OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes on Processing by Micro, Small & Medium Enterprises

2025

TABLE OF CONTENTS

DEFINITIONS

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

"Anonymisation" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

"Confidentiality" is the degree to which access and disclosure of given information is limited to authorised entities (e.g., users) and for intended purposes only, thereby preventing access by or disclosure to unauthorised entities (users).

"Data Commissioner" means the person appointed pursuant to 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 Handler" means a Data Controller and/or a Data Processor.

"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.

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

"Enterprise" means an undertaking or a business concern, whether formal or informal, engaged in production of goods or provision of services;

"Farm enterprise" includes micro and small scale agricultural, livestock and fishing enterprises;

"Manufacturing sector" means enterprises that add value to basic raw material to produce an enhanced product;

"Medium enterprises" means a firm with an annual turnover of between Ksh.5 – 100 million and engaging between 51-250 employees; in the manufacturing sector, total assets and investment in plant and machinery or the registered capital of the enterprise does not exceed Ksh.250 million; in the service and agricultural sectors, investment in equipment or registered capital of the enterprise does not exceed Ksh.125 million.

"Micro enterprise" means a firm, trade, service, industry or a business activity—

a) whose annual turnover does not exceed five hundred thousand shillings;
b) which employs less than ten people; and
c) whose total assets and financial investment shall be as determined as in the Micro and Small Enterprises Act, 2012, and includes—
    i. the manufacturing sector, where the investment in plant and machinery or the registered capital of the enterprise does not exceed ten million shillings;
    ii. the service sector and farming enterprises where the investment in equipment or registered capital of the enterprise does not exceed five million shillings;

"MSMEs" means Micro, Small and Medium Enterprises;

"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" is the right of individuals to be free from unauthorised intrusion, surveillance, and publicity. This is the ability to control access to personal information and activities.

"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, color, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behavior, location or movements;

"Processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as
(a) collection, recording, organisation, structuring;
(b) storage, adaptation or alteration;
(c) retrieval, consultation or use;
(d) disclosure by transmission, dissemination, or otherwise making available; or
(e) alignment or combination, restriction, erasure or destruction.

"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;

"Legitimate Interest Assessment (LIA)" means a form of risk assessment that should be conducted when personal data processing is based on legitimate interest.

"Sensitive personal data" is 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.

"Small enterprise" means a firm, trade, service, industry or business activity—

a) whose annual turnover ranges between five hundred and five million shillings; and
b) which employs between ten and fifty people; and
c) whose total assets and financial investment shall be as defined in Section 2 of the Micro and Small Enterprises Act, 2012**,** and includes—
    (i) the manufacturing sector, where the investment in plant and machinery as well as the registered capital of the enterprise is between ten million and fifty million shillings; and
    (ii) service and farming enterprises, where the equipment investment as well as registered capital of the 2012 Micro and Small Enterprises No. 55 7 enterprise is between five million and twenty million shillings;

THE OFFICE

The Office of the Data Protection Commissioner (Office) is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It is responsible for 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 of persons located in Kenya by both private and public sector organisations.

The Office plays a vital role in ensuring that individuals have control over 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 uniquely positioned to facilitate both the government and private sector entities in achieving Government's strategic goals under the "**Bottom-Up Economic Transformation Agenda**" and, in particular, 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.

FOREWORD

Micro, Small and Medium Enterprises (MSMEs) are the backbone of Kenya's economy, accounting for the vast majority of businesses and contributing significantly to employment, innovation and national output. Recognising their vital role, the Government of Kenya continues to support MSMEs through the Bottom-Up Economic Transformation Agenda (BETA) and the Digital Superhighway by enhancing digital infrastructure, building skills and expanding digital services. However, as these enterprises increasingly embrace digital tools and data-driven solutions, they also assume greater responsibility in ensuring the lawful, fair and transparent processing of personal data.

The Data Protection Act, 2019, established a comprehensive legal framework for the protection of personal data and created the Office of the Data Protection Commissioner (Office) to oversee its implementation. While compliance with data protection obligations is a legal requirement, it is equally a business imperative. For MSMEs, responsible data management fosters customer trust, strengthens competitiveness, and enhances access to local and international markets. Conversely, non-compliance can expose businesses to reputational damage, financial penalties, and loss of consumer confidence.

This Guidance Note has been developed to provide MSMEs with a simplified and practical resource to support their compliance journey. It outlines the key principles of data protection, lawful bases for processing, the rights of data subjects, and the compliance obligations specific to MSMEs. It also provides practical examples, sector-specific insights, and a compliance checklist to make the requirements of the law more accessible and actionable for enterprises of varying sizes and capacities.

The Office recognises the unique challenges faced by MSMEs in aligning with multiple regulatory requirements amidst limited resources. Accordingly, this Guidance Note complements existing support mechanisms, such as awareness programmes, templates, and self-assessment tools developed by the Office. Through these efforts, we aim to make compliance attainable, particularly for small businesses, while reinforcing the overarching goal of safeguarding the dignity, privacy and rights of all Kenyans.

It is my expectation that this Guidance Note will assist MSMEs in embedding data protection within their daily operations, not as an administrative burden but as a core component of ethical business practice and long-term sustainability. By embracing these principles, MSMEs will not only comply with the law but also play a pivotal role in building a trusted, resilient, and inclusive digital economy for Kenya.

Immaculate Kassait, MBS
Data Commissioner

INTRODUCTION

Background

The Kenya National Bureau of Statistics estimates that Micro, Small, and Medium-sized Enterprises (MSMEs) constitute approximately 98% of all business entities, registered and non-registered, in the country. MSMEs substantially contribute to job creation, innovation, and economic growth, therefore playing a significant role in Kenya's economy. However, a lack of awareness regarding legal obligations particularly in relation to data protection presents significant compliance challenges and undermines trust among customers and partners

According to the Economic Survey of 2022, small businesses contributed 33.8% of the national output. The number of MSMEs is poised to grow, as seen by their annual growth rate, particularly as they become the drivers of innovation. MSMEs operate in all sectors of the economy, with greater concentrations in the wholesale, retail trade, agriculture, hospitality and manufacturing.

In recognition of the crucial role MSMEs play, the Micro and Small Enterprises Act of 2012 was enacted to promote and regulate their development. The Act defines and sets thresholds for entities that qualify as MSMEs, based on key criteria such as the number of employees, revenue, and company assets. One of the objectives of the Act is to ensure compliance with existing policies among MSMEs. To this end, the MSE Authority, created under the Act, monitors and evaluates the implementation of policies affecting MSMEs, which are required to meet various legal requirements to operate lawfully.

Challenges in complying with numerous statutory requirements were highlighted in a situational analysis of the SME sector in Kenya, as noted in the Kenya Micro and Small Enterprises Policy of 2020. The policy further emphasises that non-compliance hinders access to markets and services. Additionally, it underscores the importance of innovation and technology adoption to enhance business efficiency.

An area of compliance that is less recognised among MSMEs is data protection, which remains a relatively new legal field in the country. While data protection law may be novel, the collection and use of personal data in business is not. MSMEs collect personal data, either manually or through automated systems, which requires compliance with the Data Protection Act. As technology adoption continues to grow, with off-the-shelf solutions like mobile money services, payroll systems, websites, and social media marketing becoming more common, MSMEs must responsibly incorporate these tools in line with the Act to foster consumer trust.

The importance of protecting personal data among MSMEs is driven by several factors, including the growing role of data in driving business competitiveness and increasing awareness among consumers about the need to safeguard their privacy.

To support MSMEs in complying with data protection requirements, the Office provides assistance through awareness programs, simplified compliance processes, and self-assessment tools. The Office has also developed sector-specific guidance, templates, and

online resources tailored to help MSMEs understand and efficiently implement the requirements of the Act.

Privacy Concerns

The nature of processing data by MSMEs raises significant privacy concerns, including the potential misuse of personal data, lack of transparency around data processing, and the inadequacy of technical and organisational safeguards implemented.

The increasing adoption of technologies among the MSMEs has made them a target for cyberattacks, putting the privacy of collected and stored data at risk. Another critical privacy concern is how vendors use the personal data to which they access. Untrustworthy vendors can collect and reuse personal data in ways that MSMEs may not be aware of, such as using data for direct marketing purposes or packaging and selling data to third parties.

Due to the heavy initial cost of technology adoption, most MSMEs have opted for cloud-based solutions such as email platforms, mobile money systems and SaaS-based inventory tools, that present their own set of risks, such as data transfer to unsafe jurisdictions and the minimal control over data that data subjects have in a cloud system setup.

Another privacy concern that faces MSMEs is where non-automated means are used to process personal data. Non-automated means, such as manual record-keeping or face-to-face interactions, often have the following privacy concerns:

i. **Unauthorised Access** - Manual records held by MSMEs can be easier to access without proper authorisation, leading to breaches of privacy if sensitive information falls into the wrong hands. For example, paper files left unattended or shared among individuals without proper clearance pose significant risks.
ii. **Human Error** - Manual processes are prone to human error, including misfiling documents, unintentional disclosure of information, or inadequate data protection measures. Such errors can compromise the privacy of individuals whose data is being handled.
iii. **Limited safeguards** - Non-automated means may lack robust security measures compared to automated systems, making them more vulnerable to theft, loss, or tampering. For example, physical documents may not be encrypted or protected by access controls, increasing the risk of data breaches.
iv. **Inadequate consent management** – MSMEs may find obtaining and managing consent manually to be cumbersome and prone to oversights, leading to potential violations of the act.
v. **Excessive and/or insecure retention and disposal of personal data** - manual records may be more susceptible to retention beyond necessary periods or improper disposal practices, increasing the risk of unauthorised access or misuse of outdated information. Proper procedures for retention and secure disposal are essential to mitigate these risks.

By prioritising privacy and data protection, MSMEs in Kenya can enhance customer trust, mitigate legal risks, and safeguard the confidentiality and integrity of personal information.

Scope and Purpose

This Guidance Note applies to the processing of personal data by MSMEs and seeks to provide a clear understanding of their obligations under the Act. It presents a simplified approach to assist MSMEs in understanding the scope of their data processing activities, including the collection, use, retention, disclosure, and disposal of personal data. The Guidance Note is intended to help MSMEs implement best practices for data protection while promoting compliance with the Act.

The Guidance Note applies to all MSMEs established or ordinarily resident in Kenya that process the personal data of data subjects located in Kenya or not established or ordinarily resident in Kenya but processing personal data of data subjects located in Kenya. It sets a minimum standard for data protection practices, which can be supplemented by additional measures to ensure the protection of privacy and individual rights. MSMEs are encouraged to adopt further safeguards, particularly when handling sensitive or high-risk data.

This Guidance Note considers:

a) The Data Protection Act, 2019;
b) The Data Protection (General) Regulations, 2021;
c) The data protection (Registration of data controllers and data processors) Regulations, 2021;
d) The Data Protection and Privacy Policy, 2018;
e) Other applicable laws and regulations and
f) International Best Practices.

Legislative Framework

The legal framework for data protection covering MSMEs is aimed at protecting personal data and ensuring that it is processed, stored, and shared in a lawful, fair, and transparent manner. All sectors in Kenya are regulated by laws and policies that require and recognise data protection principles when personal data is processed. In addition, the legislative framework demonstrates how data in the MSMEs is perceived in the adoption of new technology in the sector and gives insight as to the extent to which data protection has been considered in the implementation and use of new technologies that are implemented by MSMEs.

The laws include:

(i) **The Constitution of Kenya** – Article 31 (c) and (d) recognises the right to privacy including, the right not to have a citizen's personal information in relation to their family or private affairs, unnecessarily required or revealed.

(ii) **The Data Protection Act, 2019–** This is the legislative framework designed to safeguard personal data and ensure individuals' privacy rights are protected. In the context of MSMEs, the Act applies to the collection, processing, storage, and usage of personal data pertaining to employees, customers, suppliers, and other

stakeholders. Further, the Act establishes the Office as a regulator to oversee the processing of personal data in Kenya.

(iii) **The Micro and Small Enterprises Act, 2012:** This Act provides for the development, regulation, and support of micro and small enterprises in Kenya. It outlines measures for promoting entrepreneurship, facilitating access to finance, and enhancing the competitiveness of MSMEs.

(iv) **The Companies Act, 2015**: The Companies Act governs the registration, operation, and dissolution of companies in Kenya, including MSMEs. It provides regulations for the formation, management, and governance of companies, regardless of their size.

(v) **The Business Registration Service Act, 2015:** This Act establishes the Business Registration Service, which oversees the registration of businesses, including MSMEs, in Kenya. It provides for the registration of business names, partnerships, and companies, among other entities.

Application of Data Protection Principles

Lawfulness, fairness, and transparency

Personal data collected by MSMEs must be processed lawfully, fairly and in a transparent manner. In lawful processing, the requirement is that MSMEs shall process personal data in accordance with the law by identifying a legal basis for processing the personal data such as obtaining consent of the data subject, fulfilling a contract, complying with a legal obligation, protecting the vital interests of a data subject, performing a task carried out in the public interest or exercising official authority, or pursuing legitimate interests, where permissible.

MSMEs shall further ensure fairness by maintaining a Record of processing activities, notifying data subjects of the processing and offering opt-out mechanism for obtained consent. This includes being transparent about how the data collected is being processed and ensuring that they are aware of their rights regarding their personal data. The personal data processed should be handled transparently and fairly, in a way that a data subject would reasonably expect and not used in ways that are unjust or discriminatory.

Example:

Mazingira retail business specialises in selling environmental-friendly household products. The company ensures compliance with the principle of lawfulness, fairness, and transparency by explicitly informing customers about the data they collect, and reasons for collection, and obtaining consent before processing any personal information for marketing or transactional purposes. The company develop simplified privacy notices using plain language and visual aids where possible, also maintains a transparent and easily accessible privacy notice on its website. The privacy notice is also read out to customers who place orders through calling. The notice outlines the types of data collected, the purposes of processing, the legal basis for processing, data retention periods, and information about customers' rights under the Act. Fairness in data processing is achieved by providing equal opportunities and services to all customers. They do not use personal data for

discriminatory purposes and treat all customers equally in their marketing efforts and product offerings. The company ensures lawfulness by having a valid lawful basis for processing personal data. For example, they may process customer data based on consent obtained during account registration or for fulfilling contractual obligations, such as processing orders and delivering products. Lastly, the company regularly reviews and updates its data processing practices to ensure compliance with data protection regulations. They stay updated with changes in legislation and adapt their policies and procedures accordingly to maintain transparency and legality in their operations.

Purpose limitation

This principle requires that personal data should only be collected and processed for an explicit, specific, and legitimate purpose determined at the time of the collection of personal data. To comply with this principle, MSMEs must have clarity on what personal data will be used for and should not be used for any other purpose inconsistent with the identified legal purposes/basis.

Example:

Kangaruu software development company ensures compliance with the principle of purpose limitation under the Act by explicitly stating the purpose of data collection to its clients, primarily focused on developing custom software solutions. The company collects only the necessary personal data, such as client contact information and project specifications, required for software development projects. Further, it strictly limits the use of collected personal data to the intended purpose of developing software solutions for its clients. Any data obtained from clients is solely utilised for project management, communication, software development, and related support activities.

The company also seeks explicit consent from clients before using their data for any purposes beyond the agreed-upon scope of software development. For instance, if the company intends to showcase completed projects on its website for marketing purposes, it seeks separate consent from clients. Lastly, the company implements internal controls, data anonymisation and access restrictions within its systems to ensure that employees only access client data necessary for their job roles related to software development. Access to personal data is limited to authorised personnel, reducing the risk of unauthorised use or sharing of data. The company also conducts regular internal checks to ensure data processing activities align with the defined purposes. They review data handling practices to verify adherence to the principle of purpose limitation and make necessary adjustments as required.

Data Minimisation

This principle of data protection emphasises collecting and processing only the minimum amount of personal data necessary for a specific purpose.

Example:

Saku Ltd operates an e-commerce platform where it gathers customers' personal information to facilitate product delivery. Saku Ltd limits its data collection to only essential details required for order processing, such as the customer's name, delivery address, and payment information. Requesting additional information, such as the customer's social media accounts or irrelevant personal data, would contravene the principle of data minimisation. After completing the order, sensitive payment information is either deleted or anonymised.

Accuracy

The personal data collected by MSMEs must be accurate and kept updated, with necessary steps being taken to ensure that inaccurate data is erased or rectified. MSMEs should establish adequate routine verification measures and ensure that data subjects can easily exercise their right to rectification.

Example:

Fedha Ltd operates as a financial advisory company. To uphold the accuracy principle, Fedha Ltd enforces a comprehensive verification procedure for gathering client financial details. They verify all data inputted into their systems, including names, addresses, contact information, and identification numbers, by cross-referencing them with official documents.

To maintain accuracy, Fedha Ltd conducts regular updates, client engagement for data review, internal quality checks, documentation of changes, and reviews client access to information. Furthermore, Fedha Ltd ensures that employees are educated on the importance of accurate data and are equipped with the necessary tools to update, verify, and maintain accuracy in client records. These practices help ensure that the financial information held by the firm is accurate, up-to-date, and reliable for providing sound financial advice to clients while complying with the Act.

Storage Limitation

This principle requires MSMEs to ensure that personal data is kept in a form that identifies data subjects for no longer than necessary and stores their data for no longer than the purposes for which it was collected. Personal data should be reviewed periodically and erased or anonymised where it is no longer needed. However, certain laws or regulations mandate retaining data for a specific timeframe, e.g., tax records.

Example:

A small online e-commerce platform company complies with the storage limitation principle by having a clear policy outlining retention periods for different types of customer data. For example, they retain order history and transaction details for a specific period necessary for accounting and customer service purposes, usually as required by tax laws. The platform also employs automated processes to routinely identify and delete outdated customer data beyond the defined retention periods. This includes clearing customer profiles that have been inactive for a specified duration. The platform restricts the collection of unnecessary customer data. They only collect essential information for processing orders, customer support, and marketing communications, minimising the volume of stored data. The platform provides account management options for customers to control their data. Users can edit or delete their profiles, including personal information or order history, through a self-service portal. The company conducts periodic reviews of stored customer data. They verify that retained data aligns with their defined retention periods and delete any information that exceeds the prescribed limits. Customer data stored is encrypted and securely stored using industry-standard security protocols. This ensures the protection and confidentiality of stored information. Lastly, the company regularly updates its data retention policies to adapt to changing regulations and conducts internal compliance checks to ensure ongoing adherence to the storage limitation principle.

Integrity and Confidentiality

This principle requires that personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Confidentiality and data security are critical principles in the data protection sector, given the sensitivity and volume of the personal data collected. This principle requires that personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing against accidental loss, destruction, or damage. Therefore, all technical procedures used to gather, process, store, use, or distribute data should make use of strong security safeguards, for which threshold standards must be established. This may involve data encryption, security keys, two-factor authentication, and password requirements.

Example 1

Mkesho Ltd is a marketing agency that collects and processes personal data for its clients' marketing campaigns. To ensure the security and confidentiality of the data, the agency ensures that all personal data collected from its clients, such as customer contact information, is stored in a secure and encrypted database. Access to this database is restricted to authorised personnel only, using strong authentication methods. The agency conducts regular security assessments and

audits of its systems and processes to identify and address any vulnerabilities or risks that could compromise the security of the stored personal data. This includes testing for potential breaches and updating security protocols accordingly.

Example 2

Safari Traders diligently manages the personal data of its clients, employing manual filing systems for record-keeping. These files are meticulously maintained within a secure cabinet, safeguarded by safety lock. Access to these files is strictly restricted to authorised personnel, ensuring confidentiality and data integrity. Safari Traders prioritises the protection of client information, adhering to stringent security measures to prevent unauthorised access. By upholding these standards, Safari Traders fosters trust and reliability, reinforcing its commitment to safeguarding the privacy and confidentiality of its clientele's personal data.

Accountability

Accountability involves taking proactive steps to safeguard personal data and demonstrate compliance with the principles of data protection. The accountability principle within the MSMEs refers to the responsibility of data handlers to ensure compliance with relevant laws and regulations related to the processing of personal data and sensitive personal data. MSMEs should have policies and procedures in place to govern the collection, use, and disclosure of personal data, which should be reviewed and updated regularly to ensure compliance with changing legal and regulatory requirements. Additionally, MSMEs should maintain documented compliance records including but not limited to training logs, audit logs, DPIA records and personal data breach handling procedures.

Example:

Jitume Ltd demonstrates the accountability principle by implementing measures geared towards ensuring privacy at the earliest stages of its processing operations. Data protection principles and practices are strictly adhered to. The company has privacy policies and notices, maintains records of its processing activities, and has appropriate organisational and technical measures in place to ensure the confidentiality and security of the records. It has also a designated Data Protection Officer responsible for ensuring compliance with the Data Protection Act.

Lawful Basis of Processing

Before processing personal data, MSMEs, as data handlers, must identify the appropriate legal basis for processing personal data as different legal bases come with specific requirements. Based on the nature of their processing, MSMEs may choose one legal or multiple legal bases to guide their processing activities.

Consent

Many MSMEs use consent as the legal basis for processing personal data. As such, they must ensure that consent is express, unequivocal, freely given, specific, and informed. It must represent a clear indication of the data subject's wishes, given either by a statement or by a clear affirmative action, signifying agreement to the processing of their personal data.

This means individuals must have a genuine choice about whether or not to consent to the processing of their personal data. They must also be provided with sufficient information to understand what data is being processed, for what purpose, and how it will be used. Furthermore, individuals must have the ability to withdraw their consent freely and easily at any time, should they change their mind.

Minors cannot validly give consent, and as such MSMEs must seek for valid consent from their parent or legal guardian and ensure that the consent is specific, informed, and freely given.

The elements of valid consent:

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

Example 1

Uptown Boutique in Nairobi, specialising in handmade jewelry and clothing, wants to send promotional emails and SMS messages to its customers to inform them about new arrivals, special offers, and upcoming sales events. The boutique needs to obtain consent from its customers before sending marketing communications to ensure compliance with data protection regulations in Kenya.

The boutique can obtain explicit consent for marketing by providing the customers with clear and easy-to-understand opt-in options. This often involves checking a box or clicking a button on websites, sign-up forms, or during checkout processes.

Additionally, the business can offer preference centers where customers can customise their marketing preferences, such as opting in or out of specific types of communications or choosing their preferred communication channels. For in-person transactions, businesses can provide a physical form to be signed.

The consent process should be documented to demonstrate compliance with the Act and avoid potential legal and reputational risks.

Example 2

ZetuKe is a studio that specialises in children's portraits. The studio plans to offer a discounted package deal for the December holidays and wants to use existing photos of minors as testimonials and examples of their work.

Since minors cannot give consent, the studio must obtain permission from parents or guardians to use their children's images for advertising. They should specify where the images will be used and for how long. The studio should also have a clear policy for the retention and disposal of the photographs and associated data after the advertising campaign period. The studio should also inform parents and guardians that they have the right to withdraw consent at any time. If consent has been withdrawn, the studio should stop using photos as testimonials.

Performance of a contract

Personal data may be processed if the processing is necessary for the performance of a contract to which the data subject is a party. Entities in the MSMEs sector may process personal data to fulfill a contractual obligation and must not use it for any other purposes not related to the contract's performance. This provision also covers pre-contractual relationships. For instance, in cases where a party intends to enter into a contract, but has not yet done so, possibly because some checks remain to be completed. If one party needs to process data for this purpose, such processing is legitimate as long as it is necessary, in order to take steps at the request of the data subject prior to entering into a contract.

Example;

Anzani applies for a loan from a microfinance company, Tumaini Credit Ltd. To assess the application and define loan terms, the financial institution collects Anzani's personal data including ID number, income details, employment status, and credit history. This data is processed as necessary steps before entering into a contract i.e. the loan agreement. Based on the assessment, the institution offers Anzani a loan with specific terms and interest rates. Once the contract is signed, some of the data continues to be processed for repayment tracking and customer service. After the loan is settled, non-essential data is securely deleted, while key records are retained for regulatory and accounting purposes.

Compliance with Legal Obligation

Personal data may be processed where it is necessary for a data controller to comply with a legal obligation. For MSMEs, adherence to legal obligations is fundamental not only to ensure lawful operations but also to safeguard their interests and foster trust with stakeholders. These

obligations can arise in various areas, including business registration, taxation, employment law, health and safety requirements, environmental compliance, consumer protection, and data protection, among others.

Accordingly, MSMEs may lawfully rely on the legal obligation basis for processing personal data where such processing is essential to meet these regulatory requirements.

Example

Mwakazi Enterprises, a small manufacturing business with 25 employees, processes personal and financial data of its employees, including bank details, KRA PINs, National Social Security Fund (NSSF) numbers, and Social Health Insurance Fund (SHIF) membership numbers. Mwakazi Enterprises processes this data as part of its legal obligation to comply with various Kenyan labour laws and tax regulations, which require the company to remit statutory deductions to relevant authorities such as the Kenya Revenue Authority (KRA), NSSF, and SHA.

Protection of Vital interests of the data subject or another natural person

The Act recognises that there may be situations where the processing of personal data is necessary to protect the vital interests of the data subject or another natural person. "Vital interests" are those fundamental aspects of life essential to an individual's well-being, survival, or safety. In such cases, an entity may process personal data without the data subject's explicit consent, particularly when obtaining consent is not possible.

Example:

An employee at a beauty shop collapses during working hours and becomes unresponsive. The supervisor, witnessing the medical emergency, immediately calls for an ambulance. While waiting for the ambulance to arrive, the supervisor retrieves the employee's personnel file to provide the paramedics with the employee's full name, age, known allergies, and emergency contact information.

Upon arrival, the paramedics request additional medical information to administer appropriate care. The supervisor contacts the employee's next of kin, who shares critical details about the employee's medical history, including a known heart condition and prescribed medication.

In this situation, both the supervisor and the next of kin are justified in sharing the employee's personal and medical information without explicit consent. Their actions fall under the lawful basis of protecting the employee's vital interests, as the data processing is necessary to preserve the life and health of the employee in an emergency where consent cannot reasonably be obtained.

Legitimate interests

The Act provides that personal data may be processed if it is necessary for the purposes of the legitimate interests pursued by the data handler or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection. MSMEs should ensure that any processing of personal data under this basis is necessary and proportionate, and that it does not infringe upon the rights and freedoms of data subjects. Where applicable, MSMEs should conduct a Legitimate Interest Assessment (LIA) to demonstrate compliance and to ensure that their legitimate interests do not override the rights of the data subjects.

Example 1

Msoko Ltd, a small business specialising in organic produce, collects customer data through its loyalty programme, including names, contact details, and purchase history. It uses this data to analyse buying trends, adjust stock levels, reduce waste, personalise promotions, and plan deliveries more efficiently. These actions support its legitimate interest in improving business performance and enhancing customer experience.

Before proceeding, Msoko Ltd carries out a Legitimate Interest Assessment (LIA) to evaluate necessity, balance its interests against customers' privacy rights, and confirm the processing is transparent, limited in scope, and includes safeguards like data minimisation, clear privacy notice and an opt-out option for the customers.

Historical, Statistical, Journalistic, Literature and Art or Scientific Research

While this lawful basis is not commonly used by most MSMEs, personal data may be processed on the basis of historical, statistical, journalistic, literary, artistic, or scientific research in limited circumstances. This basis is relevant where an MSME engages in activities such as customer trend analysis, product testing, or small-scale research projects. For instance, a health-tech startup analysing anonymised user feedback to improve wellness solutions may rely on this lawful basis.

Where applicable, this basis requires an entity to implement strict safeguards, including anonymisation or pseudonymisation, adherence to data protection principles, and a clear demonstration that the processing serves a public interest without infringing upon the rights and freedoms of data subjects.

Rights of a Data Subject

These are rights of a data subject exercisable with respect to the processing of their data. The Act grants data subjects specific, enforceable rights regarding their personal information. The goal of data protection is to empower data subjects and ensure they have control over how their personal data is processed. MSMEs should ensure that data subjects are allowed to exercise their rights and that appropriate data subjects' rights requests handling procedures are implemented. The following are the rights of the data subjects:

Right to be informed

This is the right to be informed of the use of the data. It allows data subjects to know what personal data is collected about them, why, who is collecting data, how long it will be kept, how they can file a complaint, and with whom their data is shared. The right to be informed promotes transparency by helping data subjects understand what will be done to their data. The duty to inform can be exercised at the time of collecting personal data or any time during the processing period or after it has been processed.

Example

XYZ Manufacturing Ltd. collects personal data from its employees and suppliers during the onboarding process. This data includes names, ID numbers, contact information, and account details. In line with the right to be informed under data protection principles, the company ensures that all individuals are provided with a clear and accessible privacy notice. The privacy notice explains how their personal data will be used, who will have access to it, the legal basis for the processing, how long the data will be retained, and the rights individuals have in relation to their data.

The company ensures the privacy notice is provided at the time of collection, therefore enabling employees and suppliers to understand how their data is handled and to make informed decisions about their personal information.

Right to access personal data

A data subject has the right to access personal data that is held by a data controller/processor. This includes the type and details of data held about them. This right allows the data subject to have visibility on what personal data is being processed. To exercise this right, a data subject can make an access request. The Regulations require that an access request be fulfilled within seven (7) days and should be free of charge.

Example 1

Jikoni Limited collects personal data from its customers and prospective customers during an online shopping experience. The company has provided a link on its portal that allows customers to access their personal information, along with the privacy policy that outlines the procedure for doing so. The customers have the right to request access to their personal

information. This access can be made by logging in to the portal with their password, allowing them obtain their information.

Example 2

Kijana shops at EPC supermarket for his daily supplies. Kijana has a loyalty card where he provided his name, ID number, and contact details. Kijana has a right to access his personal data in the custody of EPC supermarket. The supermarket must provide the same within 7 days and with no charges upon request.

Right to rectification of personal data

The right to rectification of personal data allows individuals to request corrections to any inaccurate, outdated, misleading, or incomplete information held about them by an MSME. To comply with this right, MSMEs must establish clear procedures and technical systems to receive such requests, verify the validity of the claims, update the records accordingly, and notify the individual once the correction has been made.

This right plays a critical role in ensuring the accuracy and integrity of personal data, which in turn supports fair treatment and improves the quality of service delivery to customers, employees, and other stakeholders.

Example

Alex, a customer of Nunua Market Place App, discovers that his name has been misspelt in the portal. After reading through the privacy policy in the Nunua Market Place App portal, he notes the prescribed procedure for correction of any details and the customer support contacts provided. He contacts customer support, verifies his identity, and requests the correct name to be updated. After confirmation, the representative updates the name to reflect the correct information provided by Alex.

Nunua Market Place App sends a confirmation email acknowledging the rectification. Alex verifies the change by logging into his account with the corrected details. This demonstrates his right to rectification, as he promptly notified Nunua Market Place App of the error, and it was promptly corrected.

Right to object to all or part of their personal data being processed

This right allows individuals (data subjects) to object to the processing of their personal data, which may result in the processing being stopped. Whether a data subject can object to processing depends on the legal basis on which such personal data is processed. A data subject may not object to processing if the personal data is being used:

i. For a task carried out in the public interest
ii. For the exercise of official authority

iii. For the legitimate interests of the data controller/processor that override the data subject's interests.

A request to object to processing cannot be fulfilled where the personal data is required to establish, exercise or defend a legal claim and where a data controller's legitimate interests override the data subject's interests. A data subject may exercise this right by:

i. Giving a verbal or written reason(s) why the controller should stop using the data
ii. Stating what should happen to the personal data

Once an objection is raised, the data controller is required to assess the request and inform the data subject of the outcome, including whether the objection has been upheld or rejected, and the reasons for the decision.

Example

Emy is a regular customer of a small bookstore. Emy has been receiving promotional emails from the bookstore but no longer wishes to receive them due to a change in her preferences. Even though she initially subscribed to the bookstore newsletter, she now wants to stop receiving marketing emails.

Emy decides to exercise her right to object to the processing of her personal data for direct marketing purposes by the bookstore. She emails the bookstore using the contact information provided in the promotional emails. In her email, she clearly states her objection to the processing of her personal data for marketing purposes and requests the immediate cessation of such communications. She mentions that she wishes to opt out of receiving any further marketing emails or promotional materials from the bookstore and provides her email address, and any relevant identifiers used by the bookstore to ensure they can identify and cease sending her promotional communications.

The bookstore promptly acknowledges Emy's request, confirming the receipt of her objection. They inform her that they will immediately cease processing her data for marketing purposes and will update their records accordingly.

The bookstore takes swift action to honour Emy's request. They update their systems to ensure that Emy's email address or contact details are flagged as opted-out for marketing communications. They cease sending her any further promotional emails or marketing materials and confirm to Emy through a follow up email that her objection has been processed.

Right not to be subjected to automated decision making

This right protects a data subject from being subjected to a fully automated decision. An automated decision takes place when an electronic system uses personal data to make a decision without human intervention. In most cases, automated decision making closely relates to profiling, which is automated processing of personal data to evaluate or determine certain features (such as performance at work, economic situation, health, preferences, interests, reliability, behaviour or location) related to the natural person.

As with other data subject rights, this is not an absolute right, and a data subject may be subjected to decision making that is based solely on automated processing under certain circumstances; such as where a data subject consents, where a decision is necessary for entering or performing a contract between a data subject and a data controller, and where such automated decision making is authorised by a law that has suitable safeguards.

MSMEs that make decisions which produce legal effects or significantly affect the data subject based solely on automated processing must notify the data subject as soon as reasonably practicable and take necessary steps such as reconsidering the decision or making a new decision not based solely on automated processing.

Example

John is seeking a loan from a microfinance organisation that relies on automated systems to evaluate creditworthiness. His application is rejected exclusively based on an automated decision. Exercising his right to avoid being subject to such decisions, John asks for a human review. A credit officer reevaluates his application manually, taking into account additional context that was not part of the automated assessment. This results in a new decision granting approval for the loan. The procedure maintains fairness by integrating human judgment with automated processing.

Right to erasure

This right, commonly referred to as the right to be forgotten, allows data subjects to request the deletion or removal of their personal data by a data handler. A data subject may request a data handler to delete personal data concerning them when the data handler is no longer authorised to retain the personal data, the personal data is irrelevant, the personal data held by the data handler is excessive or the personal data was obtained unlawfully.
Where the data handler has shared the personal data with a third party for processing purposes, the data handler shall take all reasonable steps to inform third parties processing such data, that the data subject has requested for the erasure or destruction of such personal data.

However, the right to erasure is not absolute and a data controller may decline a request to erase personal data in its custody when the personal data is required for evidence. In this case, the data controller shall restrict processing and inform the data subject within a reasonable time. A request to erase data shall be met within 14 days.

Example:

Faith bought shoes at "Ndula Fiti Kenya"; a shoe store located at Nakuru town dealing in ladies' shoes. She left her name and contact details at the store for the purposes of being notified when the new shoes are in stock. Faith is no longer interested in buying shoes from the store and requests deletion of her data from the store's database. Ndula Fiti Kenya has an internal data protection policy that guides on the deletion procedure when the customer requests for such

deletion. After the verification of Faith's request, Ndula Fiti Kenya reviewed records and deleted her data promptly within 14 days and notified her of the same via a text message.

Right to data portability

This right allows a data subject to receive a copy of their personal data in a structured, commonly used, and machine-readable format, and the right to transmit that data to another data controller without hindrance, where this is technically possible. A data subject may not exercise this right in certain scenarios such as where processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority and when porting data may adversely affect the rights and freedoms of others. The Data Protection (General) Regulations, 2021 require that a request to port data be met within 30 days of receiving the request. Where porting requests are complex and numerous, the period may be extended for a period to be determined in consultation with the Data Commissioner. A data controller may charge a reasonable fee for the request. While there is no stated figure, best practice dictates that the fee must not exceed the cost of implementing the request.

Example:

Sarah is a subscriber to MelodyStream, which she has been using for several years to stream music and create playlists. She decides to exercise her right to data portability to transfer her music preferences and playlists to a new music streaming service called "StreamVibe." Sarah logs into her MelodyStream account and navigates to the account settings where she finds an option for data portability. She selects the 'Export Data' feature and confirms her request to receive her music preferences and playlists in a portable format. Upon receiving Sarah's request, MelodyStream prepares her data in a portable and commonly used format, liked tracks and music history. MelodyStream notifies Sarah via email once her data export is ready. The email contains a secure link or download option for Sarah to access and download her music preferences and playlists in the portable format to her device.

Sarah creates an account on StreamVibe and navigates to their 'Import Data' section. She uploads the file containing her music preferences and playlists, following StreamVibe's instructions for importing external data. StreamVibe processes the imported file and verifies the data provided by Sarah. Once verified, Sarah's music preferences, playlists, and liked tracks from MelodyStream are replicated within her new StreamVibe account, allowing her to continue her music experience seamlessly. Sarah verifies that her playlists, liked tracks, and other music preferences have been accurately imported into her new StreamVibe account. She can access her favorite songs and playlists, ensuring a smooth transition to the new music streaming platform.

Compliance Obligations

1.1. Registration with the Office

The Act establishes a legal obligation on all entities, including individuals, that process personal data to register with the Office, subject to certain thresholds for mandatory registration. Given that most MSMEs in Kenya operate informally, any MSMEs processing personal data must ensure timely registration and renewal as a data controller and/or a data processor.

The Office has published a Guidance Note on the Registration of Data Controllers and Data Processors, which provides a step-by-step guide for completing the registration process and outlines the required information. This guidance can be accessed through the website www.odpc.go.ke.

1.2. Data Mapping

To fully understand the nature of personal data held by MSMEs, it is crucial to conduct a thorough data mapping process with well-documented results.Data mapping is an initial step that will help MSMEs better understand what personal data is collected, why it is collected, where it is stored, whether the personal data is needed, how it moves internally within systems, and how it flows out of the organisation to third parties.

An ancillary benefit of data mapping that MSMEs could leverage is having records of their processing activities (ROPA) documented. Records of processing activities are instrumental in numerous ways, including:

- Demonstrating accountability, which is useful in the event of compliance audits by the Office;
- Complying with data protection principles and;
- Identifying a legal basis and facilitating managing data subject rights.

Additionally, due to the dynamic nature of MSMEs, the process of data mapping should be continuous as they might collect different categories and types of personal data at various stages of the business or depending on the nature of the business at a particular point in time.

Data mapping maybe broken down into various processes that MSMEs can rely on:

- Data discovery: the process of finding out what personal data MSMEs processes, and learning how and why it processes personal data;
- Data inventory: enables MSMEs to document the types of personal data they process, identify where the data is stored (both the physical asset and its geographic location), and include additional details such as the legal basis for processing, retention periods, and access controls.
- Data flow mapping: establishing how personal data enters and exits.

A basic guide to data mapping involves asking the following questions:

- What personal data do we process?
- Why do we process personal data?
- Where do we obtain, store, and send personal data?
- When do we delete personal data?
- Who has access to the personal datain our custody?

1.3. Privacy by Design and Default

Data protection by design is a concept that refers to the incorporation of data privacy and security measures into the design of products, services, and systems from the very beginning, rather than as an afterthought. This is especially important for MSMEs, where extensive personal information is processed.

Section 41 of the Act outlines the requirement for entities to implement appropriate technical and organisational measures to ensure the effective implementation of data protection principles and necessary safeguards in data processing. Also, it is a requirement that only necessary personal data is processed, considering the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

MSMEs should engage in self-regulation by adopting strategies that would incorporate data protection measures by default into existing systems and practices to ensure compliance with the Act. This means that data protection measures must be in place from the onset, without relying on individuals to take additional steps to protect their personal information. Examples of data protection by default by MSMEs would include:

a. **Access controls:** Implementing access controls, such as password-protected accounts, can help to ensure that only authorised personnel have access to customer information.
b. **Data encryption:** Encrypting customer information at rest and in transit can help to prevent unauthorised access and protect against data breaches.
c. **Anonymisation:** This involves removing all identifying information from customer information, making it impossible to identify individuals.
d. **Data retention policies:** Implementing policies that limit the retention of personal customer information to only what is necessary can help to reduce the risk of privacy breaches and protect individual privacy.
e. **Data protection impact assessments:** Conducting regular data impact assessments can help MSMEs identify and mitigate potential privacy risks in the processing of personal information. More information on how to conduct DPIA is available below in Section 6.5.
f. **Data protection policies and procedures:** MSMEs should establish clear and comprehensive data protection policies and procedures that outline the measures taken to protect personal data. These policies should be communicated to all employees and regularly reviewed and updated.
g. **Staff training:** All staff should receive regular training on data protection policies and procedures. This can include how to handle personal data, how to recognise and respond to data breaches, and how to comply with data protection regulations.

h. **Physical Safeguards:** MSMEs should ensure that personal data is safeguarded through physical measures such as fireproof cabinets, lockable desks and lockable offices.

Example:

Safari Traders, a tour company, operates a secure customer booking management system where all collected data is encrypted both in transit and at rest, access is restricted to essential personnel with strong, unique passwords, and their privacy policy transparently outlines its data processing activities.

The company also maintains manual files that contain personal data. These files are stored in a fireproof cabinet under secured locks. Moreover, a straightforward data access or deletion process is available on their website, and all staff have undergone training on the significance of data privacy and the company's protective measures.

1.4. Data Retention

MSMEs are required to only collect and retain personal data for as long as it is necessary to fulfil the purpose for which it was originally collected. Once the purpose has been fulfilled, personal data should either be erased, anonymised or pseudonymised to ensure it is not retained beyond the required period. MSMEs should further ensure that personal data is not stored indefinitely, thus reducing the risk of data breaches and misuse of personal data.

MSMEs should establish clear personal data retention schedules that specify the retention purpose, duration, among other details. Regular audits should also be conducted to ensure personal data that has already fulfilled its intended purpose is not unnecessarily retained, the information held is up-to-date and the purpose of retention has been clearly specified.

Example

Kazisasa Solutions manages data storage limitations principle by implementing a clear data retention policy, regularly reviewing personal data (including client names, email addresses, contact numbers, and service usage statistics), and securely disposing of data that is no longer needed. The company applies short-term, medium-term, and long-term measures to ensure compliance with data protection principles and maintains transparent communication with clients about their data storage practices.

1.5. Data Protection Impact Assessment (DPIA)

The carrying out of a DPIA is mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". In situations where it is unclear whether a DPIA is

required, it is recommended that a DPIA is carried out nonetheless as a DPIA will be a useful tool to help MSMEs comply with data protection laws. Furthermore, the Act requires that all data controllers and processors implement appropriate technical and organisational measures and integrate appropriate safeguards to ensure adequate protection of personal data. Certain processing activities are considered high-risk and would typically necessitate a DPIA. These include, but not limited to:

- Automated Decision Making with a legal or similar significant effect that includes profiling.
- The large-scale processing of personal data for purposes different from those for which it was originally collected.
- Processing sensitive personal data or children's data.

Example

Tiba, a small health service offering health services, decides to launch a health information management system to manage their services. Aware of the importance of data protection, Tiba decides to conduct a Data Protection Impact Assessment (DPIA) before launching the new system.

In conducting the DPIA, Tiba outlines the project's scope, explains its processing activities, identifies and assesses the risks associated with the system as well as the mitigation measures for the identified risks.

The Office has published a Guidance Note on Data Protection Impact Assessments on 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.

1.6. Notification and Communication of Data Breach

Data controllers must notify the Office within 72 hours of personal data breaches that occur without delay within 72 hours of becoming aware of the breach, whereas the data processor must report to the data controller within 48 hours of becoming aware of the breach. Where there has been unauthorised access, MSMEs are required to communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established. To fulfil these and other obligations under Section 43 of Act, MSMEs should have documented robust personal data breach handling and reporting procedures.

In reporting a data breach to the Office, MSMEs need to provide the following:

1. The date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;
2. A chronological account of the steps taken by the data controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;
3. Details on how the notifiable data breach occurred, where applicable;

4. The number of data subjects or other persons affected by the notifiable data breach;
5. The personal data or classes of personal data affected by the notifiable data breach;
6. The potential harm to the affected data subjects as a result of the notifiable data breach;
7. Information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissioner of the occurrence of the notifiable data breach to
    i. eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or
    ii. address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach; the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach; and
    iii. contact information of an authorised representative of the data controller or data processor.

Example 1

Rimbo Ltd, a business specialising in personal care products, has experienced a data breach in which customer email addresses and order histories are exposed due to a vulnerability in their e-commerce platform. Understanding the seriousness of the situation, Rimbo Ltd takes immediate action to address the breach and ensure notifying the Office of the Data Protection Commissioner within 72 hours of becoming aware of the breach. The notification provides a detailed account of the breach and the steps taken to mitigate potential harm. It further informs the affected individuals about the breach, advises them on mitigation measures, and the security safeguards adopted to prevent future breaches.

Example 2

DataKE Solutions Ltd., acting as the data processor for CBS National Bank, detects a data breach and notifies the Bank within 48 hours, as required by their contractual and regulatory obligations. Upon receiving the breach notification, CBS National Bank, being the data controller, promptly notifies the Office of the Data Protection Commissioner and affected customers within 72 hours. Both DataKE Solutions Ltd. and CBS National Bank collaborate to contain the breach, support affected individuals and implement corrective measures to ensure continued compliance with the Data Protection Act.

1.7. Engagement of Data Processors

MSMEs often engage various service providers to deliver different solutions or services which may involve processing personal data on their behalf or for its purposes. Before sharing

personal data with a data processor, MSMEs should ensure that the data processor is registered with the ODPC and that a written contract (Data Processing Agreement) stipulating the data processing obligations of the parties and terms of engagement must be entered into by the parties.

It is important for MSMEs to engage with service providers who demonstrate the ability to protect data subject rights and personal data confidentiality in compliance with the requirements under the Act. This will help to ensure that personal data is handled securely and ethically, and that privacy is protected. Both parties should, however, take all reasonable steps to ensure that any personnel action on their behalf complies with the relevant security measures.

Example

Data Controller (DC): Mkate Bakery that processes customer personal data such as name, address, contact details.

Data Processor (DP): Fikisha Haraka, a courier service provider that the DC has outsourced to facilitate quick deliveries to its customers' orders.

Contract Terms: The DC and the DP will enter into a written contract that stipulates

processing details including instructions of the DC, duty on the data processors to obtain a commitment of confidentiality from any person or entity that the data processor allows to process the personal data, security measures subjecting the data processor to appropriate technical and organisational measures in relation to keeping personal data secure, a provision stipulating that all personal data must be permanently deleted or returned on termination or lapse of the agreement, as decided by the data controller, data breach notification obligations, and auditing and inspection provisions by the data controller.

1.8. Commercial Use of Personal Data

Commercial use of data happens when a data controller/processor uses personal data to advance their economic interests. Several instances amount to commercial use of data such as direct marketing and data brokerage, such as buying and selling personal data to other businesses.

A common example of commercial use of personal data among MSMEs is direct marketing. However, not all marketing efforts fall under commercial use of personal data. For example, when a marketing agency places a billboard on a highway which does not contain any personal data.

Example

Jirani Foods leverages customer data for commercial use by personalising marketing campaigns, analysing customer behavior, and selling aggregated data insights. By doing so, the company not only improves its service offerings but also creates new revenue streams. Importantly, the company ensures compliance with Data Protection Act by obtaining consent, anonymising data where necessary, informing the customer of how their personal data is being processed and providing opt-out options to customers.

a. Lawful commercial use of personal data

For commercial use of personal data to be lawful, some conditions that must be met include:

- Collection of personal data from the data subject
- Notifying the data subject of the intended commercial use
- Obtaining express consent from the data subject
- Data controllers are required to provide simple opt-out mechanisms
- Data controller imposes safeguards such as anonymisation to protect the identity of the data subject

b. Unlawful commercial use of personal data

Common challenges for lawful commercial use of personal data that MSMEs need to be aware of include:

- Complex notification and consent processes through hard-to-read data protection notices. The Regulations propose using appropriate consent management mechanisms including documenting the consent forms.
- Using hard-to-navigate opt-out mechanisms. The Regulations provide guidance on how to comply with the opt-out requirements and features of an opt-out message.
- Sending unsolicited marketing emails without obtaining prior consent or ignoring opt-out requests. MSMEs need explicit consent from individuals before sending commercial information.

1.9. Data Sharing

The Data Protection (General) Regulations,2021 guide on the conditions to be met for lawful data sharing. Any data sharing should be restricted to the purpose and means stated by the data controller/processor.

Personal data may be shared upon request by another controller, processor, third party, or data subject, provided the sharing is for clearly defined purposes, and appropriate safeguards are in place. Where sufficient safeguards are lacking, explicit consent from data subjects is required.

Data subjects must be informed about how their data will be used, who will access it, and any potential privacy risks. Data controllers and processors must clearly define the purpose and means of sharing, establish written agreements before routine sharing, and implement

strict access and security controls. All data sharing arrangements must be regularly reviewed to ensure compliance and effective risk management.

Requests for sharing must be made in writing, specifying the purpose, retention period, and safeguards. Notably, sharing data within the internal structures of a controller or processor is not considered data sharing under the Regulations.

Example:

Tuko-Pamoja Group shares the personal data of its farmers with Tulime Agricultural Co-operative through a data-sharing platform aimed at improving agricultural productivity and market access. Before any data is shared, informed consent is obtained, and a data-sharing agreement is established, specifying the data's use, protection measures, and retention policies. The process complies with the Data Protection Act, ensuring that farmers' privacy is protected while leveraging data sharing for economic and agricultural growth.

1.10. Duty to Notify

One of the fundamental principles of data protection is transparency, which means that personal data collected by entities in the MSMEs must be processed in a fair and transparent manner.

According to Section 29 of the Act, data controllers and data processors are obligated to notify data subjects of their rights specified in the Act, provide them with information about the purpose of data collection, disclose any third parties who may receive the data and the safeguards adopted, describe the technical and organisational security measures, and outline the consequences if data subjects fail to provide all or part of the requested data.

Example

Nguo Ltd, a small MSMEs in Kenya that sells custom-made clothing, decided to launch an online store. As part of its business operations, Mitumba collects personal data from customers, such as names, email addresses, phone numbers, delivery addresses, and payment information. In compliance with the Data Protection Act, 2019, Mitumba Fashion Ltd has a **duty to notify** its customers when collecting their personal data through the online platform.

1.11. Co-operation with the Office

The Office was established to regulate the processing of personal data, and it is therefore crucial for MSMEs to consult with the Office to achieve compliance in the face of limited resources and capacity. The Office has published several guidance notes for reference on its website www.odpc.go.ke. Additionally, MSMEs should take advantage of the regional offices alongside the service desks in Huduma Centers around the country to receive guidance on compliance with the Act and the Regulations.

Annex A- Checklist for Compliance

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

#	Description	Yes	No	Comments/ Remedial Actions
1.	We respect the right to privacy as a fundamental human right as provided by Article 31(c) and (d) of the Constitution.			
2.	We have identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (DPA).			
3.	We process sensitive data, and we have identified permitted grounds under section 44 of the DPA			
4.	We restrict processing where the legal basis or legitimate interests ceases to apply.			
5.	How can we ensure that personal data is always processed lawfully and only for its intended purpose?			
6.	If 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.			
7.	We have considered how the processing may affect the individuals concerned and can justify any adverse impact.			
8.	We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified			

9.	We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject.			
10.	We do not deceive or mislead people when we collect their personal data.			
11.	We have clearly identified our purpose or purposes for processing and have clearly documented those purposes.			
12.	We include details of our purposes in our privacy notices.			
13.	We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.			
14.	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.			
15.	We use technical measures to limit the possibility of repurposing personal data.			
16.	We only collect personal data, which is adequate, relevant, and limited to what is necessary for our specified purposes.			
17.	We can demonstrate the relevance of the data to the processing in question.			
18.	We periodically review the data we hold and delete anything we don't need.			
19.	We avoid the creation of more copies or entry points for data collection than is necessary.			

20.	We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
21.	We ensure the accuracy of any personal data we process and the reliability of our sources.			
22.	We have appropriate processes in place to check and verify the accuracy of the data we collect, and we record the source of that data.			
23.	We carry out tests for accuracy at critical steps.			
24.	We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain.			
25.	We have a process in place to identify when we need to keep the data updated to fulfil our purpose properly, and we update it as necessary.			
26.	If we need to keep a record of a mistake, we clearly identify it as a mistake.			
27.	We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of personal data.			
28.	As a matter of good practice, we keep a note of any challenges to the accuracy of personal data.			
29.	We know what personal data we hold and why we need it.			
30.	We carefully consider and can justify how long we keep personal data.			

31.	We have a policy with standard retention periods where possible.			
32.	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.			
33.	We have appropriate processes in place to comply with individuals' requests for rectification and/or erasure of false or misleading data about them.			
34.	We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.			
35.	We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards or valid consent from the data subject.			
36.	We checked and fulfilled all conditions set under part VI of the DPA and Regulations 2021.			
37.	We have clearly identified our purpose or purposes for processing in the RoPA.			
38.	We have documented those purposes.			
39.	We include details of our purposes in our privacy notices.			
40.	If one of the purposes is direct marketing, we make sure that the data subject is notified that direct marketing is one of the purposes for which personal data is collected or consented to the use of this/her data for the purpose of direct marketing and in any case, is provided with simplified opt-out mechanism.			

41.	We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.			
42.	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.			
Data Mapping				
43	We fully understand the nature of personal data held by the organisation			
44	The organisation conducts data mapping processing with well documented results			
Data Subjects Rights				
45	Is there a documented policy/procedure for handling Data Subject Access Requests?			
46	Is your organisation able to respond to Data Subject Access requests within 14 days?			
47	Are procedures in place to provide individuals with their personal data in a structured format, including a machine-readable format?			
48	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
49	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
50	Are individuals told about their right to object to certain types of processing, such as direct marketing?			
51	Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
52	If automated decision-making, which has a legal or significant similar effect for an individual, is based on consent, has explicit consent been collected?			
53	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, are procedures in place to			

	facilitate an individual's right to obtain human intervention and to contest the decision ?			
Data Processor Agreements				
54	We have agreements with data processors (such as suppliers and other third parties) processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included.			
Data Protection Impact Assessments (DPIAs)				
55	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			
Appropriate technical and organisational security measures				
56	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
57	Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative, and physical safeguards for personal data?			
58	Is there a designated individual who is responsible for preventing and investigating security breaches?			
59	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
60	Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
61	Does the organisation conduct mandatory data protection training for staff engaged in the processing of personal data?			
62	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			
Data Breach Response Obligations				
63	Does the organisation have a documented privacy and security incident response plan?			
64	Are there procedures in place to notify the Office of the Data Protection Commissioner of a data breach?			

65	Are there procedures in place to notify data subjects of a data breach?			
66	Are the plans and procedures regularly reviewed?			
67	Are all data breaches fully documented?			
68	Are there cooperation procedures in place between data controllers, data processors, and other partners to deal with data breaches?			