naming all potential recipients of the data as well as the protective measures in place.
5. supplying the data controller's or processor's contact details.
6. describing the security precautions used to guarantee the integrity and confidentiality of data.
7. indicating whether the processing of data is mandatory or voluntary and describing the repercussions of withholding the data.
8. Maji Limited's privacy policy goes into detail and is available on their website or upon request.
9. To make the policy easy to read, it is presented in simple terms and contains illustrations.
10. Every so often, Maji Ltd evaluates and updates the policy to take into account modifications to applicable legislation or data processing practices.
11. This guarantees that biometric data is processed by Maji Ltd in an equitable and transparent manner, allowing data subjects to comprehend the use of their personal information.

10.3. Privacy by Design and Default

The continued use of biometric technology in processing of personal data poses serious privacy risks because it has the potential to reveal much more about a data subject than just their identity. For instance, retina scans, and other methods, can reveal medical conditions and thus biometric technology in its initial design must comply with privacy by design and default principles.

The Act, in section 41, outlines the requirement for data controllers and/or processors to implement appropriate technical and organisational measures, including but not limited to encryption, access controls, and regular security audits, to ensure effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the data controller must ensure that only necessary personal biometric data is processed, considering the amount of data processed, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by design is an approach that ensures data controllers and data processors consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

This could be achieved by data controllers and/or processors specifying the personal data required before the processing starts, appropriately informing individuals and only processing the personal data needed for the specific purpose. Applying appropriate security measures to such data, and its processing environments, both at rest and in transit, is vital to ensure the personal data is protected to the highest standards. Security measures should consider the current state-of-the-art data security methods and techniques in the field of data processing.

Service providers should take appropriate security measures to prevent accidental or unauthorized access to, destruction, loss, use, modification, or disclosure of personal data. These measures include training in privacy and security; access controls; confidentiality agreements; and physical controls.

Some of the appropriate safeguard data handlers could include, implementing secure data transmission protocols and encryption techniques to protect customers' personal data. For example, a telecommunication company may implement end-to-end encryption to secure personal data during transmission and establish secure user authentication methods.

Entities should ensure that they are continuously raising awareness on data protection among staff and their stakeholders. This should also include raising awareness internally of security measures that their organisation is implementing and the proper procedures for conducting tasks related to or involving personal data.

To ensure interoperability and correct data interchange between different biometric applications and systems, the International Electrotechnical Commission (IEC) has developed several International Standards for a wide variety of biometric applications. As technology evolves, however, so do the data elements and formats. So, in order to avoid any future interoperability challenges, data controllers and/or processors are advised to adhere to the released standards and other future standards. The first in this series have

just been published and includes, but is not limited to:

- ISO/IEC 39794-1, Information technology – Extensible biometric data interchange formats –: Framework
- ISO/IEC 39794-4, Information technology – Extensible biometric data interchange formats –: Finger image data
- ISO/IEC 39794-5, Information technology – Extensible biometric data interchange formats –: Face image data
- KSISO IEC 24745:2022 Information security, cybersecurity and privacy protection - Biometric information protection, which covers the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer
- KS ISO 19092:2023 Financial services - Biometrics - Security framework which describes the security framework for using biometrics for authentication of individuals in financial services

10.4. Engagement of Data Processors

Many entities handling biometric data work with vendors/service providers (data processors) providing different cloud-based and data management solutions or security guard services. Entities should consider the vendors they engage and ensure that they opt only for a data processor who provides sufficient guarantees that processing will meet the requirements under the Act and protect data subjects' rights. In particular, in instances where a data controller processes biometric data, they must remain aware of their ongoing responsibilities as data controllers. Controllers must demonstrate due diligence to establish the vendor's and/or service provider's ability to protect personal data.

To assist with this, the Act sets out that where an entity engages a vendor or service provider (processor) to process the information on its behalf, there must be a written contract stipulating that the processor acts only on the controller's instructions and is bound by the instructions of the controller. Further, both parties should take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor complies with the relevant security measures.

Further, the Act specifies that a contract between a data controller and data processor should include key elements, such as the subject matter of processing, the type of personal data, the nature and duration of processing, security measures, and situations requiring prior authorisation from the controller. The contract must also outline the obligations of the processor to ensure confidentiality, assist the controller in meeting its obligations under the Act, and erase and/or delete all biometric data or cease the processing of such biometric data when the contract ends, discharges or terminates. The contract should include provisions for auditing and inspection, as well as liability in case of failure to meet obligations or acting outside the controller's instructions.

Example:

Biometric access control systems provider Mambo Ltd works with cloud-based data management provider Mambo Safi Ltd. To safeguard the rights of data subjects, Mambo Ltd must guarantee that Mali Safi Ltd complies with all the Act, regulations, policies, rules and practices. To ensure that Mambo Safi Ltd can protect the privacy of biometric data, Mambo Ltd performs extensive due diligence on the company. They created a contractual agreement that states that Mali Safi Ltd will only process biometric data in accordance with the guidelines provided by Mambo Ltd to fulfill the assigned duties. In this regard, Mambo Ltd is the data controller while Mali Safi Ltd is the data processor. They go ahead and draw a controller – processor agreement and included in the contract is:

i. the type of biometric data involved and the subject matter of the processing.
ii. the nature of processing.
iii. Appropriate safeguards to keep the data safe.
iv. requirements for consent from Mambo Ltd prior to taking any decision outside the contractual agreement.
v. Mali Safi Ltd to maintaining employee privacy, supporting Mambo Ltd in fulfilling duties and obligations, and
vi. Mali Safi cessation of processing upon conclusion, discharge or termination of the contract.
vii. The contract also specifies the nature and extent of responsibility in the event of non-compliance, operating outside the intended scope and mandate, and
viii. audit, and inspection procedures.

By doing this, Mambo Ltd and Mali Safi Ltd guarantee that biometric data integrity and confidentiality are maintained in accordance with the Act.

10.5. Limitations on Data Transfers

According to Section 49 of the Act, the processing of sensitive personal data out of Kenya shall only be effected upon obtaining informed consent of a data subject and on obtaining confirmation of appropriate safeguards. The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests. The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

A data controller and/or processor should therefore ensure the following:

- A DPIA specifically related to the data transfer, assessing the risks to data subjects' rights and detailing the safeguards that have been put in place to mitigate these risks.
- A comprehensive overview of the types of personal data being transferred, the purposes of processing, and the categories of data subjects affected.
- Consent forms utilized to seek consent for transfer of data where feasibly possible.
- Copies of contracts or agreements with third-party service providers in the destination country, in line with Section 42 and Regulation 24. This should include details on how compliance will be monitored and enforced, including any audit rights and the roles of each third-party recipient.

- Detailed description of the technical and organizational measures implemented to protect the data before, during, and after the transfer. This might include encryption, pseudonymisation, access controls, and data minimization techniques.
- Details of the mechanisms in place to ensure that data subjects can exercise their rights (e.g., access, objection, erasure) effectively in the destination jurisdiction.
- Procedures for notifying relevant stakeholders, including the Office and data subjects, in the event of a data breach.

Example 1

The management at Mani Payment Service Provider, which is a government organ, is considering storing its data in South Africa. Due to the strategic interests of the state and sensitive nature of the personal data held by the service provider, which also includes biometric data used by its clients (the data subjects) for verification and validation in accounts managements, the bank must comply with the conditions of data transfers according to the Act. To achieve this, the service provider should: -

i. obtain consent of all the concerned data subjects (its clients),
ii. obtain confirmation of appropriate safeguards;
iii. demonstrate the effectiveness of these security safeguards;
iv. fulfill requirements for data localization.

10.6. Biometric Data Localization

Data localization refers to the practice of storing and processing personal data within the country's borders. Section 50 of the Act and Regulation 26 of the General Regulations provide that a certain category of personal data and sensitive personal data, must be processed through a server or data centre located in Kenya or, in the alternative, an organisation processing those listed categories of data, must store at least one full serving copy of the personal data in a data centre located in Kenya.

Entities must ensure at least one full, up-to-date serving copy of biometric data is stored in a data centre located in Kenya, in line with Section 50 of the DPA and Regulation 26.

10.7. Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far as possible. A DPIA may not eliminate all risks altogether but should help identify and manage them. There is often more than one way of achieving an outcome.

Given the wide range of sensitivity of biometric data, Data controllers and/or processors who intend to process biometric data must first consider whether such processing is necessary at all. Regulation 49(1)(c) of the General Regulations, 2021, identifies processing of biometric data to be a high-risk processing operation, and Section 31(1) of the Act provides that for any processing that is likely to result in a high risk to data subject's rights

and freedoms, by virtue of its nature, scope, context and purposes, the organisation shall, prior to the processing, carry out a Data Protection Impact Assessment (DPIA).

The Office has published a Guidance Note on Data Protection Impact Assessments at www.odpc.go.ke. The Guidance Note includes the form in which a Data Protection Impact Assessment should be submitted and guidance on when it should be submitted.

A DPIA must be conducted and submitted to the ODPC at least 60 days before initiating any biometric data processing, with emphasis on risks specific to biometric technology such as irrevocability, data permanence, etc.

10.8. Notification of Breach

Biometric data breaches must be reported to the ODPC within 72 hours and to affected data subjects without undue delay. Such notifications must include specific mitigation steps and biometric-specific risks.

Additionally, entities must provide the number of data subjects affected, the personal data or classes of personal data affected, and the potential harm to the affected data subjects. The entity must also provide information on any action taken to mitigate the harm and remedy any failure or shortcoming that contributed to the breach and how affected individuals can mitigate potential harm.

Example 1:

Mvua Ltd, a biometric security systems management business, suffered a cyber-attack where hackers unlawfully accessed employees' fingerprint and facial recognition for purposes of illegal trade of biometric data. Within 72 hours of becoming aware of the compromise, it notified the ODPC as mandated and required as per the Act about the data breach. Among the steps in the process were:

i. Notifying the Data Commissioner of the breach in writing, detailing the period when the breach occurred and the period when the entity became aware of the breach, the nature and extent of the breach, and the nature and extent of damage done and/or expected on concerned data subjects as a result of the breach and the mitigation measure being undertaken to mitigate the breach.
ii. Identifying and determining whose biometric data is impacted and whether the data subjects may suffer any consequences and to which extent
iii. Notifying the concerned data subjects of the breach via written notice of the breach, including the period when the breach occurred and the period of discovery and the mitigation measure being undertaken to mitigate the breach, further advises them on how to eliminate or mitigate potential harm and offers free data monitoring services.
iv. The company conducts a review of its security measures and implements additional measures to prevent future breaches.

By doing this, Mvua Ltd ensured compliance with the Act and protected the rights and interests of the data subjects concerned. Breach notification can be filed with the Office in a number of ways, including through a breach notification form accessible through www.odpc.go.ke, by email or by post.

10.9. Penalties for Non-compliance

Non-compliance with the Act's requirements for processing biometric data can lead to significant penalties, including fines, reputational damage, and legal liability. The Office can impose fines and take other corrective measures where a data handler fails to protect biometric data adequately.

ANNEX: COMPLIANCE CHECKLIST

A service provider can use the following checklist to determine if they are compliant with the Act and other subsidiary regulations.

#	Description	Yes	No	Comments/ Remedial Actions
	We respect the right to privacy as a fundamental human right as provided by Article 31(c) and (d) of the Constitution.			
	We have identified an appropriate legal basis for our processing under Section 30 of the Act (DPA).			
	When we process biometrics which is sensitive personal data, we identify permitted grounds under section 44 of the DPA			
	We restrict processing where the legal basis or legitimate interests cease to apply.			
	We do not do anything generally unlawful with personal data or inconsistent purpose for processing.			
	We are subject to mandatory registration; we have submitted to the Office of Data Protection Commissioner (ODPC) accurate and up-to-date information concerning our processing activities.			
	We have considered how the processing may affect the individuals concerned and can justify any adverse impact.			
	We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified			
	We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject.			
	We do not deceive or mislead people when we process their personal data.			
	We have clearly identified our purpose or purposes for processing and have clearly documented those purposes.			

	We include details of our purposes in our privacy notices.			
	We use technical measures to limit the possibility of repurposing personal data.			
	We only process personal data, which is adequate, relevant, and limited to what is necessary for our specified purposes.			
	We can demonstrate the relevance of the data to the processing in question.			
	We periodically review the data we hold and delete anything we don't need.			
	We avoid the creation of more copies or entry points for data processing than is necessary.			
	We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
	We have appropriate processes in place to check and verify the accuracy of the data we process, and we record the source of that data.			
	We use technological and organisational design features to decrease inaccuracy and mitigate risks			
	We have a process in place to identify when we need to keep the data updated to fulfill our purpose properly, and we update it as necessary.			
	We know what personal data we hold and why we need it.			
	We carefully consider and can justify how long we keep personal data.			
	We have a policy with standard retention periods where possible.			
	We regularly review our records with a view of identifying personal data that no longer requires to be retained and delete or anonymise such data.			
	We have clearly identified our purpose or purposes for processing.			
	We have documented those purposes.			

	We include details of our purposes in our privacy notices.			
	We regularly review whether the processing is necessary for the purposes for which the data was processed and test the design against purpose limitation.			
	If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose, or we obtain specific consent for the new purpose.			
	Where we rely on consent to process data, we ensure that the data subject has freely given informed consent			
	We have ensured that our consent forms have met the conditions of consent set out in the Act and Regulations			
	We have ensured that the data subject is aware of their right to withhold or withdraw consent and explained the consequences of doing so			
	Where the data subject wishes to withdraw their consent, we have made the process easily accessible to them			
	We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards and a valid consent is from data subjects			
	We checked and fulfilled all conditions set under part VI of the DPA and Regulations 2021.			
	We have put in place a framework for data subjects to exercise their rights when their data is transferred out of the country			
Data Mapping				
	We fully understand the nature of personal data held by the organization			
	The organization conducts data mapping with well documented results			
Data Subjects Rights				
	We have a documented policy/procedure for handling Data Subject Access Requests			
	We have put mechanisms in place to respond to Data Subject Access requests within the stipulated timeframes in the Act			
	We have put procedures in place to provide individuals with their personal data in a structured format, including a machine-readable format			

	We ensured that controls and procedures are in place to allow personal data to be deleted or rectified where applicable			
	There are controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing			
	Data subjects have been informed of their right to object to certain types of processing			
	There are controls and procedures in place to halt the processing of personal data where an individual has objected to the processing			
	Explicit consent has been collected and documented where automated decision-making based on consent has a legal or significant effect for an individual			
	Where an automated decision is made which is necessary for entering into, or performance of a contract, or based on the explicit consent of an individual, there are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision.			
Data Processor Agreements				
	We have agreements with data processors where such third parties process biometric data on our behalf.			
	The agreements have been reviewed to ensure all appropriate data protection requirements are included.			
Data Protection Impact Assessments (DPIAs)				
	Biometric data processing is considered high risk, and we conduct DPIA all the time to identify and mitigate risks.			
	We submit our DPIA to the Office of the Data Protection Commissioner 60 days prior to engaging in any process that requires of Biometric data processing			
	We regularly audit our processes and update our DPIAs			
Data Breach Response Obligations				
	We have a documented privacy and security incident response plan			
	We have procedures in place to notify the Office of the Data Protection Commissioner of a data breach			

	We have procedures in place to notify data subjects of a data breach			
	We regularly review our plans and procedures			
	We maintain a data register where all data breaches are fully documented			
	We have cooperation procedures in place between data controllers, data processors, and other partners to deal with data breaches			