MEDIA
COUNCIL OF KENYA

DATA GOVERNANCE GUIDE
FOR MEDIA PRACTICE IN KENYA

TABLE OF CONTENTS

CEO'S FOREWORD

Journalists and media organisations play a critical role in informing the public and holding power to account. However, this vital function goes hand-in-hand with a growing responsibility to protect the privacy of individuals whose information is collected and used in the course of reporting.

The Media Council of Kenya (MCK) is pleased to present the "Data Governance Guide for Media Practice in Kenya" guidelines to our media industry.

This guide is a vital resource for journalists, media practitioners and media enterprises across the country. It provides a comprehensive framework for implementing robust data governance practices in compliance with the Data Protection Act, 2019, and other relevant legal and regulatory instruments.

This guide is about upholding the core values of journalism including accuracy, transparency, and accountability. By adopting strong data governance practices, media organisations can build trust with audiences and ensure that the right to privacy is respected while upholding the right to freedom of expression.

The guide provides practical guidance on various aspects of data governance, from data collection and storage to data sharing and data subjects' rights management. It highlights the key principles of data protection and explains how to apply them in the context of media work.

The Council believes that this guide will be a valuable tool for journalists and media organisations seeking to navigate the evolving landscape of data privacy. It will help them strike the right balance between responsible journalism and the protection of personal information.

I encourage all stakeholders in the Kenyan media industry to carefully review this guide and implement its recommendations. Through collective action, we can ensure that Kenyan media continues to thrive in a way that respects both the right to information and freedom of expression.

Mr David Omwoyo Omwoyo, MBS

Chief Executive Officer & Secretary to the Council

ACKNOWLEDGEMENTS

In light of significant advancements in data technology, the Media Council of Kenya (MCK) formed a taskforce to create a *Data Governance Guide for Media Practice in Kenya*. This guide is designed to provide Kenyan media professionals with ethical and clear directives for the responsible use of data, ensuring a balance between individual privacy rights and the public's right to information.

Launched in October 2023, this initiative brought together experts from the media, technology, academia, and legal fields to establish strong data management frameworks. These frameworks are designed to support ethical journalism practices while incorporating contemporary data tools.

The Council extends its gratitude to the taskforce, including Sara Mumbua Nzuki, Michael Michie, Prof. John Walubengo, Susan Mute, Ellen Wanjiru, Carole Kimutai, Silas Kiragu, Margaret Kalekye, Michael Oriedo, Dr. Gilbert Mugeni, Rosemary Mwangi, Demus Kiprono, Ken Bosire, Alexander Masiga, Oliver Mathenge, Jeremiah Wakaya, George Mwamodo, Francis Mureithi, Alex Mwangi, Joel Karanja, Oscar Otieno, Paul Kaindo, Anhosi K'Obonyo, Jared Kidambi, Lilian Kimeto, Antony Laibuta, Kenneth Kibet, Fridah Naliaka, and Eric Munene, for their invaluable input and dedication.

We would also like to extend our sincere gratitude to Abraham Mariita, whose expertise and insights were invaluable throughout the development of this document. We further acknowledge the support of Internews, through the European Union-funded *Kenya Safe and Inclusive project (KenSafeSpace)*, whose resources and collaborative spirit greatly contributed to the quality and comprehensiveness of this work.

The Council also appreciates the support of departmental staff, including Victor Bwire OGW, Eric Ndung'u, Jamila Yesho, Sally Washiko, Jackie Kiruja, Jacob Nyongesa, Jerry Abuga, Prudence Wakesho, Stella Kaaria, and Eric Ngaira, whose commitment was instrumental to this guide's success.

We are especially grateful to MCK CEO David Omwoyo, MBS, for his leadership in ensuring this crucial guide supports both media freedom and responsible journalism.

ABBREVIATIONS

CA – Communication Authority of Kenya

DPA – Data Protection Act No. 24 of 2019

DPO – Data Protection Officers

DPIA- Data Protection Impact Assessment

EUGDPR – Regulation (EU) 2016/679 (General Data Protection Regulation)

ICT – Information Communication and Technology

KICA – Kenya Information and Communications Act No. 2 of 1998

KRA – Kenya Revenue Authority

MCK – Media Council of Kenya

NHIF – National Hospital Insurance Fund

NSSF – National Social Security Fund

ODPC – Office of the Data Protection Commissioner

PDF – Portable Document Format

Key definitions

Key definitions under Section 2 of the Data Protection Act (DPA) applicable to this Guide include the following:

Data controller refers to a natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purpose and means of processing personal data. Journalists, media practitioners**,** and media enterprises are data controllers as they collect, store, analyse, and share personal data for media use.

Data processor refers to a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller.

Journalists, media practitioners and media enterprises may seek the services of vendors or service providers to collect, store, analyse, and share personal data on their behalf. These institutions that act on personal data on behalf of media houses are data processors.

Journalists, media practitioners, and media enterprises may also be data processors who process personal data on behalf of regulatory authorities. Examples of other data processors may include media agencies, news agencies, media associations, law firms, insurance companies, ICT service providers, retirement benefits funds, banks, development partners, and independent consultants.

Data governance refers to the overall management of the confidentiality, availability, usability, integrity, and security of data used in an organisation.

Responsible data governance requires journalists, media practitioners and media enterprises to develop policies, strategies, and procedures to ensure data is managed appropriately within an organisation.

Data subject refers to a natural person who is the subject of personal data. The natural person can be identified directly or indirectly by name, identification number, location data, online identifier, or one or more specific factors, such as physical, physiological, genetic, mental, economic, cultural, or social identity.

In media practice, data subjects include journalists, staff at media houses, news sources, consultants, vendors, and members of the public or target audience.

Where the data subject is a child, the DPA mandates journalists, media practitioners, and media enterprises to seek the consent of the child's parent or guardian and ensure that the processing of the child's data is done while advancing the rights and best interests of the child. The DPA also ensures the incorporation of appropriate mechanisms for age verification and consent.

According to the DPA and the MCK Code of Conduct for the Practice of Journalism in Kenya, if the data subject is a minor, journalists, media practitioners, and media

enterprises must seek consent from the parents or guardians to either obtain or process the minor's data. The minor can only be identified by age and not by name.

A similar approach to consent should be applied *mutatis mutandis* for persons with mental illness who lack capacity as defined and protected under the Mental Health Act, Cap 248.

Under the laws of Kenya, a minor or child is defined as any person who has not attained the age of eighteen years. This definition is entrenched in the Constitution of Kenya, 2010, and the Children Act (Cap. 141, Laws of Kenya), and is applicable across all Kenyan legislation.

However, where a data processor relies on consent as a basis for processing personal data, different rules may apply when handling data belonging to citizens of the European Union. Article 8 of the EU General Data Protection Regulation (GDPR) stipulates that the processing of a child's personal data is lawful only where the child is at least 16 years old. For children under the age of 16, such processing is lawful only if, and to the extent that, consent is given or authorised by the holder of parental responsibility. Member States of the EU are however allowed a margin of appreciation of up to an irreducible minimum of 13 years. Journalists, therefore, may rely on this margin of discretion, but only insofar as the child data subject is a citizen of an EU Member State.

The data subjects may be identified using personal data.

The EU General Data Protection Regulation (EU GDPR) refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. It concerns the protection of natural persons with regard to the processing of personal data and the free movement of such data, and it repealed Directive 95/46/EC. The EU GDPR is the primary legislation on data protection within the European Economic Area (EEA). It also applies extraterritorially to data controllers or processors not established in the EU, where the processing activities relate to: the offering of goods or services to individuals in the Union, regardless of whether payment is required; or the monitoring of individuals' behaviour, where that behaviour takes place within the Union.

Accordingly, Journalists, media practitioners, and media enterprises should take into account the provisions and standards of the EU GDPR when processing personal data belonging to individuals or organisations based in the European Union.

Personal data refers to any information pertaining to an identified or identifiable natural person.

Sensitive personal data is information revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex, or the sexual orientation of the data subject. The

Data Commissioner retains the right to classify other forms of data as 'sensitive personal data.'

Journalists, media practitioners and media enterprises may process sensitive personal data for legitimate purpose. Journalists, media practitioners and media enterprises may process sensitive personal data of their employees.

Data processing is any operation or sets of operations performed on personal data or sets of personal data, whether or not by automated means. The operations include activities such as:

(a) Collection, recording, organisation, structuring

Collection could be done physically through filling out forms or digitally through the input of information to digital platforms such as websites and mobile phone applications, among others. Recording and structuring can also be physical or digital.

The collection of personal data may be done directly from the data subject or indirectly from another person, publications, databases, surveillance cameras, information associated with web browsing, or biometric technology, among others. Personal data will be collected for specific, explicit and legitimate purposes. The personal data collected will only be those strictly necessary to the purposes for which they are processed.

On the collection of personal data, Section 28 of the DPA directs that journalists, media practitioners and media enterprises shall collect personal data directly from the data subject. However, personal data may be collected indirectly where:

a) the data is contained in a public record;
b) the data subject has deliberately made the data public;
c) the data subject has consented to the collection from another source;
d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source;
e) the collection from another source would not prejudice the interests of the data subject;
f) collection of data from another source is necessary —
    i. for the prevention, detection, investigation, prosecution and punishment of crime;
    ii. for the enforcement of a law which imposes a pecuniary penalty; or
    iii. for the protection of the interests of the data subject or another person.

(b) Storage, adaptation, or alteration

Journalists, media practitioners and media enterprises may store personal data physically in files and ledgers or digitally in servers hosted within or outside the country.

Alteration, on the other hand, may involve the correction of personal data. Personal data will only be retained for the minimum time necessary for the purposes of its treatment.

(c) Retrieval, consultation, or use
Retrieval involves getting personal data from physical or digital records to gain insights or apply the data to any media operations. For example, for research on a developing story.
(d) Disclosure by transmission, dissemination, or otherwise making available Personal data may be shared with third parties. For example, sharing data between media houses.

(e) Alignment or combination, restriction, erasure, or destruction
Journalists, media practitioners and media enterprises may combine personal data sets in their possession with those of other journalists, media practitioners and media enterprises.

Journalists, media practitioners and media enterprises may also erase personal data that they have no further need to keep or store. For example, journalists, media practitioners and media enterprises may erase or destroy personal data that they erroneously collected.

Third Party means a natural or legal person, public authority, agency, or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

1. SCOPE AND OBJECTIVE OF THIS GUIDE

This document guides journalists, media practitioners, and media enterprises on adherence to data protection principles as provided in the Data Protection Act. It aims to facilitate the adoption and implementation of data governance practices by the media for compliance with the DPA, and other relevant legal and regulatory instruments while paying consideration to international best practices. This Guide recognises the need for the media sector to balance and reinforce the right to privacy while promoting the right to freedom of expression through responsible journalism.

The primary objective of this Guide is to ensure responsible and effective management of data by journalists, media practitioners and media enterprises by:

a. Promoting compliance and regulatory alignment,
b. Promoting quality assurance,
c. Promoting security and privacy,

d. Providing for clear ownership and stewardship,
e. Guiding data lifecycle management,
f. Providing for continuous improvement, and
g. Promoting adequate risk management.

2. APPLICATION

This guide applies to journalists, media practitioners and media enterprises in Kenya.

3. LEGAL FRAMEWORK

The legal framework regulating the media in Kenya includes the Constitution of Kenya, 2010, the Media Council Act No. 46 of 2013, the Data Protection Act No. 24 of 2019, Access to Information Act No. 31 0f 2016, Kenya Information and Communication Act No. 2 of 1998, and the Computer Misuse and Cybercrimes Act No 5 of 2018:

3.1. The Constitution of Kenya

Article 31 of the Constitution provides for the right to privacy. The right to privacy is, however not absolute. It can be limited by way of specific legislation in certain circumstances, provided that such limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. For instance, the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others. As such the right to privacy has to at times to be counter-balanced with other rights including the right to freedom of expression, and the right to freedom of the media, among others.

Data governance in the media involves balancing the right to privacy, freedom of expression, and freedom of the media. Achieving a harmonious equilibrium involves considering the interests of individuals, the public, and the press while addressing the legal, ethical, and societal implications. Key considerations to be made include the law, media ethics, public interest, protection of sources, right to information, ensuring anonymity and protecting whistleblowing.

3.2 Media Council Act No. 46 of 2013

The Media Council Act No. 46 of 2013 provides for the Code of Conduct for the Practice of Journalism in Kenya, which outlines key provisions on privacy, confidentiality, non-discrimination, the rights of children, and professional standards for journalistic practice in Kenya. For instance, Clause 14 provides that:

"(1) The public's right to know shall be weighed against the privacy rights of people in the news.

(2) Intrusion and inquiries into an individual's private life without the person's consent are not generally acceptable unless public interest is involved. Public interest shall itself be legitimate and not merely prurient or morbid curiosity.

(3) Things concerning a person's home, family, religion, tribe, health, sexuality, personal life and private affairs are covered by the concept of privacy except where these impinge upon the public."

The practice of journalism in Kenya would generally necessitate allowable instances of collection and processing of personal data, and sometimes sensitive personal data. This Guide gives further interpretation, and guidelines for data protection in this context. The code should be read together with other codes and guidelines developed from time to time by MCK. For instance, the Code of Conduct for Digital Media Practitioners, the Media Practitioners' Codes of Conduct, among others.

3.3 Data Protection Act No. 24 of 2019

Journalists, media practitioners and media in the course of their work collect, analyse, store, and share data, including personal data. The DPA provides the framework for lawful processing of personal data. To give effect to the DPA, three regulations are in place, the Data Protection (General) Regulations, 2021, the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

Journalists, media practitioners and media enterprises have a duty to comply with provisions of the DPA and the respective Regulations by ensuring that they are registered with the ODPC as data controllers or data processors, or both.

Additionally, the DPA makes provisions for the processing, retention, and the principles applicable to the processing of personal data by journalists, media practitioners and media enterprises as highlighted below:

3.3.1. Processing of Personal Data: The DPA requires that a data controller or data processor shall not process personal data unless the processing is necessary for historical, statistical, journalistic, literary, artistic, or scientific research.

3.3.2. Retention of Personal Data: The Data Protection Act (DPA) provides that a data controller or processor should retain personal data only for as long as is reasonably necessary to fulfil the purpose for which it was collected, unless the data is retained for historical, statistical, journalistic, literary, artistic, or research purposes.

3.3.3. Principles of Processing Personal Data: Journalists, media practitioners and media enterprises in Kenya are allowed to process personal information under the 'journalistic purpose exemption'.

3.4 Access to Information Act No. 31 of 2016

The Act operationalises Article 35 of the Constitution on the right of access to information. Section 6(1)(b) of the Access to Information Act limits access to information where it may *"involve the unwarranted invasion of the privacy of an individual, other than the applicant or the person on whose behalf an application has, with proper authority, been made"*.

3.5 Kenya Information and Communication Act No. 2 of 1998

Clause 7 of the Programming Code for Broadcasting Services, enacted pursuant to section 46H of the Act, obligates broadcasters to protect the right to privacy of individuals.

3.6 Computer Misuse and Cybercrimes Act No. 5 of 2018

The Act addresses offences related to computer systems to facilitate the timely and effective detection, prevention, prohibition, response, investigation, and prosecution of computer and cybercrimes. Journalists, media practitioners, and media enterprises must ensure that their systems are secured to prevent them from being used to commit offences under the Act. Additionally, media enterprises should ensure that their staff are well informed about the provisions of the Act. Finally, journalists and media practitioners should be able to identify, assess, and report cybercrimes as stipulated in the Act.

4. DATA PROTECTION PRINCIPLES

Section 25 of the Data Protection Act

When processing data, media enterprises, journalists, and media practitioners should ensure data is:-

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

(g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

(h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Exemptions

In terms of application of the law, it is noted that the provisions in the DPA relating to journalism, including the exceptions under section 52 (1) of the DPA, applies to editorial journalistic content. For this reason, journalists, media practitioners and media enterprises must ensure that in the publication of editorial journalistic content they apply the following principles of data protection:

a) lawful processing,
b) minimisation of collection,
c) data quality, and
d) the adoption of security safeguard

a) Lawful processing

Explicit and specified purposes: Journalists, media practitioners and media enterprises must expressly indicate to data subjects why they seek to process their data.

The explicit and specified purpose identified must fall within any of the following legitimate purposes.

Legitimate purposes: The DPA provides a list of lawful instances for the processing of personal data. A data controller or data processor should rely on one legal basis of processing personal data at a time. Legal bases for processing personal data are outlined below.

(I) Consent from Data Subject

Personal data can be processed where the data controller and/or processor obtains informed express **consent from the data subject**. Consent within the context of data governance can be understood within the following principles:

a) The data controller or data processor bears the responsibility for establishing a data subject's consent for the processing of their personal data.

b) The data subject retains the right to withdraw consent at any time. However, withdrawal of consent does not negate consent provided before the withdrawal.
c) Consent provided by a data subject should be freely given, specific, informed, and unambiguous.
d) Consent may be provided in written form, electronic form, via email, by sending scanned documents, an electronic signature, or orally.

Where the processing of personal data is based on consent, the data controller or data processor shall inform the data subject of:

a) the identity of the data controller or data processor,
b) the purpose of each of the processing operations for which consent is sought,
c) the type of personal data that is collected and used,
d) information about the use of the personal data for automated decision-making, where relevant,
e) the possible risks of data transfers due to the absence of an adequacy decision or appropriate safeguards,
f) whether the personal data processed shall be shared with third parties,
g) the right to withdraw consent, and
h) the implications of providing, withholding, or withdrawing consent.

The information about the data subject may be presented through a written notice, oral statement, audio, or video message.

(ii) Performance of a contract

Another legitimate purpose for processing personal data is the **performance of a contract**. Where journalists, media practitioners and media enterprises process personal data for the performance of a contract between journalists, media practitioners and media enterprises and a data subject, that processing will be deemed lawful.

(iii) Statutory Compliance

The third legitimate purpose for processing personal data is **compliance with any legal obligation to which the controller is subject**. The Constitution and statutes provide for circumstances under which journalists, media practitioners and media enterprises may process personal data subject to statutory requirements.

(iv) Protection of the vital interests of the data subject or another natural person

The fourth legitimate purpose for processing personal data is **to protect the vital interests of the data subject or another natural person**. Journalists, media practitioners and media enterprises may for example process personal data of a data subject to protect their fundamental rights and freedoms.

(v) Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

The fifth legitimate purpose for processing personal data is the **performance of a task carried out in the public interest or in the exercise of official authority vested in the controller**. Examples of tasks in public interest may include when addressing a natural disaster, for national security purposes, or addressing a public health emergency.

(vi) Legitimate interests pursued by the processor/controller or by a third party

Where one seeks to rely on legitimate interest as a basis for processing personal data, the same can be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, for instance, where the data subject is a child.

The following activities may be indicative of such legitimate interest include:

a) fraud prevention;
b) ensuring network and information security;
c) indicating possible criminal acts or threats to public security;
d) processing employee or client data;
e) direct marketing; or
f) administrative transfers within a group of companies.

Journalists, media practitioners and media enterprises relying on this ground have to give more details and particulars to demonstrate the legitimate interest.

vii) Research

The seventh legitimate purpose for processing personal data is **for historical, statistical, journalistic, literature, and art or scientific research**. This provision is self- explanatory; however, journalists, media practitioners and media enterprises must inform data subjects in advance of the intention to process personal data for research purposes.

b) Minimisation of collection

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This principle requires that journalists must have enough information to do the job, but at the same time avoid having too much information than what is required for the job.

c) Data Quality

Media enterprises and journalists should ensure accuracy and security of personal data. Personal data should be accurate and, where necessary, kept up to date. Steps must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

d) Adopting security safeguards

The media must take reasonable steps to protect personal data. Media enterprises should consider technical (electronic) and physical security measures, staff training and supervision, and policies and procedures including a data breach management plan.

5. DATA GOVERNANCE IN MEDIA

5.1 Key Components of Data Governance in Media

Key components of data governance to be considered are:

(a) **Data collection and storage:** Journalists, media practitioners and media enterprises should collect and store data securely and ensure that it complies with data privacy regulations. This includes implementing appropriate data security measures, such as encryption and access controls.

(b) **Data use and access:** Journalists, media practitioners and media enterprises must define who has access to their data and how it can be used. This includes the application of appropriate data analytic tools, developing clear data usage policies and procedures and training staff on these policies.

(c) **Data sharing and collaboration:** Journalists, media practitioners and media enterprises often share data with partners and third-party vendors and should establish protocols for sharing data safely and securely.

(d) **Data retention and disposal:** Journalists, media practitioners and media enterprises must define how long they will retain data and when and how it will be securely disposed of. This includes developing data retention policies and procedures.

5.2 Implementing Data Governance in Media

Implementing effective data governance in media involves:

(a) **Establishment of clear policies and procedures:** Journalists, media practitioners, and media enterprises should develop policies and procedures for processing, collecting, using, sharing, and disposing of data. These policies should be communicated to all staff and regularly reviewed and updated.

(b) **Creation of a data governance framework:** A data governance framework defines the organisation's data governance strategy, roles, and responsibilities, including the use of technology to automate tasks, track compliance, and generate reports.

(c) It should be developed in collaboration with key stakeholders from across the organisation.

(d) **Training of staff on data governance best practices:** All staff should be trained on the organisation's data governance policies and procedures. This training should help staff understand their roles and responsibilities in protecting the organisation's data.

6. ORGANISATIONAL AND TECHNICAL MEASURES

To comply with the DPA, journalists, media practitioners, and media enterprises should put in place organisational and technical measures. The activities listed below, when carried out comprehensively, will enhance the protection of personal data.

6.1. Data Protection Training

Media enterprises should ensure that all employees working as journalists and media practitioners receive sensitisation training on compliance with the DPA.

Data protection training will not only ensure compliance with the law, but is also key in preventing data breaches.

6.2. Privacy Assessment

Journalists, media practitioners and media enterprises should evaluate their level of compliance with the provisions of the DPA. This evaluation is termed a privacy assessment or a readiness assessment. To carry out a privacy assessment, media enterprises should follow the following steps:

1. Define the scope of the assessment, indicating what systems, technical and organisational measures will be assessed, the data flows, and the risks associated with personal data processing.

2. Identify data protection provisions applicable to the organisation, including the DPA and Regulations under the DPA.
3. Identify gaps in data governance or information governance policies.
4. Create a data inventory that lists the personal data processed. The data inventory will also identify the types of data processed, sources of the data, and reasons the data is processed.
5. Identify sensitive personal data being processed and assess potential harms that could be occasioned through sensitive personal data processing operations.
6. Identify risks to processing personal data, such as unauthorised access, use, disclosure, or modification of personal data.
7. Evaluate controls in place to protect personal data. Assess the adequacy of its technical and organisational controls, policies and procedures, and employee training.
8. Provide concrete recommendations to address the risks and gaps identified in the assessment. Prioritise the recommendations.
9. Implement the recommendations.

Data inventories are to be crafted for all departments and collated into one master data inventory that should be updated regularly.

6.3. Data Retention

Media enterprises should be very clear about how long they may retain personal data. The duration of retention of personal data shall be determined by:

a) Requirements of national and county legislation,
b) The lawful purpose for retaining the data,
c) Authorisation or consent by a data subject, and
d) Need for historical, statistical, journalistic literature and art or research.

6.4. Incident and Data Breach Management

Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, journalists, media practitioners, and media enterprises shall:

(a) notify the Data Commissioner without delay, within **seventy-two (72) hours** of becoming aware of such breach, and
(b) communicate to the data subject in writing within a reasonably practical period unless the identity of the data subject cannot be established.

A data breach is taken to result in a real risk of harm to a data subject and is notifiable to the Data Commissioner if it relates to:

(a) The data subject's full name or identification number and any of the personal data or classes of personal data relating to the data subject set out in the Second Schedule of the Data Protection (General) Regulations, 2021 *or*

(b) The following personal data relating to a data subject's account with a data controller or data processor—

(i) the data subject's account identifier, such as an account name or number; and

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

6.5. Data Sharing Agreements

Where journalists, media practitioners and media enterprises share data, they ought to enter into data-sharing agreements.

6.6. Digital Platforms

Journalists, media practitioners and media enterprises should ensure privacy by design and by default for their mobile phone applications and digital platforms.

6.7. Registration with ODPC

Journalists, media practitioners and media enterprises shall ensure that they are registered with the Office of the Data Protection Commissioner.

MEDIA COUNCIL OF KENYA

Ground Floor, Britam Centre,
Mara /Ragati Road Junction, Upper hill,
P.O.BOX 43132 00100 Nairobi, Kenya

Tel(Office)
0111019200

Cell(Office)
0727735252 | 0702558233 | 0702558234 | 0702558453

- Mombasa: 0111019220
- Kisumu: 0111019230
- Meru: 0111019250
- Nakuru: 0111019240

Email :info@mediacouncil.or.ke
www.mediacouncil.or.ke
Media Council of Kenya
@MediaCouncilK