REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

Data Sharing Code

INTRODUCTION

1.1 Background

Data Sharing is the process of exchanging data between individuals and organizations while preserving data quality and accessibility. Data sharing has become an integral part of modern research, business operations, and societal progress. Data sharing can be carried out using automated and non-automated means.

In its simplest form, data sharing can involve two people exchanging contact information. However, data sharing can also be a complex and multifaceted process, involving the exchange of large volumes of data often across different platforms and systems.

In recent years, the volume and complexity of data have grown exponentially, driven by the proliferation of digital devices, the rise of the Internet of Things (IoT), and the increasing adoption of cloud computing. The growth of big data presents both opportunities and challenges. On one hand, big data can be used to generate new insights, improve decision-making, and drive innovation. On the other hand, big data also raises concerns about privacy, security, and the potential for misuse.

As the digital landscape evolves, the volume of data generated and processed by organizations has reached unprecedented levels. The accelerating pace of digital transformation, coupled with increasing interconnectivity, has led to a proliferation of data-driven initiatives across sectors. From healthcare to finance, and from government services to private enterprises, data sharing has emerged as a cornerstone for innovation, efficiency, and collaborative problem-solving.

Data sharing can be a valuable tool for research, innovation, and collaboration. For example, scientists can share data with each other to replicate studies and make new discoveries. Businesses can share data with each other to improve their products and services. Government agencies can share data with each other to improve public services, enhance decision making, boost productivity, foster innovation and improve data quality.

However, data sharing also raises a number of concerns, such as privacy, security, and confidentiality as it may lead to unauthorized access, use or disclosure. Therefore, there is need for transparency about how data is being collected, stored, used, and shared.

Recognizing the transformative potential of responsibly sharing data while acknowledging the associated risks, it has become imperative to establish clear guidelines and ethical standards through the development of the Data Sharing Code. This code guides on both private and public entities sharing data within or outside the country.

1.2 Privacy concerns

The increasing volume and complexity of data, coupled with the growing sophistication of data collection, storage and processing techniques, have raised significant privacy concerns. These concerns stem from the potential for misuse, unauthorized access, and the erosion of individual control over personal information.

1.2.1 Unauthorized Access and Data Breaches

One of the primary privacy concerns associated with data sharing is the risk of unauthorized access and data breaches. As data is shared across multiple entities, the potential exposure points increase, making it more vulnerable to cyberattacks and malicious actors. Data breaches can result in the theft of sensitive personal information, such as financial records, health data, and communications, leading to identity theft, financial fraud, and reputational damage.

1.2.2 Misuse of Personal Data

Personal data shared for specific purposes can be misused for unauthorized or unintended purposes, posing a significant threat to individual privacy. This can include profiling individuals for targeted advertising, discrimination in employment or insurance decisions, and even manipulation of behavior or social outcomes. The lack of transparency and accountability in data sharing practices often makes it difficult for individuals to identify and prevent such misuse.

1.2.3 Lack of Transparency and Informed Consent

Many individuals are unaware of how their personal data is being collected, used, and shared, making it challenging for them to make informed decisions about their privacy. Data collection and sharing practices often lack transparency, with organizations failing to provide clear and accessible information about data handling procedures. Informed consent, a crucial aspect of privacy protection, is often compromised due to complex terms of service agreements, confusing privacy policies, and the lack of alternative options.

1.2.4 Secondary Use of Data

Personal data collected for a specific purpose may be used for another purpose without the individual's consent or knowledge. This practice, known as secondary use of data, can significantly expand the scope of data usage and increase the potential for privacy violations. For instance, data collected for online shopping might be used for marketing purposes, or health data gathered for research might be utilized for commercial insurance underwriting.

1.2.5 Data Aggregation and Re-identification

Even if data is anonymized or pseudonymized, it can still be aggregated and analyzed to re-identify individuals. With advanced data mining techniques and growing datasets, it is becoming increasingly feasible to link anonymized data to individuals, revealing sensitive personal information. This poses a challenge for protecting privacy, as individuals may not be aware of the potential for their anonymized data to be re-identified.

Owing to the above privacy concerns, having in place a comprehensive data sharing code that addresses privacy concerns in data sharing is a multifaceted endeavor that requires a comprehensive approach encompassing technical, legal, and ethical considerations.

1.2.6 Social Media and Online Platforms

Social media platforms collect extensive personal data, often without users fully understanding how it will be used. This data can be exploited for targeted advertising or even political manipulation. The rise of online harassment, doxing (publishing private information without consent), and cyberbullying poses significant risks to individuals' privacy and safety.

1.3 Scope and purpose

The purpose of this code is to provide a framework for responsible and ethical data sharing practices. It outlines key principles, guidelines, and responsibilities for organizations and individuals involved in data sharing activities. The code aims to promote transparent, secure and accountable data sharing that respects individuals' privacy rights and promotes collaboration in personal data management.

This code applies to all forms of data sharing of personal data, including data sharing between organizations within the private and the public sector.

1.4 Applicable legal framework

Section 55 of the Act provides for the issuance of a Data sharing code by the Data Commissioner, which shall contain practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation and such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data. Further the Data Sharing code under subsection 55 (2) should specify the lawful exchange of personal data between government departments or public sector agencies.

2. KEY PRINCIPLES OF PERSONAL DATA SHARING

2.1 Key Data Sharing Principles

- Lawfulness, fairness and transparency – data must be processed lawfully, fairly and transparently to the data subject
- Purpose limitation – data must be collected for specified, explicit and legitimate purposes
- Data minimization – only the minimum data necessary for the specified purpose should be collected or processed
- Accuracy – data must be kept accurate and up to date
- Individual Rights - Respect individuals' rights to access, correct, or delete their data.
- Storage limitation – data must be kept for only as long as necessary for the specified purpose
- Integrity and confidentiality – data processing must be done in a way that ensures appropriate security, integrity and confidentiality
- Accountability – the data controller is responsible for demonstrating compliance with these principles
- Data sharing agreements should be non-exclusive, have defined time limits, and permission for data use should be revocable at any time.
- Data sharing agreements confer stewardship; data ownership cannot be transferred and, as such, recipients cannot redistribute or sell the data.
- Data recipients should not attempt to reidentify deidentified data.
- Data cannot be associated with other data sets without explicit permission.
- The key purpose of data sharing activities and engagements should be transparent to all stakeholders.
- Data sharing should be timely.
- Data should be interoperable, when necessary.
- Data may be restricted for a limited time, if adequately justified, restrictions may be placed on access to and uses of publicly funded data and datasets for specified periods of time. Justified restrictions may include specific protections of national security, personal privacy, intellectual property and confidentiality.

3. PRIVATE SECTOR DATA SHARING

This section provides a guidance on data sharing within the private sector. This section includes; the legal basis for sharing data, the scope, the responsibilities, rights of the data subject, and the elements of the data sharing and assessment of the safeguards in the private sector.

3.1 Legal basis for sharing

3.1.1. There is need to clearly explain the lawful basis for sharing data. The lawful basis for one organization in a data sharing arrangement might not be the same as that for another organization. Where consent is used as a lawful basis for disclosure, then the agreement should provide a consent form and ensure that all conditions for consent are met as stipulated in Regulation 4 in the Data Protection (General) Regulations, 2021.

3.1.2. The processing of personal data is governed by principles set out under section 25 of the Data Protection Act, 2019. Regulation 21 of the Data Protection (General) Regulations, 2021 permits data controllers and data processors to share or exchange personal data.

3.1.3. In sharing personal data, data controllers and data processors are required to determine the purpose and means of sharing personal data from one data controller or data processor to another.

3.1.4. All instances of data sharing must be on the basis of a data request as stipulated in Regulation 21 (6) of the Data Protection (General)Regulations.

3.1.5. As per Regulation 21 (5) of the Data Protection (General) Regulations 2021, data sharing within the organizational structures of a data controller or data processor is not considered as data sharing.

Summary table of legal basis of data sharing.

Legal Basis	Description	Example
Consent	Individual provides explicit, informed, and voluntary consent.	A customer agrees to share their data with a marketing firm.
Performance of a Contract	Required to fulfill a contract with the individual.	Sharing data with a delivery service to complete an online order.
Legal Obligation	Required to comply with a legal obligation.	Sharing employee data with the Kenya Revenue Authority (KRA).
Vital Interests	Required to protect someone's life or health.	Sharing medical data in an emergency.
Public Interest	Necessary for tasks in the public interest or official authority.	Sharing data for national security or public health initiatives.
Legitimate Interests	Necessary for legitimate interests, provided individual rights are respected.	Sharing customer data for targeted advertising after a balancing test.

Research/Statistics	Necessary for research, statistics, or archiving in the public interest.	Sharing anonymized data for academic research.
Publicly Available Data	Data already made public by the individual.	Sharing information from a public social media profile.

3.2 Scope of sharing

The scope of personal data sharing as contemplated by the Data Protection Act, 2019 is personal data shared on a routine basis, where the same data sets are regularly shared between the same entities for an established purpose; and exceptional, one-off decisions to share personal data for a purpose that is ad hoc, unexpected or due to an urgent situation or an emergency.

The Data Protection (General) Regulations, 2021 also requires data controllers and data processers who routinely share data to enter into data sharing agreements for purposes of data sharing.

3.3 Responsibilities of the transferring entities

The entity sharing personal data shall ensure that they comply with the principles of data protection enumerated in the Data Protection Act, 2019 and its Regulations and must consider the rights of the data subject.

A data controller or data processor shall:

1. Determine the purpose and means of sharing personal data from one data controller to another.
2. Enter into data sharing agreements prior to sharing of personal data.
3. Be in receipt of a written data sharing request as per regulation 21 of the Data Protection (General) Regulations 2021.
4. Inform the data subjects that their personal data will be or is being shared.
5. In a data sharing arrangement, organizations must have policies and procedures that allow data subjects to exercise their individual rights easily. There are additional requirements if your data sharing involves automated decision-making. The position on individual rights is slightly different for law enforcement processing.

3.4 Responsibilities of the receiving entities

Before personal data is shared, the party receiving personal data shall ensure that it has put in place adequate measures for confidentiality, use, access, notification of breach, inspection review, audits and return or destruction and security of personal data as enumerated below —

a) Confidentiality of personal data

i. Protect the confidentiality of the personal data.

ii. Release or publish only data that do not directly or indirectly identify a person.

iii. Do not release any data that the data controller or data processor has kept confidential.

iv. Take all steps necessary to protect the personal data in accordance with the Data Protection Act, 2019.

v. Consult with the data controller or data processor prior to publishing or sharing personal data if there are any concerns with confidentiality.

b) Use of information

i. Limit the use of personal data to the purpose for which it was requested.

ii. Do not match the personal data that is shared without identifiers to any other records or data files for any reason, including to identify a person.

c) Inspections, reviews and audits

Upon request by a data controller, provide a self-assessment, a site inspection, a review and/or an audit according to the provisions of any data sharing agreement, in order to review compliance with the terms set out in the agreement.

d) Return or destruction of the information

i. Upon termination or expiry of the duration for sharing of the personal data, and within the period agreed, return to the data controller or data processor all personal data, with no copy or portion retained; or,

Request the data controller or data processor's approval to destroy all personal data in accordance with security requirements agreed upon with the data controller or data processor and provide a written confirmation of destruction from the receiving entity to the transferring entity.

Illustration

Company A, a data controller, has engaged Company B, a data processor, to process personal data on its behalf. After the completion of the data processing activities, Company A decides to terminate the contract with Company B and no longer requires its services. As part of the contract termination process, Company A requests Company B to destroy all personal data it holds on behalf of Company A.

1. **Request for Data Destruction:**

Company A formally notifies Company B of its decision to terminate the contract and requests the destruction of all personal data in Company B's possession. The request specifies the timeframe within which the data destruction must be completed and any security requirements agreed upon between the two parties.

2. **Approval from Company B:**

Upon receiving the request, Company B reviews the security requirements agreed upon with Company A to ensure compliance. Company B evaluates the feasibility of destroying the personal data within the specified timeframe and confirms its approval to proceed with the data destruction process.

3. **Data Destruction Process:**

Company B initiates the data destruction process in accordance with the agreed-upon security requirements and best practices for data disposal. Personal data stored in electronic databases or systems is securely erased or deleted using industry-standard data destruction methods. Any physical copies of personal data, such as paper documents or storage devices, are securely shredded or destroyed to prevent unauthorized access or retrieval.

4. **Confirmation of Destruction:**

Once the data destruction process is complete, Company B provides a written confirmation of destruction to Company A. The confirmation document includes details such as the date and time of data destruction, the methods used for destruction, and any other relevant information required by Company A. Company A verifies the accuracy of the confirmation document and retains it as evidence of compliance with data destruction requirements.

5. **Closure of Contract:**

With the successful destruction of personal data and receipt of confirmation from Company B, Company A formally closes the contract and terminates its relationship with Company B. Both parties update their records accordingly and take any necessary steps to ensure the

proper handling of any remaining contractual obligations or liabilities.

This illustration demonstrates the process of requesting and obtaining approval from a data processor for the destruction of personal data in accordance with security requirements agreed upon with the data controller. It emphasizes the importance of ensuring compliance with data protection obligations and maintaining transparency and accountability throughout the data destruction process.

3.5 Elements of the data sharing agreements

A data sharing agreement is a legally-binding document or agreement, between two or more entities, which regulates how personal data is shared among these parties and for what purpose. Data sharing agreements are especially valuable when it comes to personal data transfers.

Benefits of data sharing agreements include—

a) Ensures legal compliance.
b) Defines the roles and responsibilities of all parties.
c) Sets out the purpose of the personal data sharing.
d) Covers what happens to the personal data shared.
e) Sets standards for personal data sharing.
f) Establishing trust with your partners and customers by showing them that you are implementing privacy-friendly practices for protecting the data shared.

A **well-structured data sharing agreement** may clarify the following elements—

(a) Definition of parties: clearly identify all parties involved in the personal data sharing process. This includes the data controller or data processor or data subject (the person or entity providing the personal data), the personal data recipient (the entity receiving the data), and any third parties involved.
(b) Purpose of data sharing and legal basis: articulate why the data is being shared.
(c) Categories of data to be shared: specify the types and categories of data being shared (for example name, address, phone numbers) and the rights of the data subject whose personal data is being shared.
(d) Function of the parties: define the function of the party disclosing and the party receiving data, in relation to their purpose.
(e) Processing details: description of how data will be processed (for example information is sent via a secure file transfer, then stored). Duration and frequency of the sharing should be indicated.
(f) Security measures: detail the security measures in place to protect the data during transmission and storage. For example: password protection, unique identifiers, data breach procedures and data encryption.

Illustration:

Company X, a data controller, is considering sharing personal data with Company Y, another data controller, for the purpose of conducting a market research survey. Before proceeding with the sharing of personal data, Company X must ensure that the sharing is justified and complies with data protection principles.

1. **Enhancement of Data Subject Rights:**

Company X assesses whether the sharing of personal data with Company Y enhances the rights of the data subjects. For example, Company X may consider whether the survey results will benefit the data subjects by improving products or services tailored to their needs.

2. **Proportionality of Data Transfer:**

Company X evaluates whether the transfer of personal data to Company Y is proportionate to the purpose for sharing. It considers whether the amount and type of personal data to be transferred are necessary and appropriate for conducting the market research survey.

3. **Minimum Personal Data Required:**

Company X determines the minimum personal data that can be transferred to Company Y to achieve the intended purpose of the sharing. It identifies the specific data elements needed for the survey while minimizing the collection and transfer of unnecessary personal data.

4. **Exploring Alternatives to Data Sharing:**

Company X explores whether the objective of conducting the market research survey could be achieved without sharing personal data or by sharing less personal data. It considers alternative methods, such as anonymized data or aggregate statistics, to achieve the desired outcomes while reducing privacy risks.

5. **Implementation of Safeguards:**

Company X ensures that appropriate safeguards are in place to minimize the risks or potential adverse effects of the sharing. This may include implementing encryption measures, access controls, and data protection agreements with Company Y to protect the confidentiality and integrity of the personal data.

Once Company X has carefully considered these factors and decided to proceed with the sharing of personal data with Company Y, it ensures that the sharing complies with data protection principles and the rights of data subjects as provided by relevant sections of the Data Protection Act, 2019. Company X takes steps to document the decision-making process and ensures transparency and accountability in its data sharing practices.

(g) Retention and deletion: specify how long the data will be kept before it is deleted.
(h) Period of agreement: This specifies the term for which the data sharing agreement is valid. Individual parties to the data sharing agreement should have the right to terminate their participation with adequate notice.
(i) Timing and frequency of updates—If data is to be provided on an ongoing basis, it is important to specify when new data should be shared.
(j) Custodial responsibility and data stewardship—This section establishes the responsibility for maintenance of data security. This should include the secure process for transmitting the file and any particular file format. If there are special circumstances regarding data access, they should be specified here.
(k) Resources and costs of personal data sharing and data management—If necessary, the agreement can stipulate which entities will be responsible for specific data sharing costs.
(l) No warranty for data or linkage quality—This section provides protection for the receiving organization, which commits to make reasonable efforts to promote data quality, but does not guarantee any specific standard.
(m) Indemnification—This clause provides that in the case of legal claims against any of the parties to the agreement, normal legal rules and principles will apply, and states that if one party becomes aware of a claim against the other, they should inform the other party in a timely manner.

3.6 Assessment of safeguards

In order to mitigate risks associated with sharing of personal data, a data controller or a data processor must ensure that the sharing is justified by considering the following factors—

a) Whether the sharing enhance the rights of the data subject.
b) Whether the transfer of personal data is proportionate to the purpose for sharing.
c) What are the minimum personal data that can be transferred to achieve the intended purpose of the sharing?
d) Could the objective be achieved without sharing personal data, or by sharing fewer personal data?
e) What safeguards are in place to minimize the risks or potential adverse effects of the sharing?

Once a decision is taken to share personal data, the sharing of personal data should comply with the principles of data protection and rights of data subjects provided by sections 25, 26 and 41 of the Data Protection Act, 2019.

3.7 Data Protection Policy

Data processors and data controllers are encouraged to develop, publish and regularly update a policy reflecting their personal data handling practices and reflects the data sharing practices.

3.8 Contracts of Data Controllers and Data Processors

Data controllers and data processors may only engage through a written contract. The contract must provide specified particulars specified under the Data Protection (General) Regulations, 2021.

Data processors are not permitted to engage the services of a third party without the prior authorization of the data controller. Once authorization is given, the data processor shall enter into a contract with the third party.

3.9 Elements in Implementing Data Protection by Design or Default

Data controllers and data processors are required under the Regulations to establish data protection mechanisms aligned with the Data Protection Act, 2019 and the Regulations and design technical and organizational measures to safeguard and implement the data protection principles as stipulated in Part V of the Data Protection (General) Regulations, 2021.

4. PUBLIC SECTOR DATA SHARING

Public bodies are expected to comply with the Data Protection Act, 2019 and the Regulations in their personal data sharing activities. This part of the code seeks to guide public sector bodies on how to handle personal data.

Data subjects are entitled to expect that public sector bodies will only handle and share their personal data lawfully, fairly, and in a transparent manner. Their data should only be processed where it is relevant, essential, and necessary to provide them with public services or to carry out another public good function.

Whilst data sharing can bring benefits in terms of efficient delivery of public services, it must be done in a way that respects the rights of individuals to have their personal data treated with care and not accessed or used without good reason.

As such, the data sharing arrangements in the public sector should generally:

a. Identify a clear legal basis of sharing personal data as provided by the Data Protection Act, 2019;
b. Facilitate implementation of Data Protection by design and default;
c. Have a clear justification for each data sharing activity;
d. Make clear to individuals that their data may be shared and for what purpose;
e. Be proportionate in terms of their application and the objective(s) to be achieved;
f. Share the minimum amount of data to achieve the stated public service objective;
g. Have strict access and security controls; and
h. Ensure secure disposal of shared data.

Example:

The Ministry of Education identifies students with frequent absences and declining grades as at risk of dropping out of school so as to implement a program geared to offer personalized educational support and interventions to such students. Personal data collected includes names, school attendance records, recent grades, and teacher notes on student engagement.

This information is shared with a partnered NGO specializing in educational psychology; with parental/guardian consent and following the signing of a data sharing agreement. The NGO uses the data to create customized support plans for each student, involving academic tutoring, counseling, and sometimes financial aid, directly addressing the factors contributing to the risk of dropping out of school. This targeted approach allows for effective use of personal data to provide significant educational support, while also adhering to the principles of data protection outlined in the Data Protection Act.

Illustration:

A County government agency, Municipal Council A, is contemplating sharing residents' personal data with a neighboring Town's transportation department, Municipal Council B, to improve public transportation services. Before proceeding with the data sharing arrangement, Municipal Council A conducts a thorough assessment, considering the following checklist:

1. Objective of Data Sharing:

Municipal Council A identifies that the purpose of sharing residents' personal data with Municipal Council B is to enhance public transportation services, such as optimizing bus routes and schedules based on commuting patterns.

2. Exploring Alternatives:

Municipal Council A explores whether the objective could be achieved without sharing personal data or by anonymizing it. It considers alternative methods, such as conducting surveys or using anonymized data from transportation usage cards, to gather necessary information while minimizing privacy risks.

3. Minimum Information Required:

Municipal Council A identifies the minimum information required to achieve the purpose of improving public transportation services. This may include data such as residential addresses, commuting patterns, and preferred transportation modes.

4. Assessment of Risks

Municipal Council A identifies potential risks associated with the data sharing arrangement, such as unauthorized access, data breaches, or misuse of personal information. It evaluates the likelihood and impact of these risks and develops strategies to mitigate them.

5. Frequency and Timing of Data Sharing:

Municipal Council A determines when and how often the data should be shared with Municipal Council B. It may decide to share data on a periodic basis, such as monthly or quarterly, to ensure the timeliness and relevance of the information for transportation planning purposes.

6. Consideration of DPIA:

Municipal Council A considers whether a Data Protection Impact Assessment (DPIA) is required for the data sharing arrangement. Given the sensitive nature of personal data involved and the potential impact on individuals' privacy rights, City Council A decides to conduct a DPIA to assess and address any data protection risks associated with the sharing.

After conducting a comprehensive assessment and considering the checklist items, Municipal Council A makes an informed decision regarding the data sharing arrangement with Municipal Council B. It implements appropriate safeguards, such as data encryption and access controls, to protect residents' personal data and ensures compliance with data protection laws and regulations. Additionally, City Council A remains vigilant in monitoring the data sharing activities and regularly evaluates their effectiveness in achieving the intended objectives while safeguarding individuals' privacy rights.

4.1 Lawful/legal basis

Section 30 of the Data Protection Act 2019 provides for the lawfulness and legal basis of which public entities process personal data.

Public entities should prior to entering into any data sharing agreement, identify the lawful basis that would require them to share the personal data, in line with section 30 of the Act. This lawful basis may include:

i. for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
ii. for compliance with any legal obligation to which the controller is subject;
iii. in order to protect the vital interests of the data subject or another natural person;
iv. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
v. for the performance of any task carried out by a public authority;
vi. for the exercise, by any person in the public interest, of any other functions of a public nature;
vii. for the purpose of historical, statistical, journalistic, literature and art or scientific research.

To ensure that data sharing is lawful, public bodies should only share personal data where the receiving entity complies with the principles set out in section 25 of the Act as well as the requirement to have a legal basis for the processing of personal data.

The public policy objective being pursued by a particular data sharing arrangement, as well as the legal basis for the processing in question, should be explicit and transparent. An assessment by the transferring entity should be made as to whether the likely benefits of the sharing are balanced with the individual's data protection and privacy rights.

When entering into an arrangement to share personal data (either as a provider, a recipient or both) it is imperative to identify the purpose that it is meant to achieve. In doing so, public sector bodies should consider the potential benefits and risks, either to individuals or society, of sharing the data.

An assessment as to the likely results of not sharing the data should also be conducted. The benefits- risks assessment referred above would require public bodies to consider the following non-exhaustive checklist from the outset when assessing a data sharing arrangement (either as a provider, a recipient, or both):

a. Identify what the sharing is meant to achieve.
b. Identify whether the objective could be achieved without sharing the data or by anonymizing it.
c. Identify the minimum information required to achieve that purpose.
d. Identify any risks which the data sharing may pose.
e. Identify when and how often the data should be shared.
f. Consider whether a Data Protection Impact Assessment (DPIA) is required.

4.2 Sharing for emergencies purposes

Upon request, a data holder shall make data available to a public sector body demonstrating an exceptional need to use the data requested. An exceptional need to use data within the meaning of this Section is deemed to exist if any of the following circumstances apply:

(a) Where the data requested is necessary to respond to a public emergency or public good. The following situations shall constitute public emergencies

i. preventing serious physical harm to a person;
ii. preventing loss of human life;
iii. protection of public health;
iv. safeguarding vulnerable adults or children;
v. responding to a crisis;
vi. an immediate need to protect national security.
vii. taking appropriate action in relation to any suspected unlawful activity or serious misconduct.

(b) Where the data request is limited in time and scope and necessary to respond to a crisis or to assist the recovery from a public emergency;

(c) Where the lack of available data prevents the public sector body from fulfilling a specific task in the public interest that has been explicitly provided by law;

4.3 Responsibilities for the public body in emergency situations

When requesting data in an emergency situation, a public sector body shall put the request in writing, specifying:

i. what kind of data is being requested;
ii. the nature of the emergency situation.
iii. the deadline by which the data is to be made available or within which the data holder may request the public sector body to modify or withdraw the request.

A request for data shall be expressed in clear, concise and plain language and be proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested.

4.4 Obligations of public sector bodies receiving information

A public sector body having received data pursuant to a request shall:

(a) not use the data in a manner incompatible with the purpose for which it was requested;
(b) implement necessary technical and organizational measures that safeguard the rights and freedoms of data subjects;
(c) destroy the data as soon as they are no longer necessary for the stated purpose and inform the data holder that the data has been destroyed.

4.5 Cost

Data made available to respond to a public emergency must be provided free of charge.

4.6 Data Sharing for Research purposes

- A public sector body shall be entitled to share data received with individuals or organizations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested, or to national statistical institutes for compilation of official statistics.
- Organizations receiving the data shall act on a not-for-profit basis and in the context of a public-interest mission. Organizations receiving the data shall not include organizations upon which commercial undertakings have a decisive influence or which could result in preferential access to the results of the research.
- Personal data shall, to the largest extent possible, be in an anonymized format and in a manner that individuals cannot be re-identified.
- Any personal data sharing between parties has to be guided by a valid agreement including nondisclosure, data confidentiality provisions, data protection safeguard provisions including the data destruction technique to be used, data protection impact statement and a data responsibility matrix.
- Under no circumstances should the data collected be sold to third parties or transferred out of the country, unless the concerned individual consents to the transfer. The transfer of personal data to another country shall only take place where sufficient proof has been given on the appropriate safeguards with respect to the security and protection of the personal data.
- For public entities, requests for personal data shall be channeled through the relevant agencies. **For example,** health data shall be sourced from the Ministry of Health; telecommunications data from the Communications Authority of Kenya, transport data from the National Transport and Safety Authority, among others.

4.7 The benefit risk assessment form

A public sector periodically involved in data sharing may undertake the benefit risk assessment form to evaluate their data sharing practices in the form below.

Form: Benefit-Risk Self-Assessment Form for by Public Entities

Section 1: Basic Information

Field	Details
Project Name	
Project Lead	
Department/ Agency/ Organisation	
Date of the Assessment	

Section 2: Purpose of Data Sharing

Field	Details
Description of Data Sharing Purpose	
Objectives of Data Sharing	
Anticipated Benefits	
Legal Basis for Data Sharing	

Section 3: Data Description

Field	Details
Type of Personal Data to be Shared	
Data Categories (e.g., Name, Address, Date of Birth, Health Records)	
Volume of Data	
Data Source(s)	

Data Recipients	

Section 4: Benefits Assessment

Criterion	Details	Description
Public Interest	Describe how data sharing serves the public interest	
Service Improvement	Describe how data sharing will improve public services	
Research and Innovation.	Describe the potential for research and innovation	
Efficiency Gains	Describe any cost savings or efficiency improvements	
Compliance with Legal and Policy Requirements	Detail how the data sharing complies with legal and policy frameworks	

Section 5: Risks Assessment

5.1 Data Security and Privacy Risks

Risk	Likelihood	Impact	Mitigation measure
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	

5.2 Compliance Risks

Risk	Likelihood	Impact	Mitigation

			Measure
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	

5.3 Operational Risks

Risk	Likelihood	Impact	Mitigation Measure
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	

5.4 Reputational Risks

Risk	Likelihood	Impact	Mitigation Measure
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	
	High / Medium / Low	High / Medium / Low	

Section 6: Risk-Benefit Analysis

Field	Details
Summary of the benefit	

Summary of the Risk	
Overall Assessment	
Conclusion	Based on the assessment, is data sharing justified? (Yes/No)

Section 7: Review and Monitoring Plan

Field	Details
Review Frequency	
Responsible Person	
Monitoring Mechanisms	
Next Review Date	

5. CROSS BORDER DATA SHARING OF PERSONAL DATA

Cross border sharing of personal data is guided by Part VI of the Data Protection Act 2019, and part VII of the Data Protection (General) Regulations, 2021. It provides that:

1. Data controllers and data processors shall **conduct cross-border transfers in a lawful, fair and transparent manner**, ensuring that the rights of data subjects are respected.
   For example, a healthcare provider transferring patient records to a facility abroad must first inform the patients and obtain their explicit consent, detailing the purpose and security measures in place to protect their data.
2. **Personal data must be collected and transferred for specified, explicit and legitimate purposes** and not processed in a manner that is incompatible with these purposes. For instance, if a company collects data for employee tax compliance, using this data for marketing without additional consent would be prohibited.
3. **Where the recipient country or organization does not have an adequate level of protection,** the data controller or processor must **implement appropriate safeguards** to protect the personal data during the transfer and processing. These safeguards may include contractual terms, data encryption and technical security measures. An example is a Kenyan company using encrypted communications and a binding contractual agreement with the recipient entity when transferring personal data to a country without an adequacy decision.

4. Should be **based on the data subject's consent**, provided that the data subject is informed of the risks of the transfer and has the right to withdraw consent at any time. For example, a software firm located in Country X may ask for consent to transfer developers' data to a branch in a third Country B, clearly outlining potential privacy risks and the right to withdraw consent.
5. Data controllers and data processors shall **take all reasonable technical, legal and organizational measures**, including contractual arrangements, in order to prevent unlawful international transfer or governmental access to personal data held in the Kenya where such transfer or access would create a conflict with the Data Protection Act or any other law of Kenya.
6. **Requests** by a court, tribunal, or administrative authority from a third country **for access to or transfer of personal data** controlled or processed within Kenya from a data controller or processor **should only be honored if it is supported by an existing international agreement between the requesting country and Kenya**, or if a Kenyan court has recognized the said court order.
7. **In the absence of such an international agreement**, where a data controller or data processor is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to personal data shall take place only:
    a. where the **third-country system requires the reasons and proportionality of the decision or judgement** to be set out, and it requires such decision or judgement, as the case may be, to be specific in character, for instance by establishing a sufficient link to certain suspected persons, or infringements;
    b. the reasoned objection of the addressee is **subject to a review by a competent court** or tribunal in the third-country;
    c. the competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to consider the relevant legal interests of the data controller or data processor protected by Kenyan law. The addressee of the decision may ask the opinion of the Office of the Data Protection Commissioner, pursuant to this Code, in order to determine whether these conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may infringe on national security or defense interests of Kenya.
8. If the conditions in paragraph 7 are met, the data controller or data processor shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation.
9. The data controller or data processor shall **inform the data subject about the existence of a request of an administrative authority in a third-country to access its data** before complying with the request, except in cases where the request

serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

10. Data controllers and data processors that transfer personal data outside Kenya will be required to **notify the Office of the Data Protection Commissioner** of the transfer to ensure that the Office is aware of cross-border data flows and can monitor compliance with the Data Protection Act, 2019.
11. **The Office** of the Data Protection Commissioner **will investigate and sanction data controllers and data processors that violate the Act's** provisions on cross-border data transfers. Data Controllers and Data Processors should be aware of the potential consequences of non-compliance and take steps to ensure that their data sharing practices are aligned with the Data Protection Act's requirements

6. ENFORCEMENT

Where a data holder or data recipient fails to comply with the requirements of this Data Sharing Code, enforcement measures as guided by Section 58 of the Data Protection Act, 2019 and the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, may be pursued.

Issued by:

Immaculate Kassait, MBS
Data Commissioner – Kenya

Date: 4/3/25 Sign: .....