OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE FOR THE COMMUNICATION SECTOR

DECEMBER 2023

TABLE OF CONTENTS

DEFINITIONS:

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

"Content data" means information contained in an electronic communication and which may include any attachment to such communication that attract a duty of confidentiality information relates to identifiable user of the service.

"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 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 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 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 natural (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 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.

e) alignment or combination, restriction, erasure or destruction.

"Protected System" means a computer system used directly in connection with, or necessary for: -

a) the security, defence or international relations of Kenya.
b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law.
c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically.
d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.
e) the provision of national registration systems; or
f) such other systems as may be designated relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology.

"Register of Data Controllers and Data Processors" means the list of registered entities maintained and published by the Office of the Data Protection Commissioner.

"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.

"Sector Regulator" means the Communications Authority of Kenya established under the Kenya Information and Communications Act, 1998 and Central Bank of Kenya

"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.

"Service Provider" means all and any providers of services falling within the Communications sector.

"Subscriber" means any natural person who is party to a contract with the service provider for the supply of telecommunications services.

"Subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established —

a) the type of communication service used, the technical provisions taken thereto and the period of service; information, available on the basis of the service agreement or arrangement; or
b) any other information on the site of the installation of telecommunication apparatus, available on the basis of the service agreement or arrangement.

"Communication Sector" includes telecommunication, broadcasting, postal and courier services.

"Telecommunications services" includes telephony services, internet and broadband services as well as infrastructure-related services for telecommunications systems.

"Broadcasting services" includes the distribution of audio and video content to a large audience through various means such as television, radio, and online platforms.

"Postal and Courier services" includes the delivery of physical mail and packages from one location to another.

"Telecommunication system" means a system used for transmission, reception and switching of signals, such as electrical or optical, by wire, fibre, or electromagnetic means.

"Traffic data" means the data necessary to convey a message between parties and may include date and time, sender's and receiver's identifiers, devices' related identifiers such as IP addresses, devices' electronic identifiers such as IMEI or SIM based identifiers.

1. 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, both by private and public organisations, in Kenya.

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 of the Data Commissioner 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 of the Data Commissioner 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.

2. INTRODUCTION

Kenya's communications sector is made up of several service providers focused on telecommunication, broadcasting, postal and courier services. These service providers are licensed by the sector regulator.

Under the Act and Regulations, both the sector regulator and service providers have various duties and obligations vis-a-vis data subjects. To support compliance with the Act and Regulations, the Office has developed this guidance note specifically for the telecommunications sector. This guidance note shall provide information on the interpretation and implementation of the Act and Regulations as it relates to the telecommunications sector.

This guidance note shall cover a range of topics related to data protection which include:

a) Application of data protection principles in the telecommunications sector.
b) Lawful basis for processing personal data.
c) Obligations of the sector regulator and service providers as data controllers and/or data processors.
d) Rights of data subjects.

In general, the guidance note provides important information and direction for service providers operating in Kenya, and is a valuable resource for ensuring compliance with the Data Protection Act and protecting the privacy rights of their customers.

3. PRIVACY CONCERNS

Privacy concerns in the communications sector are a significant issue, as people increasingly rely on technology to communicate and share personal information. Here are some of the key privacy concerns in this sector:

1. **Data collection and tracking**: Communication service providers may collect and track a vast amount of personal data, such as phone calls, call logs, text messages, and internet browsing activity. This data can be used to build detailed profiles of individuals, which can be shared with third parties for the purpose strictly not necessary to provide a service requested by a subscriber and/or end-user without their consent.
2. **Encryption and decryption**: Encryption are used to protect sensitive information during transmission, but it also makes it more difficult for law enforcement agencies to access this information. Decryption technologies and backdoors to access encrypted data are controversial, as they may compromise the privacy of users.
3. **Surveillance**: Entities may use communications technology to monitor individuals, including their internet activity, phone calls, and text messages. This surveillance can be done with or without a warrant, and it can be difficult to know when it is happening.
4. **Cybersecurity breaches**: Communications companies can be vulnerable to cybersecurity breaches, which can expose users' personal data and leave them vulnerable to identity theft and other forms of fraud.
5. **Misuse of personal data**: Communications companies may share or sell personal data to advertisers and other third parties without users' consent, which can lead to unwanted marketing messages and other forms of spam.

4. SCOPE AND PURPOSE OF THE GUIDANCE NOTE

The Office of the Data Protection Commissioner is the regulatory office established pursuant to the Data Protection Act, 2019 ("the Act") and charged with the responsibility of exercising oversight on data processing operations to ensure that the processing of personal data of data subjects is carried out in accordance with the Act.

In exercise of the powers of the Data Commissioner pursuant to the Act and the Regulations, this Guidance Note provides other considerations that must be present in when processing subscribers' personal data, network traffic, location or geographical data, financial data, and mobile operators' privacy policies.

This guidance note considers:

a) The Data Protection Act, 2019;
b) The Data Protection Regulations, 2021;
c) The Data Protection and Privacy Policy, 2018;
d) Other applicable laws and regulations and
e) International Best Practice.

This Guidance Note applies to communication service providers processing personal data in either the public or private sectors. This Guidance Note 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 subscriber information, traffic information, location information or contents of a telecommunication.

5. LEGISLATIVE FRAMEWORK

The communications sector in Kenya is governed by several legislative frameworks, including:

A. The Constitution of Kenya, 2010

Article 31 (c) and (d) guarantees the right to privacy with regards to information relating to their family or private affairs unnecessarily required or revealed, or that of their communication infringed.

Article 34 provides for freedom of expression, which includes freedom to seek, receive and impart information and ideas. In the outset, the freedom extends to access to telecommunication services as the services are critical to the exercise of the right to seek and receive information.

Article 35 states that every citizen has the right to access information the State holds and information another person holds, necessary to exercise or protect any right or fundamental freedom.

Article 46 further provides for consumer protection for both goods and services, including telecommunication services. The provision further stipulates the protection of consumers from unfair and unconscionable practices through giving accurate information about goods and services.

B. The Data Protection Act, No. 24 of 2019, establishes the ODPC and further provides for the protection of personal data and privacy of individuals in Kenya, including data collected and processed by telecommunications service providers.

6. APPLICATION OF DATA PROTECTION PRINCIPLES IN COMMUNICATION SECTOR

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

a) **Lawfulness, fairness and transparency**: personal data collected by the service provider must be processed fairly and in a transparent manner, and may only be processed in line with a specific lawful basis.

Example 1: Lawful basis

John is interested in enrolling as a subscriber with Mali Mali Ltd. (a service provider), he is typically required to provide personal information such as his name, address, and phone number during registration. Mali Mali is required by law to collect and process certain personal data from subscriber in order to provide the telecom service.

Example 2: Fairness and Transparency

Mali Mali, a courier service company, wants to start using customer data to personalize marketing messages and offers. However, the company is unsure whether to inform customers about this new use of their data or whether to simply start using it without informing them. As per the DPA, MaliMali should inform customers about the new use of their data and obtain explicit consent, making it clear they have the right to opt-in - opt-out at any time. However, customers should not be opted into marketing services by default unless where they have chosen it. This ensures lawful, fair, and transparent processing of customer data and builds trust through personalized marketing.

b) **Purpose limitation**: service provider must ensure personal data is collected for explicit, specified and legitimate purposes, and must not be used for purposes other than those specified at collection.

Example 1:

John writes an email to Mali Mali to inquire about a service he saw being advertised or to raise an issue/complaint with Mali Mali on poor network coverage. John does not expect to have his email address automatically added to Mali Mali's mailing list or his number added to bulk marketing SMS.

c) **Data minimization**: service provider must ensure that the collected data is adequate, relevant and limited to what is necessary in relation to the purposes for processing.

> **Example:**
>
> Mali Mali, an internet service provider, follows data minimization principles when collecting customer information. During the signup process, Mali Mali only requests essential data, such as the subscriber's name, address, and contact details, to set up and manage the internet connection. Unnecessary data like the subscriber's income, occupation, or marital status is not collected, as it is not relevant to the service provided. By limiting data collection to the necessary information for providing internet services, Mali Mali ensures customer privacy and compliance with data protection regulations.

d) **Accuracy**: personal data collected by service provider must be accurate and be kept updated, with necessary steps being taken to ensure that inaccurate data is erased or rectified.

> **Example 1**:
>
> Mali Mali Solutions, an internet service provider, must ensure that they have accurate records of a customer's name, address, and phone number in order to provide them with telecom services, by validating information during registration, allowing updates, conducting audits, rectifying errors promptly, and erasing irrelevant data when needed. Inaccurate records can lead to errors in billing or disruptions in service, which can negatively impact the customer's experience.

e) **Storage minimization**: service provider must ensure that data is kept in a form that identifies the data subject (subscriber) for no longer than is necessary for the purposes of collection.

> **Example 1:**
>
> Mali Mali, a mobile service provider may need to retain a customer's call and text message logs for a certain period of time in order to provide billing or dispute resolution services. However, once this data is no longer needed, Mali Mali should delete it in order to minimise the amount of personal data that is being stored. Furthermore, Mali Mali should design and implement data retention policies that specify how long personal data is kept. They could equally delete inactive **customer** accounts or personal data that is no longer relevant to Mali Mali's business operations.

f) **Integrity and confidentiality**: service providers should ensure that personal data is safeguarded from unauthorised access and changes. This can be achieved through putting in place robust organisational and technical measures such as policies and procedures for information security and access controls. Data must not be transferred unless there is proof of adequate data protection safeguards. Similarly, service providers must ensure the security of the data in transit and in storage.

Example 1:

Mali Mali, a local Internet service provider, manages its subscriber data by partnering with a local IT company to deploy a Customer Relationship Management (CRM) system. To safeguard the integrity and confidentiality of the data it handles, Mali Mali must implement various organisational and technical measures. These include access control, data encryption both at rest and during transmission, and the ability to maintain an audit trail of system changes. Furthermore, the organization must implement mechanisms to detect unauthorized access..

6.1 LAWFUL BASIS FOR PROCESSING PERSONAL DATA

The Act provides for eight lawful bases for processing personal data. Section 30 of the Act requires that personal data shall only be processed if at least one of eight legal grounds listed in that Section apply.

Broadly, the collection of data for fulfilment of mandates and obligations enumerated in the telecommunication sector that relate to subscriber's personal data include:

6.1.1 CONSENT

As part of compliance with the provisions of the Act on consent, all service providers must obtain express, unequivocal, free, specific and informed consent from the data subject. Section 2 of the Act defines the meaning of consent as being:

i. ***Specific***: The data subject must be informed about the specific purpose for which their data will be processed.

ii. ***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 the data will be used, who will have access to the data, and how long the data will be retained.

iii. ***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.

In this case, from the customer, during registration, accepting terms and conditions for subscriptions and processing of personal data does not meet the condition of consent. Service providers should also have a clear affirmative action signifying processing of personal data relating to the data subject. The Children Act, No. 8 of 2001 defines a child as anyone below 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 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 in order to process personal data of a child.

A DPIA is required prior to the processing as provided for under Regulation 49 of the Data Protection (General Regulations) 2021.

For further information see the Office's Guidance Note on Consent available on www.odpc.go.ke

Example 1:

Mtandao mobile money platform allows users under the age of 18 to create accounts but requires parental consent before creating the account and processing their personal data.

When an individual creates an account, the platform asks for their date of birth to determine if they are under 18. If the individual is a minor, the platform sends a request for parental consent via email or other communication method. The request must clearly explain what personal data will be collected and how it will be used and must provide a way for the parent to give or withhold consent.

If the parent gives consent, the platform can collect and process the minor's personal data. Furthermore, the Mtandao mobile money must ensure the processing is in a manner that protects and advances the right and best interests of the minor.

6.1.2 PERFORMANCE OF A CONTRACT

In instances where a service provider relies on this as a basis for processing of the subscribers' personal data, such as name, address and a phone number, service providers service provider should not process more personal data than is necessary to fulfil its contractual obligations to the subscriber, and must not use the personal data for any other purposes that are not related to the performance of the contract. The subscriber must also be notified of the processing and the purpose for the same.

6.1.3 COMPLIANCE WITH LEGAL OBLIGATIONS

The Kenya Information and Communication (Registration of Sim-Cards) Regulations, 2015 provide for the process for registration of existing and new subscribers of service providers in Kenya. Other instances include where service providers are served with court orders and search warrants as stipulated by the enabling legislation. In addition, communication sector players may be legally obligated to share personal data with government agencies such as Communications Authority, Kenya Revenue Authority, Unclaimed Financial Asset Authority.

6.1.4 LEGITIMATE INTEREST PURSUED BY DATA CONTROLLER OR DATA PROCESSOR

A service provider's reliance on legitimate interest in processing the data should not outweigh the rights and freedoms of the subscribers, or data subjects, at large. For instance, where a service provider anonymously uses the subscribers' call location and GPS location data to map out areas that require improved connectivity as part of enhancing service delivery.

In relying on this basis, service providers must be guided by the principles of purpose limitation and lawfulness, fairness and transparency. The subscribers must equally be informed of the impending action and the purpose for the collection, in addition to the subscribers exercising their rights as data subjects.

6.1.5 PROTECT VITAL INTERESTS OF THE DATA SUBJECTS OR ANOTHER NATURAL PERSON

Service providers may use vital interest as a legal basis in exceptional circumstances when it is necessary to protect the life or physical integrity of a data subject or another person. Exceptional circumstances may include emergency situations, such as during natural disasters or other crises, to facilitate communication and ensure the safety of data subjects.

7. RIGHTS OF A DATA SUBJECT

A data subject has a right: -

a) **To be informed and duty to notify the use to which their personal data** is to be put.

The right to be informed means that data subjects have the right to be provided with clear and concise information about how their personal data will be used. It is an essential aspect of data protection law, which requires data controllers (i.e., service provider) to provide individuals (i.e., customers & subscribers) with specific information about the processing of their personal data. This includes who will be processing the data, why it is being processed, and how long it will be retained. Entities must ensure that this information is accessible to everyone, including people living with disabilities. This may include providing information in alternative formats such as audio, braille, or large print, or making use of assistive technologies such as screen readers or sign language interpreters.

Service providers must provide individuals with information about the purpose and legal basis of the processing. This means explaining why the service provider is collecting and processing personal data, and what legal basis it relies on (such as consent, legitimate interests, or legal obligation).

To comply with the right to be informed, service providers should provide a privacy notice to data subjects. This notice should be easy to understand and accessible to all relevant individuals. When collecting personal data from customers during registration, service providers should provide a privacy notice that explains how their data will be processed, who will have access to it, and the purposes for which it will be used.

Service providers must provide individuals with information about the data retention period. This means explaining how long the service provider will retain personal data, or how this will be determined.

The duty to notify means that data controllers must inform the relevant authorities and data subjects in the event of a data breach. This duty is crucial for ensuring that data subjects take appropriate steps to protect themselves from potential harm.

To comply with the duty to notify, service providers should have a clear procedure in place for reporting data breaches and mitigating risks to individuals. This should include a designated person or team responsible for handling data breaches and notifying the relevant authorities and data subjects. Service providers should also keep a record of all data breaches and how they were resolved.

Example 1:
John is subscribing to pay TV services with Mali Mali TV, a pay TV provider. As part of the subscription process, MaliMali TV must provide John with clear and concise information about the collection, use, and sharing of his personal information. This includes specifying what information will be collected from him (e.g., name, address, payment details), how it will be used (e.g., for pay TV services, billing, marketing), who it will be shared with (e.g., other service providers, marketing companies), how long it will be kept (e.g., for the duration of the subscription or a specific period after it expires), and how John can access, correct, and delete his information. MaliMali TV's transparency in this regard enables customers like John to make informed decisions about whether to use the service and understand the associated risks and benefits.

b) **to access their personal data** in custody of the service providers. All stakeholders have the right to access their personal data. This implies that customers and subscribers have the right to request access to their personal data such as registration details, active subscriptions information, credit information and call data records. In relation to a child, a person with parental authority or guardian has the right to access any personal data held by the service provider.

To exercise this right, customers must make a written request to the service provider that holds that personal data. The service provider must then respond either by giving access to the data or by explaining refusal to grant access. Service providers should comply with a request by a data subject to access their personal data within seven days of the request.

Example 1:
John, a subscriber of Mali Mali services, exercises his right as a data subject to access his personal data held by the service provider. This data includes his bio data, usage history, billing details, and profiles created for personalized services or marketing. Under the Kenyan Data Protection Act, Mali Mali is obliged to provide John with a digital copy of his personal data free of charge and that reasonable printing cost are charged if the personal data is required in paper format. The access request should be responded to within seven days of his request as stipulated in the DPA, 2019. The information must be presented in an accessible manner, ensuring that John can easily understand and review the data collected. This transparency empowers John to be aware of the information held about him and allows him to make informed decisions about the use of his data.

c) **to object to the processing of all or part of their personal data**- the service provider must provide the customer with an opportunity, function or feature for opting out of active subscriptions, promotional and marketing messages to withdraw their consent and it should be clear, accessible and ease to use free of charge.

Examples of when an individual may exercise their right to object to the processing of their personal data include:

i. Marketing: If an individual's personal data is being used for marketing purposes without their consent, they may object to the processing of their personal data.

Example 1:

Mali Mali is currently marketing a newly developed Internet service plan to its existing customers. Part of the marketing strategy is to send promotional messages through SMS and Emails. John, who is an existing customer, has the right to object to the marketing messages. Mali mali should make it possible for John to opt-out of the promotional messages.

ii. Research: If an individual's personal data is being used for research purposes without their consent, they may object to the processing of their personal data.

Example:

Mali Mali is conducting research on customer preferences and behavior to improve their service offerings. They analyze the data they have collected from their customers, including John's personal data. However, John learns that his personal data is being used for research purposes without his consent. In this case, John has the right to object to the processing of his personal data for research purposes. Mali Mali should respect his objection and refrain from using his personal data for research unless they obtain his explicit consent or anonymise the data for research purposes

iii. Third-party access: If an individual's personal data is being shared with third parties for purpose of direct marketing without their consent, they may object to the processing of their personal data.

Example:

Mali Mali has partnered with a third-party advertising agency to improve their targeted advertising efforts. As part of this arrangement, they share customer data, including John's personal information, with the advertising agency. However, John becomes aware that his personal data is being shared with third parties without his consent. In this scenario, John has the right to object to the processing of his personal data for this purpose. Mali Mali should respect his objection and discontinue sharing his data with the third-party advertising agency unless they have John's explicit consent to do so.

iv. Inaccurate data: If an individual believes that their personal data is inaccurate or incomplete, they may object to the processing of their personal data until it is corrected.

Example:

John contacts Mali Mali's customer support team and realizes that some of his personal data in their records is inaccurate. For instance, his address and phone number are outdated, which could lead to communication issues. In this case,

John has the right to object to the processing of his personal data until it is corrected. Mali Mali should promptly rectify the inaccuracies in John's data and ensure that they only process accurate and up-to-date information.

v. Automated decision-making: If an individual's personal data is being used for automated decision-making processes without their consent, they may object to the processing of their personal data.

Example:

Mali Mali has implemented an automated system for credit assessment when customers apply for certain services, and John's application for a new service was recently declined. He suspects that the decision was solely based on automated processing without any human involvement. In this situation, John has the right to object to the processing of his personal data for automated decision-making processes. Mali Mali should reevaluate John's application through a manual review or reconsideration to ensure that his application is treated fairly and not solely reliant on automated algorithms.

d) to not to be subject to automated decision making

Automated decision-making takes place when an electronic system uses personal data to make decisions without human intervention. Automated decision making can help entities in the communication sector improve their customer experience, increase efficiency, and reduce costs. If the personal information is digitally generated, the service provider should have safeguards for protection of the information against digital manipulation. Automated processing is used for various purposes such as registration processes, invoicing & billing, renewing active subscriptions & promotional messages and predictive analytics. However, the use of such systems may have a significant impact on the rights and freedoms of customers, especially if the decisions are made without human intervention or oversight.

The right not to be subjected to automated decision-making in the communications sector enables customers to challenge decisions made by automated systems, such as billing or subscription renewals. This right ensures that decisions that have a significant impact on customers such as registration processes, billing, or even

subscription renewals are made by humans who can consider individual circumstances, biases, and context.

However, it is important to note that the right not to be subjected to automated decision-making is subject to certain conditions and exceptions as stipulated in Section 35 of DPA,2019. For example, this right may not apply if the decision is necessary for the performance of a contract between the customer and the service provider, or if the decision is authorised by law.

Example 1:

Mali Mali is using automated decision making to optimize network performance. by analysing real-time data on network traffic and performance, an automated system can make decisions on how to allocate resources and prioritize traffic to ensure the best possible user experience. This can help to reduce network congestion and improve overall network performance. When using automated decision making to optimize network performance, there is a risk that personal data such as username, IP address and location could be collected and analyzed without the user's knowledge or consent. To mitigate this risk, Mali Mali should implement strong data protection measures such as data minimization and anonymization, and ensure that users are fully informed about how their data is being used. However, this right is not applicable where the decision is necessary for entering into, or performing, a contract between the data subject and a data controller;

Example 2:

Mtaani delivery uses automated decision making to manage its inventory. The system collects data on product sales, returns, and customer feedback, and uses this data to predict future demand and adjust inventory levels accordingly. This can help to reduce waste and improve profitability. However, there is a risk that personal data such as purchase history and customer feedback could be misused or accessed by unauthorized parties. There is also a risk that the system could make incorrect or biased decisions based on factors such as race, gender, or socioeconomic status. To mitigate these risks, Mtaani delivery should implement strong data protection measures such as data minimization and anonymization, and ensure that customers are fully informed about how their data is being used. They should also regularly review and audit their automated decision-making systems to ensure that they are fair and unbiased.

e) **to rectification of personal data**. The service provider is required to rectify the subscribers' false or misleading information without undue delay. The right to rectification allows customers to request the correction of their personal data that is inaccurate, obsolete, incomplete, false or misleading. This means that, if a customer's personal information in the service provider's system is incorrect, they have the right to request that it be updated or corrected. This is particularly important in the telecommunications system, where accurate records are essential for efficient service delivery.

Example 1:

John has noticed that his Internet monthly bills are consistently higher than what he expects based on his usage. He requests Mali Mali his billing data and discovers that the service provider has been charging him for services he did not request or use due to wrong billing information.
In this scenario, John has the right to request correction of the misleading data. He can file a complaint with Mali Mali, and the service provider is obliged to investigate the issue and correct any errors in his personal data in terms of billing. If the service provider fails to correct the personal data, the customer can escalate the issue to the Office of the Data Protection Commissioner, who can enforce the correction of the misleading personal data. .

f) of erasure

The right to erasure commonly referred to as the right to be forgotten, on the other hand, allows telecommunication stakeholders to request that their personal data be deleted if there is no legitimate reason for it to be processed or if they have withdrawn their consent. This means that if a customer or former customer no longer wants their personal information to be stored or processed by the telecommunication system, they have the right to request its deletion.

Example 1:

Mali Mali has collected personal data of John from a direct marketing company without his consent, in violation of the Kenya Data Protection Act. John discovers this and requests that his data to be deleted under the right to erasure.

In this situation, Mali Mali is legally obligated to delete John's personal data without undue delay. This includes any copies of the data that may have been made, such as backups or archives. Mali Mali must also inform any third parties that may have received John's data of the erasure request, and ensure that they also delete the data.

If Mali Mali fails to comply with the erasure request, John has the right to file a complaint with the Office of the Data Protection Authority and seek legal remedies. The company may also face fines and other penalties for non-compliance with data protection laws.

g) **to data portability**

The right to data portability is provided 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. The right to data portability in the telecommunications sector thus allows data subjects to move, copy or transfer personal data easily without hindrance to usability enabling them to obtain and reuse their personal data held by the service providers across different services.

The right to data portability also ensures that the service providers take necessary measures to make personal data available to the data subjects in a structured, commonly used, and machine-readable format. However, right to data portability is subject to certain conditions and exceptions. The right may not apply to:

i. Data that is not processed based on consent of the individual or a contract.
ii. Data processed based on other legal basis 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 authorised individuals.

8. COMPLIANCE OBLIGATIONS IN THE COMMUNICATION SECTOR

8.1. REGISTRATION WITH THE ODPC

All entities in the Communication Sector are subject to mandatory registration.

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 process and the information required during the registration process.

8.2. DUTY TO NOTIFY

One of the key principles of data protection is transparency. The personal data processed by service providers shall be processed fairly and in a transparent manner. Therefore, at the time of collection, 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 data is being collected, state the purpose of the collection; disclosing any third parties who may receive the data 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 organisational security measures taken to ensure data confidentiality and integrity; state if the data is being collected 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**. The Data Protection Policy acts as a notice to the subscribers whose data is to be collected or otherwise processed. This policy must be brought to the attention of all subscribers prior to the collection of their personal data or as soon as possible soon after where information is not collected 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 Data Protection Act, the fact that personal data is being collected, the purpose for which the personal data is being collected, 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 instances where data is collected indirectly:

Example 1:

Mali Mali collects data about its subscribers' usage patterns and location information through their mobile devices. In this case, the service provider could fulfil its duty to notify by including clear language in its privacy policy about the types of data being collected and the purposes for which it is being used. The company could also provide the notice through a pop-up or banner message on its mobile app or website that explains the data collection and provides a link to the full privacy policy.

Suppose a service provider collects data about its subscribers' usage patterns and location information through their mobile devices. In this case, the service provider could fulfil its duty to notify by including clear language in its privacy policy about the types of data being collected and the purposes for which it is being used. The company could also provide the notice through a pop-up or banner message on its mobile app or website that explains the data collection and provides a link to the full privacy policy. Additionally, the service provider could offer a simple opt-out mechanism for subscribers who do not wish to have their data collected.

The data protection policy is an external facing document and is not to be confused with any internal policies that an entity develops to ensure internal practices align with the data protection Act. The common practice of demonstrating compliance with the laws and regulations among controllers and processors is through privacy policies and notices on websites. The information in a data privacy policy must be provided in simple and clear plain language, appropriate language for the target audience and be provided free of charge. The data privacy policy must be kept up to date to meet any changes in your approach to processing data.

8.3. PRIVACY BY DESIGN AND DEFAULT

The Data Protection Act, in section 41, outlines the requirement for data controllers and data processors to implement appropriate technical and organisational measures to ensure effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the act requires 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.

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 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 ensure against accidental or unauthorised 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 measures service providers 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, such as biometric identification, to protect customer data.

Considering the nature and volume of the data processed and the risks for data subjects, some additional physical and organisational measures that should be adopted such as:

a) physical security of paper files;
b) shredding all confidential waste;
c) Keeping devices under lock and key when not in use;
d) not leaving papers and devices lying around;
e) A written information security policy outlining the responsibilities of all staff members in protecting personal data;
f) Regular training for all staff members on data protection best practices and the importance of maintaining the confidentiality of personal data;
g) Regular internal and external audits to assess the effectiveness of technical and organisational safeguards.

Entities should ensure that they are continuously raising awareness on data protection amongst 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 personal data.

Service providers can design, implement, maintain a privacy framework that is aligned with the requirements of the Act and protects the privacy and security of individuals. International standards such as:

- ISO/IEC 27001 (Information security, cybersecurity, and privacy protection — Information security management systems — Requirements)

- ISO/IEC 27002 (Information security, cybersecurity, and privacy protection — Information security controls)

- ISO/IEC 27701 (Privacy Information Management Systems)

- ISO/DIS 31700 on privacy by design for consumer goods and services can be used as a guide when designing a privacy framework.

8.4. ENGAGEMENT OF DATA PROCESSORS

Many entities within the communication sector 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 data is processed by vendors or service providers, entities in the telecommunication sector must remain aware of their ongoing responsibilities as data controllers. Controllers must demonstrate due diligence to establish the vendor's/ service provider's ability to protect personal data confidentiality.

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 obligations 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.

The Data Protection Act and related regulations specify 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 authorization from the controller. The contract must also outline the obligations of the processor to ensure staff confidentiality, assist the controller in meeting its obligations under the Act, and delete or return personal data at the end of the contract. 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 1:

Data Controller (DC): A telecommunications company that offers various services including internet and mobile network.

Many entities within the telecommunication sector 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 data is with the relevant security measures.

In the telecommunications sector, a data controller may enter into a contract with a data processor to manage customer data such as call records, location data, and internet usage. The contract should specify the purpose of data processing, the types of personal data involved, the duration of processing, and the security measures to be implemented to safeguard data. It should also outline the processor's obligation to report data breaches and the deletion or return of data at the end of the contract. Additionally, the contract may include provisions for auditing and inspection to ensure compliance with data protection regulations.

Example 2:

A broadcasting service company hires a third-party video hosting platform to store and manage its video content, which may contain personal data of viewers and users. As an obligation of data handlers, the broadcasting service company engages with the data processor to ensure that they process personal data in a lawful and transparent manner, such as through a data processing agreement that outlines the specific obligations of the data processor. The broadcasting service company may also conduct periodic audits and reviews of the data processor's practices to ensure compliance with data protection laws and regulations. Processor may also demonstrate compliance through maintaining ISO 27001 on Information Security Management System (ISMS) and ISO 27701 for privacy information management system (PIMS) By engaging with the data processor in this way, the broadcasting service company can fulfil its obligations to protect the personal data of its viewers and users, and ensure that they are processed lawfully and fairly.

8.5. LIMITATIONS ON DATA TRANSFERS

Most service providers are protected computer systems under the Computer Misuse and Cybercrimes Act, as they engage in the provision of services related to communications infrastructure. As part of compliance with data localization requirements, the service provider must process the data through a server and data centre located in Kenya or store at least one serving copy of the concerned personal data in a data centre located in Kenya.

Example 1

Mali Mali's management is considering moving its services to the cloud to improve on service delivery and cut on the operational costs. The company has to comply with the requirements of data localization in the Kenya Data Protection Act.

To achieve this, the company can use a cloud service provider that offers data centers located within its own country. The company can also negotiate a contract with the cloud service provider that includes specific requirements for data localization, such as a guarantee that all personal data will be stored within the country's borders or store at least one serving copy of the concerned customer data in a data centre located in Kenya.

8.6. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The carrying out of a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to the aforesaid, the Act requires that all data controllers and processors implement

appropriate technical and organisational measures and integrate appropriate safeguards to ensure the adequate protection of personal data of data subjects.

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

8.7. NOTIFICATION AND COMMUNICATION OF BREACH

Data Controllers have to report personal data breaches to the ODPC without delay within 72 hours of becoming aware of the breach while also notifying the affected data subjects. Where there has been unauthorised access, players within the telecommunication sector 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.

Entities are required to report data breaches to the Office and provide certain information about the breach. This information includes the date and circumstances in which the data breach was discovered, a chronological account of the steps taken after the breach was discovered, and details on how the breach occurred. Additionally, entities must provide the number of data subjects affected, the personal data or classes of personal data affected, and the potential harm to 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:

Mali Mali is the victim of a cyber-attack where unauthorized individuals gain access to the personal data of its customers. The company becomes aware of the breach during a routine security check and immediately launches an investigation. Upon realizing that the breach is a notifiable data breach, the company quickly notifies the Office of the Data Protection Commissioner, providing a detailed account of the breach, the steps taken to mitigate harm, and the potential harm to affected individuals. The company also informs its customers about the breach, advises them on how to eliminate or mitigate potential harm, and offers free credit monitoring services. The company conducts a review of its security measures and implements additional measures to prevent future breaches.

The 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.

ANNEX A: OTHER APPLICABLE LAWS AND REGULATIONS

The Kenya Information and Communications Act (KICA) 1998 (as amended) established the Communications Authority of Kenya (CA), which is responsible for regulating and licensing telecommunications service providers in the country. The same has subsequently been amended to provide for the regulation of converged communications services, including voice, data, and video services.

The Kenya Information and Communication (Registration of Sim-Cards) Regulations, 2015 provides for the process for registration of existing and new subscribers of service providers in Kenya.

The Postal Corporation Act provide for the establishment of the Postal Corporation of Kenya, to provide for its powers and functions, and for connected purposes.

Films and Stage Play Act Cap provide for controlling the making and exhibition of cinematograph films, for the licensing of stage plays, theatres and cinemas; and for purposes incidental thereto and connected therewith.

The Kenya Information and Communications (Consumer Protection) Regulations 2010 provide for the protection of consumers of telecommunications services, including the rights of consumers to information, privacy, anonymized data and complaint resolution.

The Computer Misuse and Cybercrime Act, No. 5 of 2018 protects the confidentiality, integrity and availability of computer systems, programs and data and protects the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution.

ANNEX B: 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
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.	In Communication Sector, we process sensitive data, 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.	We do not do anything generally unlawful with the personal data or inconsistent purpose for processing.			
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 fulfill 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.			
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.			