



OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes for the Transport Sector

2026

TABLE OF CONTENTS

FOREWARD.....	6
1.0 Introduction	7
<i>1.1 Background.....</i>	<i>7</i>
<i>1.2 Privacy Concerns</i>	<i>7</i>
<i>1.3 Scope and Purpose of Guidance Note</i>	<i>8</i>
2.0 Legislative Framework	9
3.0 Principles of Data Protection.....	10
<i>Lawfulness, Fairness and Transparency.....</i>	<i>10</i>
<i>Purpose Limitation.....</i>	<i>10</i>
<i>Data Minimisation.....</i>	<i>11</i>
<i>Accuracy.....</i>	<i>11</i>
<i>Storage Limitation</i>	<i>12</i>
<i>Integrity and Confidentiality</i>	<i>12</i>
<i>Accountability</i>	<i>13</i>
4.0 Relevant Lawful Bases for Transport Service Providers	14
<i>Consent.....</i>	<i>14</i>
<i>Performance of a Contract</i>	<i>14</i>
<i>Legal Obligation</i>	<i>15</i>
<i>Vital Interest.....</i>	<i>15</i>
<i>Public Authority.....</i>	<i>16</i>
<i>Legitimate Interests.....</i>	<i>16</i>
<i>Historical, Statistical, Journalistic, Literature and Art, or Scientific Research.....</i>	<i>16</i>
5.0 Compliance Obligations.....	18
<i>5.1 Registration and Collaboration with ODPC.....</i>	<i>18</i>
<i>5.2 Data Protection Governance Policies.....</i>	<i>19</i>
<i>5.3 Data Mapping/Record of Processing Activity (ROPA)</i>	<i>19</i>

<i>5.4 Privacy by Design and Default.....</i>	<i>23</i>
<i>5.5 Notification and Communication of Data Breach</i>	<i>24</i>
<i>5.6 Data Protection Impact Assessment (DPIA).....</i>	<i>24</i>
<i>5.7 Engagement of data processors</i>	<i>25</i>
<i>5.8 Cross-Border Data Transfer Considerations for Transport Operators.....</i>	<i>25</i>
<i>5.9 Data Sharing.....</i>	<i>26</i>
<i>5.10 Use of Personal Data for Commercial Purposes (Marketing)</i>	<i>27</i>
6.0 Rights of Data Subjects	29
7.0 Consequences of Non-Compliance with the Data Protection Act	31
8.0 Annexes.....	32
<i>8.1 Annex 1: Compliance Checklist.....</i>	<i>32</i>

Definitions of terms

“Act” means the Data Protection Act, No 24. of 2019

“Air charters” are private flights that are hired for specific trips, allowing people or goods to travel on their own schedule instead of using regular airline services.

“Air Freighters” are airplanes designed or used specifically to carry goods instead of passengers.

“Data Subject” means an identified or identifiable natural person who is the subject of Personal Data.

“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 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.

“Establishment documents” includes

- a statute, charter, or statutory instrument in which a body is established;
- registration certificate;
- trust deeds in which a trust has been established; and
- other instruments by which a body is established, including its governing and administrative structure.

“Non-exempt mandatory registration Entities” means data controllers and data processors that are required to register with the Office regardless of their annual turnover or number of employees, by virtue of processing personal data for any of the purposes listed in the Third Schedule to the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

“Logistics” is the process of planning and moving goods or resources from one place to another, so they arrive where they are needed, on time and in good condition.

“Protected Computer System” has the meaning assigned to it under section 20(2) of the Computer Misuse and Cybercrimes Act, 2018, and includes a computer system used directly in connection with, or necessary for 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.

“Public Transport” is a shared system that moves people, goods, and services between different places through organised routes and schedules.

“Transport” is the movement of people, goods, or animals from one place to another using any means, such as roads, rail, air, or water.

“Transport service provider” any person or entity, whether public or private, that offers or facilitates the movement of passengers, goods, or cargo by road, rail, air, water, or any other mode of transport, and includes operators, intermediaries, and digital platforms that collect, process, or manage personal data in the course of providing such services.

FOREWARD

The protection of personal data is a constitutional right guaranteed under Article 31 of the Constitution of Kenya, 2010, and remains fundamental to building trust in digital public services and the broader digital economy. As Kenya advances its digital transformation agenda, including initiatives under the Digital Superhighway and the Bottom-Up Economic Transformation Agenda (BETA), the safeguarding of personal information is both a legal obligation and a critical public responsibility.

The Office of the Data Protection Commissioner, established under the Data Protection Act 2019, is mandated to regulate the processing of personal data and ensure compliance across both public and private sectors. Within the transport sector, encompassing agencies responsible for road, rail, maritime, and aviation services, significant volumes of personal data are processed in delivering essential services such as licensing, registration, traffic management, logistics, and safety regulation. This places the sector at the forefront of ensuring adherence to data protection principles and standards.

This Guidance Note has been tailored to support the transport ecosystem by providing clear and practical direction on their obligations under the Data Protection Act, 2019, and its Regulations. It outlines key principles, lawful bases for processing, data subject rights, and institutional responsibilities, taking into account the specific data protection risks inherent in transport systems and operations.

By implementing the provisions of this Guidance Note, institutions within the sector will enhance compliance, strengthen public trust, improve service delivery, and reduce risks associated with the misuse or mishandling of personal data. The Office remains committed to supporting all sector actors through capacity building, stakeholder engagement, and, where necessary, enforcement.

It is my expectation that this Guidance Note will serve as a key reference for integrating data protection into policies, systems, and day-to-day operations across the transport sector. In doing so, we collectively safeguard the dignity and rights of Kenyans while advancing Kenya's vision of a trusted and inclusive digital economy.



Immaculate Kassait, SC, MBS
DATA COMMISSIONER
30th June 2026

1.0 INTRODUCTION

1.1 Background

The transport sector is a diverse ecosystem encompassing road, rail, air, and maritime services, all of which play a vital role in enabling mobility, facilitating trade, and supporting national development. As transport operations increasingly adopt digital tools, such as electronic ticketing, mobile applications, GPS tracking, fleet management systems, and digital payment platforms, operators now process growing volumes of personal data relating to passengers, drivers, employees, and other stakeholders.

Under the Data Protection Act and its Regulations, transport service providers, whether operating as private providers, SACCOs, authorities, or government agencies, act as data controllers and/or data processors and are therefore required to implement lawful, transparent, and secure data handling practices. As digital transformation accelerates across the transport sector, strong data protection governance has become essential to safeguarding personal data and maintaining public trust.

This sector-specific Guidance Note has, therefore, been developed to provide practical guidance on the interpretation of data protection requirements for transport operators, promote responsible personal data processing, and strengthen transparency, accountability, and safety in the delivery of transport services.

1.2 Privacy Concerns

The nature of personal data processing in the transport sector raises significant privacy concerns, including the potential misuse of passenger, driver, and client data, as well as a lack of transparency on the collection, sharing, and retention of such information. Consequently, there is need for transport operators to ensure that personal data processed during the provision of mobility, logistics, and related services is handled lawfully, fairly and transparently, with appropriate safeguards in place to protect it from unauthorised access, disclosure, or loss.

The following are some of the privacy risks that affect the transport services sector:

- a) **Profiling of Users:** Profiling riders, drivers, and passengers, processing their sensitive personal data for marketing purposes, poses risks of unlawful processing, discrimination, and loss of privacy.
- b) **Unauthorised harvesting of personal data:** A malicious actor may exploit security vulnerabilities in a transport service provider's platform to collect drivers' personal data at scale. For instance, ride-hailing systems that disclose driver information to passengers before the ride starts; a practice necessary for safety, may be exploited if adequate technical safeguards are not implemented.
- c) **Location tracking:** Transport service providers can track, in real time or offline, riders' precise locations during their rides. Compared with other forms of transportation, ride-hailing systems can reveal personal data about data subject.
- d) **Lack of transparency in data processing:** Many transport service providers and digital mobility platforms do not adequately inform users about how their personal data is collected, processed, shared, or stored. This lack of transparency reduces user trust and

may prevent individuals from making informed decisions or exercising their data subjects' rights effectively.

- e) **Cybersecurity and data breaches:** The transport service providers' increasing reliance on digital platforms and online payment systems exposes them to cybersecurity threats. Data breaches resulting from inadequate security controls, weak authentication, or system vulnerabilities may lead to unauthorised access to sensitive personal or financial information, causing identity theft, fraud, or reputational harm.
- f) **Unauthorised sharing of personal data:** Personal data collected for transport or logistics purposes may be repurposed or shared with third parties such as advertisers, analytics providers, or technology partners, without the knowledge or consent of data subjects. Such misuse undermines the principles of purpose limitation and lawfulness of processing, potentially leading to profiling, targeted advertising, or discrimination.
- g) **Surveillance and monitoring technologies:** The deployment of surveillance tools, including CCTV, dashboard cameras, and vehicle tracking systems, can enhance safety and security but may also result in excessive monitoring if not properly regulated. Without clear policies on data access, retention, and use, such technologies may infringe data subjects' rights and contribute to a sense of constant surveillance.
- h) **Inadequate Data Subjects Rights Handling Mechanisms:** Many transport services providers lack proper mechanisms and procedures to enable data subjects to exercise their rights to access, correct or delete their personal data. This can result in the breach of data subjects' rights.
- i) **Data Misuse for Marketing and Analytics:** Data collected for service delivery may be reused for advertising, insurance scoring, or other secondary purposes without complying with the principles of data protection in section 25 of the Data Protection Act.
- j) **Risk of Non-Compliance with Mandatory Registration Requirements:** Transport operators have a mandatory obligation to register with the ODPC. Failure to comply with this and other obligations may lead to enforcement measures by the Office.

1.3 Scope and Purpose of Guidance Note

The purpose of this guidance note is to provide data handlers in the transport sector with a clear understanding of their obligations under the Data Protection Act and its Regulations. The guidance note seeks to address the various aspects of data protection relevant to the transport industry, including the collection, use, retention, disclosure, and disposal of personal data processed within the sector.

This guidance has been developed to support transport operators, including public transport providers, private bus and matatu companies, matatu SACCOs, freight and logistics providers, taxi-hailing and ride-hailing platforms, rail operators, aviation service providers, and maritime operators, in ensuring legal compliance, upholding privacy rights, and mitigating the risks associated with the processing of personal data.

It outlines the specific considerations and best practices necessary for safeguarding personal data within the transport sector, and it applies to all modes of transport and should be regarded as a minimum standard.

2.0 LEGISLATIVE FRAMEWORK

The transport service operators in Kenya are governed by several legislative frameworks, including but not limited to:

Constitution of Kenya 2010; Article 31 (c) and (d) guarantee individuals the right to privacy concerning information related to their family or private affairs that is unnecessarily required or disclosed, as well as protection against infringement of their communications.

Data Protection Act (2019); The Data Protection Act, No. 24 of 2019, establishes the Office of the Data Protection Commissioner and provides various frameworks that guide the processing of personal data in Kenya. The attendant regulations to the Data Protection Act, 2019 include the *Data Protection (General) Regulations 2021*, *Data Protection (Complaints and Enforcement) Regulations 2021*, and *Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021*. These regulations outline how personal data should be handled in Kenya, emphasising data protection principles, lawful basis, consent, data subject rights, etc. They also set duties for data controllers and processors, including **mandatory registration** with the ODPC, and outline the procedure for handling complaints that relate to violations of data subject rights.

The Computer Misuse and Cyber Crime Act, 2018. This Act provides for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation, and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters, and for connected purposes.

Traffic Act (Cap 403) and National Transport and Safety Authority (NTSA) Act, 2012. These Acts regulate transport operations and related data systems, including licensing, enforcement, oversight of road transport systems, and ensuring safe, reliable, efficient land-transport operations.

The Civil Aviation Act (Cap 394) This Act provides for the control, regulation, and orderly development of civil aviation in Kenya.

Kenya Railways Corporation Act (Cap 397)– This Act sets up the Corporation which is responsible for the construction, maintenance, and operation of rail infrastructure.

Merchant Shipping Act (Cap 389) - Provides the legal framework for maritime safety, shipping operations, port management, and the regulation of vessels within Kenyan waters.

Integrated National Transport Policy 2024 - provides the overarching strategic and policy direction for the entire transport system: road, rail, aviation, and maritime.

International and regional legal frameworks - the guidance note also considers applicable international and regional legal frameworks and global best practices that regulate international transport operators who process Kenyan personal data.

3.0 PRINCIPLES OF DATA PROTECTION

Lawfulness, Fairness and Transparency

Personal data must be collected and used in a lawful, fair, and transparent manner. The essence of this principle is to ensure the legality of processing activities, the fair use of personal data collected from data subjects, and transparency on the part of data controllers and processors towards their data subjects.

Practical Compliance Steps	
Lawfulness	• Register with the ODPC as data controller, processor or both depending on processing activities. • Establish a relevant lawful basis for the processing of personal data. • Use personal data legally and not for criminal purposes or malicious reasons. • Comply with other transport industry laws on handling of personal data
Fairness	• Use personal data in a manner that maintains the dignity of the data subject and ensures processing is fair, free from prejudice or exploitation, and is consistent with applicable legal and constitutional safeguards. • Use personal data only in ways that the data subject would reasonably expect, given the purpose for which it was collected.
Transparency	• Inform all data subjects (may include drivers, pilots, passengers, etc.) of their rights. • Provide clear information on the use of personal data in plain language that data subjects can easily understand, avoiding complex legal terminology. • Ensure transparency in algorithmic decision-making processes, such as driver ratings or automated trip deactivations, by providing full disclosure of personal data use that is necessary for data subjects to make informed decisions or contest outcomes

Purpose Limitation

Personal data must be used only for the specific purpose for which it was collected. If data was collected for one purpose, it cannot be used for a different purpose without a valid legal basis or the data subject's consent. Transport service providers collect personal data for various operational reasons, including booking trips, processing payments, monitoring safety, and handling customer complaints. This personal data must not be used for unrelated

purposes, such as targeted marketing or third-party analytics, without the data subject's knowledge.

Practical Compliance Steps

- Do not use personal data for any purpose beyond what was originally disclosed to the data subject. Where you wish to use data for a new or different purpose, assess whether a valid lawful basis exists for that new use.
- Notify data subjects promptly and prior to commencing such processing, whenever their personal data is intended to be used for a purpose different from the one originally stated. Where a new lawful basis cannot be identified, such processing must not proceed.

Data Minimisation

Transport service providers should collect only the personal data necessary to deliver their services or meet legal obligations. Collecting excessive data beyond what is required is contrary to the principle of data minimisation.

Practical Compliance Steps

- Limit app permissions and trackers to what is strictly necessary.
- Regularly review your personal data collection forms, app permissions, trackers, and onboarding procedures to remove unnecessary fields.

Accuracy

Personal data must be accurate, current, and reliable; therefore, transport service providers shall establish a simplified internal procedure for data subjects to submit rectification requests and take reasonable steps to correct or delete any inaccurate personal data in compliance with the Data Protection Act.

Practical Compliance Steps

- Verify personal data at the point of collection to ensure it is correct.
- Periodically review and update personal data to keep it relevant and accurate
- Promptly correct or delete any data found to be inaccurate or outdated.

Storage Limitation

Personal data must not be kept longer than necessary. Under Section 25(g) of the Data Protection Act, 2019, transport service operators must ensure that personal data is deleted or anonymised once it is no longer needed.

Practical Compliance Steps

- Develop a data retention policy that sets clear retention periods for each category of personal data.
- Regularly audit the personal data your organisation collects to identify and delete information that is no longer necessary.
- Inform data subjects of how long their data will be retained.
- Where a transport service provider is unable to delete/destroy, either digital or physical records, due to internal policies or obligations, they should classify and anonymise/archive them.

Integrity and Confidentiality

Personal data must be kept secure. Transport service providers must protect personal data against unauthorised access, accidental loss, destruction, or damage. Operations in the transport sector require managing large volumes of sensitive personal data, including passenger details, trip records, driver/pilot information, and payment data, making security a critical requirement.

Practical Compliance Steps

- Implement appropriate technical measures such as encryption, firewalls, and secure login protocols to protect personal data.
- Restrict access to personal data to only those staff members who need it to perform their duties.
- Ensure that third parties and service providers who handle personal data on your behalf maintain adequate security standards.
- Establish procedures for detecting, reporting, and responding to data breaches promptly.
- Regularly train staff on data security practices and their obligations under the Data Protection Act, 2019.
- Conduct periodic security assessments to identify and address vulnerabilities in your systems.
- Maintain secure disposal procedures for personal data that is no longer needed.

Accountability

Transport service providers are responsible for complying with the Data Protection Act, 2019 and must be able to demonstrate compliance at any time. It is not enough to simply follow the law; Providers must actively show how they are doing so.

Practical Compliance Steps

- Maintain an up-to-date data map that documents what personal data you collect, why, how long you keep it, and lawful bases relied on for processing.
- Keep records of all consent obtained from data subjects, including when, how, and what they consented to.
- Document all Data Protection Impact Assessments (DPIAs) conducted, including the risks identified and the measures taken to address them.
- Retain records of all staff for data protection training, including dates, attendees, and topics covered.
- Keep copies of all data processing agreements signed with third-party service providers.
- Maintain a data breach register recording all incidents, their nature, impact, and the steps taken in response.
- Document all data subject requests received and how they were handled, including timelines for response.
- Keep records of all internal data protection audits, findings, and corrective actions taken.
- Retain copies of privacy notices and records of any updates made to them over time.
- Document decisions made during the design of new systems or products to show that data protection was considered from the outset.
- Maintain records of data retention and disposal, evidencing that personal data was deleted in accordance with your retention policy.

4.0 RELEVANT LAWFUL BASES FOR TRANSPORT SERVICE PROVIDERS

In accordance with Section 30 of the Data Protection Act, transport service providers must identify at least one legal ground before processing any personal data. Personal data shall not be processed unless it falls under one of the following eight bases:

Consent

In the context of the transport sector, consent can only be a valid lawful basis if the data subject is offered a genuine choice concerning accepting or declining the terms offered. If a passenger faces negative consequences for declining, the consent is not considered "freely given".

Children cannot validly give consent to the processing of their personal data. In such cases, consent must be obtained from their parents or legal guardians. Transport service providers must implement reasonable age-verification mechanisms where their services are likely to be accessed by children.

Transport service providers must therefore ensure that they obtain valid consent that is specific, informed, and freely given.

- 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 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.

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

Performance of a Contract

This lawful basis can be relied on when processing personal data to fulfil contractual obligations and in the transport sector, it may arise in several situations, such as:

- i. Onboarding and operator engagement contracts.
- ii. Provision of transport services contracts: For example, using personal details to facilitate a trip.
- iii. Employment contracts: Managing staff contracts and payrolls.
- iv. Ticketing agency contracts involve processing client details for ticketing or travel schedules.
- v. Travel advisory contracts: Processing client details for travel schedules and preferences.

The data processed must be directly necessary to deliver the service or fulfill the contract.

Legal Obligation

Transport operators may rely on legal obligation as a lawful basis for processing personal data where they can demonstrate that the processing is necessary for compliance with a statute. However, the processing must not go beyond what is strictly required to fulfil that obligation.

Example: Under Regulation 14(6) of the National Transport & Safety Authority (Transport Network Companies Owner, Drivers and Passengers) Regulations, 2022, transport networks are required to protect and process all personal data obtained from drivers and passengers in compliance with the provisions of the Data Protection Act.

Vital Interest

This basis is reserved for emergency "life-or-death" scenarios where the individual cannot give consent. Such processing will need to be documented and justification provided.

Example: Following a serious road accident, a transport service provider may share passenger identity or next-of-kin details with medical emergency teams to save a life.

Public Interest

Public interest can be a lawful basis for the processing of personal data in the transport sector if the processing is necessary for the performance of a task carried out in the public interest in the exercise of official authority vested in the transport sector.

Public interest may arise from various sources, such as:

- i. Government mandates: transport service providers may be required by the government to collect and report data related to their customers, operators and staff for statistical purposes, policy making, and public accountability.
- ii. Public safety: transport service providers may need to process personal data to ensure the safety and security of their customers, operators and staff, such as using CCTV cameras and background checks

Example: County Government M relies on public interest as the lawful basis for processing personal data when installing traffic surveillance cameras along major roads. These cameras are used to monitor traffic flow, detect congestion, enforce traffic rules, and identify incidents such as accidents, stalled vehicles, or reckless driving.

Public Authority

This lawful basis applies to mandates of public institutions established under Kenyan legislation, as well as the performance of specific functions and powers provided for under such laws.

Example: NTSA collects and uses personal data such as driver details, vehicle registration details of individuals, etc. to carry out its specific regulatory and enforcement functions under the Traffic Act and NTSA Act.

Legitimate Interests

Legitimate interest can be relied on as a lawful basis for processing personal data in the transport sector if the processing is for valid transport service provider's interests/purposes (e.g., system security or business analytics), provided these do not override the data subject's rights. Before relying on this basis, transport service providers should assess whether the legitimate interest is an appropriate lawful basis. In doing so they should consider:

- i. Purpose Test: identifying the nature of the legitimate interest pursued and explaining why the processing is necessary to achieve it.
- ii. Necessity Test – demonstrating that the processing is proportionate, cannot reasonably be achieved through less intrusive means, and is essential to the stated interest.
- iii. Balancing Test – assessing whether the data subject's rights, freedoms, and expectations override the identified interest, taking into account the type of data, safeguards applied, and any risks associated with the destination jurisdiction.

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

When relying on this lawful basis, personal data must be aggregated and anonymised. Historical, statistical, journalistic, literature and art or scientific research may be conducted by transport service providers for various purposes, such as:

- i. Transport research: transport service providers may process personal data for research purposes to improve the quality of transport services and contribute to the betterment of access to and efficiency of transport services.
- ii. Historical research: Transport service providers may process personal data for historical research purposes to document and preserve the history of the industry and its consumers.
- iii. Scientific research: transport services may process personal data for scientific research purposes to study human behavior topics, especially as it relates to consumption of transport services.
- iv. Statistical research: This is mostly possible through the quantitative research projects conducted to provide statistics of given facts.

Example: Otokaa riding app partners with a popular university to study the correlation between ride-hailing usage and road accident rates in urban areas, processing anonymised trip data spanning three years. Rather than relying on consent or contractual necessity, Otokaa processes this data on the lawful basis of historical, statistical and scientific research under Section 30 of the Data Protection Act, 2019, which permits processing of personal data beyond its original collection purpose where it is conducted in the public interest, the data is anonymised and appropriate safeguards against re-identification are in place.

5.0 COMPLIANCE OBLIGATIONS

Transport service providers should ensure that personal data is handled responsibly and in accordance with the law. The Data Protection Act sets out clear obligations for all data controllers and data processors, including transport service providers. These obligations cover every stage of the data lifecycle, from the moment personal data is collected to its storage, use, sharing, and eventual deletion. Meeting these obligations is an opportunity for transport service providers to build trust with their customers, protect the rights of passengers and drivers, and demonstrate a genuine commitment to responsible data handling. Transport service providers are encouraged to view compliance not as a burden, but as a foundation for better business practices.

5.1 Registration and Collaboration with ODPC

a. Registration

Transport service providers process personal data as part of their operations and should register with the ODPC as a data controller, data processor, or both, depending on their processing activities. Registration for transport service providers is mandatory as per the General Regulations. At the time of registration, Data Controllers and Data Processors must provide details of the categories of personal data being processed, the purposes for which the data is processed, and the security measures in place to protect it. Where a controller procures the services of a third-party vendor (processor), it shall, as part of its vendor due diligence process, confirm the registration status of potential third-party vendors. Registration alone is not sufficient; transport operators must also comply with other obligations. "

The Office has published a Guidance Note on Registration on www.odpc.go.ke. Please refer to this guidance note for more details on registration of controllers and processors.

b. Collaboration with ODPC and Appointment of Data Protection Officer

Transport service providers are also required to collaborate with the Office in providing requested information and may appoint or designate a Data Protection Officer (DPO) to act as a liaison. The DPO is responsible for overseeing data protection compliance, advising management and staff on their obligations under the Data Protection Act, and serving as the primary point of contact with the ODPC. The DPO must have relevant expertise in data protection and must be allowed to perform their duties independently. Transport service providers are encouraged to engage proactively with the ODPC and utilise the resources published to assist them in understanding and meeting their obligations under the Data Protection Act. These are freely available on the ODPC website at www.odpc.go.ke.

Example

A national bus company operating across multiple counties processes the personal data of thousands of passengers daily, including booking records, national ID numbers, and

payment information. Given the scale of its operations, the company may appoint or designate a DPO. The appointed/designated DPO develops the company's data protection policy, trains staff on compliance obligations, conducts internal audits, and liaises with the ODPC on regulatory matters.

5.2 Data Protection Governance Policies

These are fundamental documents (including standard operating procedures) that set out how transport service providers collect, use, store, and protect personal data during their operations. Every transport service provider, regardless of size, is expected to have formal procedures for the practical implementation of the Data Protection Act's requirements, tailored to the specific nature of their operations. There should be clearly defined staff roles and responsibilities for handling personal data, established internal procedures for responding to data subject requests and data breaches, and set out standards that all employees and third-party service providers are expected to meet.

The policies and procedures must not be static. Transport operators are required to develop a policy review procedure to regularly review and update their policies in line with changes in the law, new technologies, or business operations. For example, when a transport operator introduces a new mobile application, integrates a third-party payment system, or expands its operations to new countries, the policies must be updated accordingly. Staff must be informed of any updates and trained in the revised requirements.

The policies can include data protection policy, retention schedule and policy, ICT policy, access control policy, vendor management policy, incident response and management policy, etc.

5.3 Data Mapping/Record of Processing Activity (ROPA)

Data mapping is the process of identifying and documenting how personal data flows through your organisation, from the point of collection through to storage, use, and disposal. It also gives the purposes of processing and the lawful bases relied upon. It gives transport service providers a clear picture of their data processing activities and is a key tool for demonstrating compliance.

Why Data Mapping Matters:

- Helps you understand what personal data you hold and where it is stored.
- It identifies who has access to personal data in your organisation.
- Reveals how personal data is shared with third parties or transferred across borders.
- Supports risk assessments and Data Protection Impact Assessments (DPIAs).
- It guides identification and implementation of technical and organisational safeguards to protect personal data
- Enables you to respond efficiently to data subject requests such as access, correction, or deletion.
- Serves as evidence of compliance during regulatory audits.

Transport operators are expected to keep records of their personal data processing activities (RoPA), in line with their accountability obligations under the Data Protection Act and Regulations.

This may be done through a data map or similar accountability record, which should ideally follow the steps set out below.

How to Conduct Data Mapping	
1.	Identify your data: Document the categories of personal data your organisation collects, such as passenger details, driver records, payment information, and trip data.
2.	Identify your data sources: Record where the data comes from, for example, customers, employees, third-party platforms, or government agencies.
3.	Identify data categories and purposes: Identify the type of data processed and a clear purpose for each processing
4.	Map the data flow: Track how data moves through your organisation, who handles it, and whether it is shared with or transferred to third parties.
5.	Identify risks: Assess potential vulnerabilities or gaps in your data handling practices and take steps to address them.
6.	Identify retention periods: Document how long each category of personal data is kept and when it is due for deletion or anonymisation in line with your retention policy.
6.	Identify the lawful basis: For each processing activity, confirm and document the lawful basis under the Data Protection Act, 2019 that justifies the processing.
7.	Identify third-party processors: List all external service providers who handle personal data on your behalf, such as payment processors, cloud storage providers, and GPS tracking vendors, and confirm that data processing agreements are in place.
8.	Assess cross-border transfers: Identify any personal data that is transferred outside Kenya and confirm that appropriate safeguards are in place to protect it.

9. Review and update regularly: Data mapping is not a one-time exercise. Review and update your data map whenever there are changes to your systems, processes, or business operations to ensure it remains accurate and up to date.

Example: Bahari Bus Company Data Mapping & RoPA

Bahari Bus Company, a long-distance bus operator, conducts a data mapping exercise to understand and document all personal data it processes.

Identification of data: Bahari Bus identifies the following categories of personal data it collects:

- Passenger names, phone numbers, and national ID numbers collected during ticket booking.
- Payment details collected through mobile money and card transactions.
- Driver names, license numbers, and employment records.
- Trip records including departure points, destinations, and travel times.
- CCTV footage captured at bus terminals and on-board buses.

Identification of data sources:

- Passengers booking tickets online, at the counter, or through the mobile app.
- Drivers during the onboarding and employment process.
- Third-party payment processors handling mobile money and card transactions.
- CCTV cameras installed at terminals and on buses.

Map the data flow:

- Passenger booking data is captured on the company's ticketing system and shared with the payment processor to complete transactions.
- Driver records are stored in the HR system and accessed by the operations and fleet management teams.
- Trip records are automatically generated by the GPS tracking system and accessed by the operations team.
- CCTV footage is stored on a local server at each terminal and accessible only to the security team.

Identify the lawful basis e.g.

- Passenger booking data, performance of a contract.
- Driver employment records, legal obligation and performance of a contract.
- CCTV footage, legitimate interest for safety and security purposes.

Identify retention periods:

- Passenger booking records, 12 months after travel date.
- Driver employment records, 5 years after the end of employment.
- Payment records, 7 years in line with tax obligations.
- CCTV footage, 30 days, after which it is automatically overwritten.

Identify third-party processors:

- M-Pesa and card payment processors handling passenger payments.
- GPS tracking vendor managing fleet location data.
- Cloud storage provider hosting the ticketing system.

Identify risks:

- CCTV footage stored on local servers without encryption, and risk of unauthorised access.
- Passenger national ID numbers retained beyond the period necessary, risk of excessive data retention.

No data processing agreement in place with the GPS tracking vendor, risk of non-compliant data processing.

Example Record of Processing Activity (RoPA) Extract - Bahari Bus Company

Processing Activity	Data Categories	Data Subjects	Purpose	Lawful Basis	Third Parties	Retention Period
Ticket Booking	Name, phone number, national ID	Passengers	Trip facilitation	Contract	Payment processor	12 months
Payment Processing	Payment details	Passengers	Billing	Contract	M-Pesa, card processor	7 years
Driver Management	Name, license, employment records	Drivers	HR and operations	Contract, legal obligation	None	5 years
Fleet Tracking	Location data, trip records	Drivers	Safety and operations	Legitimate interests	GPS vendor	90 days

CCTV Surveillance	Video footage	Passengers, staff	Security	Legitimate interests	None	30 days
--------------------------	---------------	-------------------	----------	----------------------	------	---------

5.4 Privacy by Design and Default

Privacy by Design: Refers to integrating data protection and privacy features into the design and development of systems, products, and services from the outset. In the transport sector, this means ensuring that personal data protection is considered at every stage of data processing activities.

Privacy by Default: This principle ensures that, by default, only the personal data necessary for each specific purpose of the processing is collected, and it is not kept longer than necessary. For example, transportation apps should only request necessary personal information such as name, contact information, and payment details, without collecting unnecessary data.

Implementing Privacy by Design and Default:

- i. Make sure that you have a valid lawful basis for processing personal data, and that such processing is conducted transparently, strictly for the purpose for which the data was originally collected.
- ii. Carry out an assessment to ensure compliance with the principles of data protection, including lawfulness, transparency, purpose limitation, confidentiality, integrity and availability, data minimisation, accuracy, storage limitation, and fairness.
- iii. Conduct regular risk assessments to identify privacy risks early in the project lifecycle.
- ii. Minimise the amount of personal data collected.
- iii. Implement robust security controls (e.g., encryption, access restrictions) by default.
- iv. Train employees on data privacy principles and integrate them into business processes.

Example: A **ride-hailing app** that collects personal information (name, phone number, payment details) from users during registration implements privacy by design by:

Data minimization: Only asking for essential data (e.g., phone number, name) to use the service.

Data security: Ensuring all payment information is encrypted and securely stored.

Privacy by Default: Setting up the app so that no data is shared with third parties unless the user explicitly agrees to it (e.g., for promotional purposes).

Thus, the app ensures that personal data protection is built into the design, and only the minimum amount of data necessary is processed.

5.5 Notification and Communication of Data Breach

Transport service providers, acting as data controllers, must report data breaches to the Office within 72 hours of becoming aware of it. Where unauthorised access to personal data occurs, transport service providers must also notify affected individuals in writing, unless their identities cannot be established.

Data processors must notify the data controller within 48 hours of becoming aware of a personal data breach. This enables the data controller to investigate the incident, implement mitigation measures, and meet its statutory obligation to report the breach to the ODPC within the required timeframe.

Example

Motos, an online taxi hailing company, complies with the Data Protection Act by promptly detecting any data breach, taking immediate action to contain the incident, and notifying both the Data Commissioner and the affected data subjects within 72 hours and without undue delay, of becoming aware of the breach.

Within 72 hours, Motos submits a detailed incident report to the Office of the Data Protection Commissioner. This report explains how the breach occurred, the nature of the personal data affected, such as rider profiles, trip histories, driver details, payment information, and the corrective measures taken to secure the system.

Motos also takes steps to support affected individuals by guiding them on how they can protect themselves from potential harm. At the same time, the company works to strengthen its data security controls, improve internal processes, and maintain ongoing communication with riders and drivers to restore public trust in the platform's safety and reliability.

5.6 Data Protection Impact Assessment (DPIA)

DPIAs should be conducted before implementing projects with risks to the rights of data subjects to assist transport service providers in mitigation of those risks. Where processing is likely to result in a high risk to the rights and freedoms of data subjects, transport service providers must submit the DPIA to the ODPC for review 60 days before implementation.

Example:

A ride-hailing company plans to introduce a feature that records in-vehicle audio and video for safety and security, while linking trip history to passengers' profiles for personalised promotions. This involves high-risk processing of sensitive personal data, including recordings and behavioral patterns. Conducting a Data Protection Impact Assessment (DPIA) helps identify risks such as unauthorized access, misuse of recordings, or profiling biases, and implement safeguards like

restricted access, data encryption, limited retention periods, and obtaining explicit consent. This ensures compliance with the Data Protection Act, 2019 and protects passengers' privacy.

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.

5.7 Engagement of data processors

Transport service providers 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 engaging with a data processor, data controllers 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 the providers 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 Data Protection Act. This will help to ensure that personal data is handled securely and ethically, and that privacy is protected.

Example: A taxi company contracts a cloud-based fleet management service to track drivers and trips. They sign a written agreement detailing data protection obligations, require the provider to implement encryption and access controls, and ensure staff handling the data are trained in security measures. This ensures personal data is managed securely and in compliance with the Data Protection Act.

5.8 Cross-Border Data Transfer Considerations for Transport Operators

Transport operators increasingly operate across borders, whether through international courier services, cross-border bus routes, aviation, or partnerships with foreign technology platforms. Where personal data is transferred outside Kenya, transport operators must comply with the Data Protection Act, which set out the conditions under which personal data may lawfully be transferred to another country.

A transfer of personal data outside Kenya is only permitted where one of the following bases applies:

- **Appropriate Safeguards** – The country to which the transferring entity is sending the personal data has implemented adequate measures to protect it, or the transferring entity has other safeguards in place, such as binding corporate rules, legal instruments, and ratification of the Malabo Convention, etc.
- **Adequacy Decision** - The Data Commissioner has determined that the destination country provides an adequate level of data protection comparable to that required under Kenyan law.
- **Derogations**

- a. Transfer as a Necessity** – The transfer is necessary for the performance of a contract with the data subject, for the protection of the vital interests of the data subject, for a legal claim, or for other compelling legitimate reasons recognised under the Data Protection Act.
- b. Consent of the Data Subject** - The data subject has given explicit, informed consent to the transfer of their personal data to the specified country due to the lack of the other safeguards provided above.

What Transport Operators Must Do:

- Before transferring any personal data outside Kenya, identify and document the lawful basis for the transfer.
- If you rely on consent, make sure to clearly inform the data subject about the destination country, the purpose of the transfer, and any associated risks.
- Maintain records of all cross-border data transfers in your data map.
- Do not transfer personal data to a country with inadequate data protection standards without first putting appropriate safeguards in place.
- Engage your Data Protection Officer to assess and advise on proposed cross-border data transfers before they commence.

For more information on cross-border data transfers, the Office has published a Guidance Note on Cross-Border Data Transfers at www.odpc.go.ke, which provides a framework for responsible, ethical data transfer practices in line with the requirements of the Data Protection Act.

5.9 Data Sharing

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. Requests for sharing must be made in writing, specifying the purpose, retention period, and safeguards

Example: A taxi company shares customer trip data with a mapping service to improve route efficiency. They signed a data-sharing agreement specifying that only trip times and locations can be used; the data must be kept secure and cannot be used for marketing. The data is anonymised and sent over a secure connection, ensuring compliance with the Data Protection Regulations.

The Office has published a Data Sharing Code on www.odpc.go.ke to provide a framework for responsible and ethical data sharing practices in line with the requirements of the Data Protection Act.

5.10 Data Localisation

Data localisation is a requirement to domicile personal data for the strategic interest of the state in Kenya. Regulation 26 of the Data Protection (General) Regulations, 2021 requires that personal data prescribed by the Cabinet Secretary (ICT), as being of strategic interest, must have a copy domiciled in Kenya. Processing of personal data for the purpose of running any system described as a “protected computer system” in terms of Section 20 of the Computer Misuse and Cybercrime Act, 2018, is considered processing for the strategic interest of the state. Section 20 (2) (c) of the Computer Misuse and Cybercrimes Act, 2018 designates the provision of services related to public transportation as a protected computer system, which means that they need to comply with the data localisation provisions. That is:

- a) Process such personal data through a server and data centre located in Kenya; or
- b) Store at least one serving copy of the concerned personal data in a data centre located in Kenya.

Example:

Jamotokaa, a digital transport service provider operating in Kenya, stores its primary database on a cloud server hosted in Spain but maintains a live-serving copy of all personal data relating to Kenyan data subjects, including names, phone numbers, location data, payment information, and trip histories, on a local server on its own premises in Kenya. The two copies are continuously synchronised, with the local server handling real-time requests from Kenyan users, while the Spanish cloud server supports broader infrastructure needs. This dual-storage arrangement means that at any given moment, a complete and current copy of Kenyan user data exists within the country's borders, accessible without routing requests through foreign jurisdictions or relying on international data retrieval mechanisms.

5.10 Use of Personal Data for Commercial Purposes (Marketing)

Personal data is considered as being processed for commercial purposes when it advances commercial or economic interests. This includes use of personal data for:

- Sending marketing materials - sending a catalogue through any medium (by email, post, or any other medium) directly to a person using their personal information.
- Showing targeted advertisements online - displaying an advertisement on an online media site where a data subject is logged on using their personal data;
- Sending promotional messages - sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

Conditions for using personal data for commercial purposes

A firm may only use personal data for commercial purposes if:

- *Obtained an express consent* – the firm has clearly asked the person (data subject) for permission, and they have agreed to their data being used for commercial purposes. When administering consent, the firm must clearly tell the data subject that it will be used for direct marketing purposes.
- *The firm is allowed by law* - a written law gives the firm the authority to use the data for a specific commercial purpose. The person whose data is collected must be informed about this use at the time their information is collected.
- *There is a simple way to opt out* - Where consent is the lawful basis for the processing, the company must provide an easy, visible, and free way for the data subject to stop receiving marketing messages at any time (e.g., an “Unsubscribe” link or replying “STOP” to an SMS).

Example:

XYZ Transport Company Ltd operates an app that allows customers to book boda, matatus, and taxi rides. When signing up, customers are required to provide their name, phone number, and email address.

The firm has decided to use customer information to promote its new parcel delivery service. They plan to send SMS messages like:

"Hi Customer! The firm now offers door-to-door parcel delivery across Nairobi. Try it today and get 10% off your first delivery!"

This is considered a commercial use of personal data because the firm is using the data to promote its own paid service and encourage customers to use it.

Opt-Out Mechanism

Transport service providers must ensure that data subjects can opt out of receiving marketing communications or the use of their personal data for promotional purposes.

The opt-out process should:

- be easy to find and understand, with clear and simple instructions;
- be quick and straightforward, without unnecessary steps or lengthy forms;
- provide simple options such as an “Unsubscribe” link, replying “STOP” to an SMS, or contacting customer care;
- be free of charge;
- be accessible to all users, including persons with disabilities; and
- be acted upon promptly, so that personal data is no longer used for direct marketing once a data subject opts out.

6.0 RIGHTS OF DATA SUBJECTS

Data subject rights management is crucial for entities operating in the transport sector. In this context, data subjects in the transport sector may include, but are not limited to, employees, passengers or riders, drivers, and delivery partners. The Data Protection Act provides data subjects with enforceable rights in relation to the processing of their personal data. To ensure compliance, transport service providers must establish clear and documented procedures to enable the exercise of these rights, including defined timelines for responding to such requests. Transport service providers should also implement processes for receiving, tracking, and responding to data subject requests. This may include the use of standardised Data Subject Request (DSR) forms and internal registers to document and monitor requests among other mechanisms.

The Data Protection Act provides the following rights to data subjects. Some are absolute, meaning that they are mandatory, and others are conditional depending on different organisational policies or statutory requirements:

Right	What it means	Responsibilities of Transport Service Providers	Nature of right	Timeline
Right to be Informed	Data subjects must know how their personal data is collected, used, shared, and retained	Provide clear and accessible privacy notices at the point of data collection, including purpose, sharing, retention, and contact details for complaints	Absolute	At or before collection, and at any point during the processing lifecycle
Right of Access	Data subjects can request a copy of their personal data	Provide access upon request (email, app, or written), verify identity, and supply a copy of the data where needed	Absolute	Within 7 days
Right to Rectification	Data subjects can correct inaccurate or incomplete data	Update or correct personal data upon request and verify supporting information where necessary	Absolute <i>(with verification where necessary)</i>	Within 14 days
Right to Object	Data subjects can object to the processing of their data, particularly for	Act on opt-out requests (via email, app, or written request); cease processing for direct marketing immediately; assess objections where	Conditional <i>(Absolute for direct marketing)</i>	<i>Without undue delay (immediate effect for direct marketing)</i>

	direct marketing purposes	processing is based on other lawful grounds		
Right not to be subject to Automated Decision-Making	Data subjects can challenge decisions made solely by automated systems	Provide an option for human review and reconsideration upon request, unless processing is based on consent, contract, or authorised by law	Conditional	As soon as reasonably practicable
Right to Erasure	Data subjects can request the deletion of their personal data	Delete personal data where it is no longer necessary, unlawfully processed, or where consent is withdrawn	Conditional	Without undue delay
Right to Data Portability	Data subjects can receive their data in a usable format	Provide personal data in a structured, commonly used, and machine-readable format, and where applicable, facilitate its transfer to another data controller	Conditional	Within 30 Days, and where requests are complex or numerous, the timeline may be extended with consultation with the Data Commissioner

Complaints Handling Mechanism

Transport service providers must offer clear and accessible ways for data subjects, including employees (e.g., drivers) and customers, to lodge complaints about the handling of their personal data. Data subjects should be able to report any violations of their rights and other breaches of the Data Protection Act.

Providers should establish a simple internal complaint-handling process that is easy to access through channels such as email, mobile applications, websites, or physical offices. The process should clearly set out how complaints are received, reviewed, and resolved, and providers should communicate progress and outcomes to the complainant in a clear and timely manner. Providers should also maintain records of all complaints and their resolution, as this supports accountability and helps improve internal processes. If a complainant is not satisfied with the response or outcome, they can escalate the matter to the Office for appropriate action.

7.0 CONSEQUENCES OF NON-COMPLIANCE WITH THE DATA PROTECTION ACT

Failure to comply with the provisions of the Data Protection Act exposes a data controller or data processor to a range of legal consequences, including administrative, civil, and criminal. The following penalties may apply: -

Administrative penalties (issued by the Data Commissioner)

- The Data Commissioner may issue a **penalty notice** for non-compliance.
- Maximum penalty:
 - **Up to KES 5,000,000**, or
 - **Up to 1% of annual turnover** (for organisations), whichever is lower.
- Before penalties, the Commissioner may issue:
 - **Enforcement notices** requiring corrective action within a specified period.
- Failure to comply with an enforcement notice:
 - Fine up to **KES 5,000,000**, or
 - Imprisonment **up to 2 years**, or both

General criminal penalties

Where no specific penalty is provided:

- Fine not exceeding **KES 3,000,000**, or
- Imprisonment term not exceeding **10 years**, or both.

Civil liability (compensation to data subject)

- A person affected by a breach has a right to **compensation** for:
 - Financial loss
 - Emotional distress or damage
- Both **data controllers and processors can be held liable**.

Additional consequences

- Suspension or revocation of the Certificate
- **Reputational damage** and loss of business trust
- **Court orders**, including forfeiture of equipment used in offences or
- Order or prohibit the doing of any act to stop a continuing contravention.

8.0 ANNEXES

8.1 Annex 1: Compliance Checklist

Questions	Yes	No	Comments/ Remedial Action
General Compliance			
We respect the right to privacy as a fundamental human right, as provided in Articles 31(c) and 31 (d) of the Constitution.			
We have identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (2019).			
If we are processing sensitive personal data, we have identified the applicable lawful basis under section 30 of the Data Protection Act, ensured compliance with the data protection principles under section 25, and identified the relevant permitted ground under Part V of the Data Protection Act.			
We grant the highest degree of autonomy possible with respect to control over their personal data.			
We restrict processing where the legal basis or legitimate interests cease to apply.			
We do not do anything generally unlawful with personal data or inconsistent purpose for processing.			
If we are subject to mandatory registration, we have submitted accurate and up-to-date information concerning our processing activities to the Office of Data Protection Commissioner (ODPC).			
We have considered how the processing may affect the individuals concerned and can justify any adverse impact.			

We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified			
We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject.			
We do not deceive or mislead people when we collect their personal data.			
We have clearly identified our purpose or purposes for processing and have clearly documented those purposes.			
We include details of our purposes in our privacy notices.			
We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitations.			
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.			
We use technical measures to limit the possibility of repurposing personal data.			
We only collect personal data that is adequate, relevant, and limited to what is necessary for our specified purposes.			
We can demonstrate the relevance of the data to the processing in question.			
We periodically review the data we hold and delete anything we don't need.			
We avoid the creation of more copies or entry points for data collection than is necessary.			

We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
We ensure the accuracy of any personal data we process and the reliability of our sources.			
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.			
We carry out tests for accuracy at critical steps.			
We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain.			
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.			
If we need to keep a record of a mistake, we clearly identify it as a mistake.			
We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of personal data.			
We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitations.			
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.			
We use technical measures to limit the possibility of repurposing personal data.			

We only collect personal data that is adequate, relevant, and limited to what is necessary for our specified purposes.			
We can demonstrate the relevance of the data to the processing in question.			
We periodically review the data we hold and delete anything we don't need.			
We avoid the creation of more copies or entry points for data collection than is necessary.			
We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
We ensure the accuracy of any personal data we process and the reliability of our sources.			
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.			
We carry out tests for accuracy at critical steps.			
We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain.			
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.			
If we need to keep a record of a mistake, we clearly identify it as a mistake.			

We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.			
As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.			
We know what personal data we hold and why we need it.			
We carefully consider and can justify how long we keep personal data.			
We have a policy with standard retention periods where possible.			
We regularly review our records with a view of identifying personal data that no longer requires to be retained and delete or anonymise such data.			
We have appropriate processes in place to comply with individuals' requests for rectification and/or erasure of false or misleading data about them.			
We identify any personal data that we need to keep for public interest in archiving, scientific or historical research, or statistical purposes.			
We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards or valid consent from the data subject.			
We checked and fulfilled all conditions set under part VI of the DPA and Regulations 2021.			
We have clearly identified our purpose or purposes for processing.			
We have documented those purposes.			

We include details of our purposes in our privacy notices.			
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 a simplified opt-out mechanism.			
We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitations.			
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.			
We use technical measures to limit the possibility of repurposing personal data.			
Processing personal data based on consent			
Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of a statement or a clear affirmative action			
Are procedures in place to demonstrate that an individual has consented to their data being processed?			
Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
Processing children's personal data			
Are procedures in place to verify the age of a child?			

Have you obtained consent from a parent/ legal guardian?			
Processing personal data based on legitimate interest			
If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate?			
Does the analysis must demonstrate that: there is a valid legitimate interest, the data processing is strictly necessary in pursuit of the legitimate interest, and the processing is not prejudicial to or overridden by the rights of the individual			
Data Subjects Rights			
Is there a documented policy/procedure for handling Data Subject Access Requests?			
Is your organisation able to respond to Data Subject Access requests within 7 days of the request?			
Are procedures in place to comply with data portability requests within 30 days, including by providing personal data in a structured, commonly used and machine-readable format?			
Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
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?			
Are individuals told about their right to object to certain types of processing such as direct marketing?			

Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
If automated decision-making, which has a legal or significant similar effect for an individual, is based on consent, has explicit consent been collected?			
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?			
Accuracy and Retention			
Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?			
Do you have procedures in place to ensure data are destroyed securely, in accordance with your retention policies?			
Transparency Requirements			
Are individuals fully informed of how you use their data in a concise, transparent, intelligible, and easily accessible form, using clear and plain language?			
Where personal data are collected directly from the individuals, are procedures in place to ensure you have complied with your duty to notify?			

If personal data are not collected from the subject but from a third party (e.g. shared due to legal obligation) are procedures in place to provide a data protection policy to the individuals?			
When engaging with individuals, such as when providing a service or CCTV monitoring, are procedures in place to proactively inform individuals of their data subjects' rights?			
Is the information on how the organisation facilitates individuals exercising their data subjects' rights published in an easily accessible and readable format?			
Data Processor Agreements			
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)			
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			
Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative, and physical safeguards for personal data?			
Is there a designated individual who is responsible for preventing and investigating security breaches?			

Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			
Data Breach Response Obligations			
Does the organisation have a documented privacy and security incident response plan?			
Are there procedures in place to notify the Office of the Data Protection Commissioner of a data breach?			
Are there procedures in place to notify data subjects of a data breach?			
Are the plans and procedures regularly reviewed?			
Are all data breaches fully documented?			
Are there cooperation procedures in place between data controllers, data processors, and other partners to deal with data breaches?			
Compliance Reporting			
Is there compliance assessment carried out to ensure compliance with the data protection Act and its attendant Regulations?			
The organisation prepares compliance report regularly and undertakes to address any non-compliance finding			

The organization considers submitting compliance report to the Data Commissioner			
--	--	--	--