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 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 practises 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 practises, 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 the right to information.

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.

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 DPA, applicable to this Guide include:

- **Data controller** is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

  Journalists, media practitioners and media enterprises are data controllers as they collect, store, analyse, and share personal data for media use.

- **Data processor** is 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 where they 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 tothe 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 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 to one or more factors specific such as the 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 consent of the child's parent or guardian and ensure that processing of the child's data is done while advancing the rights and best interests of the child as well as ensuring the incorporation of appropriate mechanisms for age verification and consent.

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

media enterprises must seek consent of 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.

A minor/child under the Laws of Kenya is any individual who has not attained the age of the age of Eighteen years. This definition is entrenched under the Constitution of Kenya, 2010, and the Children Act, Cap 141 Laws of Kenya. That definition applies across all laws of Kenya.

However, where a data processor is relying on consent as a ground for processing personal data, this may not be the case where one is dealing with citizens of the European Union. Article 8 of the EUGDPR requires the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States of the EU are however allowed a margin of appreciation of up to an irreducible minimum of 13 years. Journalists would therefore lawfully be allowed this margin but only in so far as the child data subject is a citizen of the one of the Member States of the EU.

The data subjects may be identified using personal data.

- **EUGDPR** refers to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) which is the primary law on data protection with applicability to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.

  In this regard, Journalists, media practitioners and media enterprises are advised to consider the provisions and standards of the EUGPDR when it comes to processing of personal data of the citizens, and organisations registered in the EU.

- **Journalist** is any person who holds a diploma or a degree in mass communication from a recognised institution of higher learning and is recognised as such by the Media Council of Kenya as defined under the Media Council Act, No. 46 of 2013.

- **Personal data** means any information relating 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 '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 on 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 in relation to the purposes for which they are processed.

  On 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 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.

- **Media Enterprise** means an organization whose business involves the collection, processing and dissemination of news or news articles, or in entertainment and education through the media under the Media Council Act No. 46 of 2013.

- **Media Practitioners** are persons who practice their trade in media and include talk show-hosts, comedians, continuity announcers, anchors, presenters, photojournalists, camerapersons, cartoonists, digital media practitioners, graphic designers, content producers, broadcasters under the Kenya Information and Communications Act, a publisher engaged in publication, and the manager or proprietor of a publication or broadcasting station.

1. Scope and Objective of this Guide

This Guide provides principles for data governance for journalists, media practitioners and media enterprises. 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. ensuring security and privacy,
d. providing for clear ownership and stewardship,
e. guiding data lifecycle management,
f. providing for continuous improvement, and
g. ensuring adequate risk management.

There are eight sections in this guide. It begins by providing for the application of the Guide and then delves into the legal and regulatory framework for data governance in media. The Guide then highlights key issues in data governance in media, sets out data governance principles, and underlines data subject rights. The Guide also outlines the organizational and technical measures that journalists, media enterprises and media practitioners must adopt to ensure robust data governance compliance.

Examples provided in this Guide are for illustrative purposes. Journalists, media practitioners and media enterprises ought to tailor the examples to their specific needs.

2. APPLICATION OF THIS GUIDE

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 gives effect to the right of freedom of the media. The Second Schedule read with Section 45 of the Media Council Act provides for the Code of Conduct for the Practice of Journalism in Kenya. The Code of Conduct for the Practice of Journalism is replete with numerous provisions on the protection of privacy, confidentiality, non-discrimination, the rights of children, and standards on the practice of journalistic activities 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

For journalists, media practitioners and media enterprises to execute their mandate, they need to 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 and data processors, or both.

Additionally, the DPA makes several references as relates to the processing, retention, and the principles applicable to the processing of personal data for 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 the purpose of historical, statistical, journalistic, literature and art or scientific research.

3.3.2. Retention of Personal Data: The DPA provides that a data controller or data processor can should only retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is for historical, statistical, journalistic, literature and art 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 what is called the 'journalistic purpose exemption'.

The DPA enables the Data Commissioner to prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Journalism, Literature and Art.

In line with the ODPC's powers and functions, Section 74 of the DPA provides that the Data Commissioner may issue guidelines to data controllers and data processors from time to time. Journalists, media practitioners and media enterprises should also comply with those guidelines.

As such, it is this legal basis that informs the development of this data governance guide for the media.

3.3.4. Public Interest: Public interest in media coverage is the idea that the media should report on issues that are important to the public. This can include issues that are of political, social, or economic importance, as well as issues that are of personal interest to the public.

There are a number of factors that can limit the public's interest in media coverage. These factors include the amount of time that the public has to consume media, the amount of information that the public is exposed to, and the level of trust that the public has in the media.

The Kenya Information and Communications Act, 2016 (KICA) provides for a number of exemptions in public interest for journalists, media practitioners and media enterprises. These exemptions are intended to allow journalists, media practitioners and media enterprises to report on matters of public interest without fear of reprisal. The exemptions include:

(a) the right to publish or broadcast information that is in the public interest, even if it is false or defamatory,

(b) the right to protect the identity of sources of information, even if the information is in the public interest, and
(c) the right to refuse to disclose information that has been obtained in confidence.

KICA also provides for a number of safeguards to ensure that these exemptions are not abused. For example, KICA requires that journalists, media practitioners and media enterprises act in good faith and that they balance the public interest in the information against the rights of individuals.

Examples of public interest may relate to publication of photographs of a public gathering. Journalists, media practitioners and media enterprises may balance the rights to privacy of an individual in a photograph for publication and public interest in publication of the photograph with the individual in it. At all times, journalists, media practitioners and media enterprises should be in a position to provide justification for the publication.

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. Journalists, media practitioners and media enterprises while seeking information from public and private organisations. Access to information is to be predicated by section 6(1)(b) of the Access to Information Act. It provides that the right to access information may be limited 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"*.

Hence, it is critical that journalists, media practitioners and media enterprises strike a balance between the right to access information and the right to privacy of an individual.

3.5 Kenya Information and Communication Act No. 2 of 1998

Clause 7 of the Programming Code for Broadcasting Services enacted under 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 deals with offences relating to computer systems to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes. Journalists, media practitioners and media enterprises should ensure that their systems are protected in such a way that they do not facilitate crimes under the Act. Further, media enterprises should ensure that their employees are well versed in the provisions of the Act. Lastly, Journalists, media practitioners and media enterprises should be in a position to spot, assess, and report any cybercrimes as outlined under the Act.

4. DATA GOVERNANCE IN MEDIA

4.1 Key Components of Data Governance in Media

Some of the key components of data governance in media include:

(a) **Data collection and storage:** Journalists, media practitioners and media enterprises must 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. It is important to 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.

4.2 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 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. It should be developed in collaboration with key stakeholders from across the organisation.

(c) **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.

(d) **Using technology to support data governance:** There are a variety of technology solutions that can help media enterprises implement and manage data governance programs. These solutions can help automate tasks, track compliance, and generate reports.

4.3. Classification of Media Content in Data Governance

It is noteworthy to highlight the media content that journalists, media practitioners and media enterprises process on a day-to-day basis as part of their data processing activities. The media content is divided in two main categories:

4.3.1. Editorial Content

Editorial content refers to articles, reports and other materials published in print, television or online sites by journalists, media practitioners and media enterprises intended to inform, educate, or entertain an audience. This content is not paid for and must be scrutinised by a publication's editorial team to ensure that it meets the necessary standards. The credibility and reliability of editorial content is higher due to the rigorous vetting processes it undergoes, therefore, is trusted since it is backed by the publication.

In terms of application of the law, it is noted that the provisions in the DPA relating to media 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 safeguards.

4.3.2. Non-Editorial Content

Non-editorial content refers to materials that are not produced by editorial teams or journalists, therefore, not intended for news or journalistic purpose. Non-editorial content may include materials created for purposes such as marketing and advertising. Journalists, media practitioners and media enterprises should apply all data protection principles in processing non-editorial content.

Where journalists, media practitioners and media enterprises process personal data for commercial purposes, they should ensure that they comply with provisions of the DPA by seeking and obtaining express consent from a data subject, ensuring that the person is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject and where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

5. DATA PROTECTION PRINCIPLES

The principles of data protection under the DPA provide for:

5.1. Right to Privacy

Every data controller or data processor shall ensure that personal data is processed in accordance with the right to privacy of the data subject.

Journalists, media practitioners and media enterprises should always bear in mind that Article 31 of the Constitution protects the right to privacy of individuals. Hence, when processing personal data journalists, media practitioners and media enterprises, should take into consideration the right to privacy of the data subject should be taken into consideration.

5.2 Lawfulness, fairness, and transparency

Every data controller or data processor shall ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to any data subject.

Lawful processing of personal data: Journalists, media practitioners and media enterprises should ensure that the processing of personal data is for exercise of functions set out in the Constitution and relevant media laws.

Fair processing of personal data: When processing personal data, journalists, media practitioners and media enterprises should bear in mind provisions of Article 27 of the Constitution. Every data subject should be treated equally and should not be discriminated against directly or indirectly on any ground that may include race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dressing, language, or birth.

Transparent processing of personal data: Before processing of personal data, journalists, media practitioners and media enterprises should inform data subjects of the following:

(a) What personal data they collect,
(b) Why they need the personal data,
(c) How they collect personal data,
(d) How they will use the personal data collected,
(e) How they store the personal data,
(f) The period for which the personal data will be stored,
(g) How they keep the personal data safe,
(h) Whether they share the personal data with third parties, and
(i) How the personal data can be accessed, rectified and erased to restrict future processing of the data.

5.3. Explicit, specified, and legitimate purposes

Every data controller or data processor shall ensure that personal data is collected for explicit, specified, and legitimate purposes and not further processed in a manner incompatible with those purposes.

(a) **Explicit and specified purposes**: Journalists, media practitioners and media enterprises must expressly indicate to data subjects why they seek to process their personal data. Examples:

i. Media Council of Kenya, for registration and accreditation, and handling of complaints,
ii. Media Complaints Commission, for adjudication of disputes, and
iii. Media enterprises to educate, entertain and inform and for commercial use.

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

(b) **Legitimate purposes:** The DPA provides a list of lawful instances for 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, sending scanned documents, 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 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 **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.

5.3.1. 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.

5.4. Processing limitation

Every data controller or data processor shall ensure that personal data is adequate, relevant or limited to what is necessary in relation to the purposes for which it is processed.

Journalists, media practitioners and media enterprises should not process more personal data than is necessary to achieve a stated objective.

For example, a news website wants to collect personal data from its readers to personalise their experience on the website. The website should limit collection to the following data: name, email address, location, the data subject events on the journalist's, media practitioner's and media enterprise's website, portal and apps, and browsing history. No sensitive personal information should be collected except within the confine of a lawful, and legitimate purpose.

5.5. Valid explanation

Every data controller or data processor shall ensure that personal data is collected only where a valid explanation is provided whenever information relating to family or private affairs is required.

Before processing personal data, journalists, media practitioners and media enterprises should inform data subjects why they need the personal data. Some valid explanations include for: contractual purposes, compliance with the law, planning and budgeting, public interest, compliance with a court order, research purposes, and journalistic purposes.

5.6. Accuracy

Every data controller or data processor shall ensure that personal data is 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.

Accuracy is at the very heart of a journalist's work and features prominently in the Media Council of Kenya's Code of Conduct for the Practice of Journalism in Kenya. A data processor and or controller should, therefore, record details accurately and take logical steps to check facts, as well as distinguish between facts from opinions.

Journalists, media enterprises and media practitioners should put in place due diligence measures to ensure the accuracy of personal data it processes.

Strategies to ensure the accuracy of data include:

- Before publishing personal data, journalists, media enterprises and media practitioners should verify the accuracy and authenticity of the data. Journalists, media enterprises and media practitioners should cross-check from multiple sources or contact the data subject directly for confirmation.

- There should be documented guidelines on how to collect, process and store personal data. The guidelines should outline the purpose of data collection, the method used to collect the data and how the media enterprise plans to protect the subjects confidentiality and integrity.
- When outsourcing data to third parties, for example, through content syndication, the media enterprise must ensure that the third party safeguards and complies with the DPA.

5.7. Storage limitation

Every data controller or data processor shall ensure that personal data is kept in a form which identifies the data subjects for no longer than is necessary for the purposes for which it was collected.

The DPA provides limitations to the retention of personal data. It stipulates that a data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is —

a. required or authorised by law;
b. reasonably necessary for a lawful purpose;
c. authorised or consented by the data subject; or
d. for historical, statistical, journalistic literature and art or research purposes.

It further requires data controllers/processors to delete, erase, anonymise or pseudonymise personal data not necessary to be retained at the expiry of the retention period.

Media enterprises are required to:

a. have clear internal procedures for deletion and destruction;
b. determine what data and length of storage of personal data that is necessary for the purpose;
c. formulate internal retention statements of implementing them;
d. ensure that it is not possible to re-identify anonymised data or recover deleted data and testing whether this is possible;
e. justify why the period of storage is necessary for the purpose and disclosing the rationale behind the retention period;
f. determine which personal data and length of storage is necessary for back-ups and logs.

Journalists, media practitioners and media enterprises should ensure they have a data retention schedule for all personal data in their possession and comply with the above provisions.

5.8. Data transfers

Every data controller or data processor shall ensure that personal data is not transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

Before transferring data out of Kenya, a data controller/processor is required to ascertain that the transfer is based on—

(a) appropriate data protection safeguards;
(b) an adequacy decision made by the Data Commissioner;
(c) transfer as a necessity; or
(d) consent of the data subject.

(a) Transfers on the basis of appropriate safeguards

A transfer of personal data to another country or a relevant international organisation is based on the existence of appropriate safeguards where—

a. a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations; or
b. the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.

In this context of data transfer on the basis of appropriate safeguards, the following requirements apply:

a. the transfer shall be documented;
b. the documentation shall be provided to the Commissioner on request; and
c. the documentation shall include—
    i. the date and time of the transfer;
    ii. the name of the recipient;
    iii. the justification for the transfer; and
    iv. a description of the personal data transferred.

A country is deemed to have appropriate data protection standards where such a country or a territory has—

a. ratified the African Union Convention on Cyber Security and Personal Data Protection;
b. a reciprocal data protection agreement with Kenya; or
c. a contractual binding corporate rules among a concerned group of undertakings or enterprises.

Binding corporate rules

The contractual binding corporate rules contemplated hereinabove shall be valid if they—

a. are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

b. expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
    a. Further, those corporate rules must specify:
c. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
d. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of another country or countries in question;
e. their legally binding nature, both internally and externally;
f. the application of the general data protection principles;
g. the rights of data subjects in regard to processing and the means to exercise those rights;
h. the complaint procedures; and
i. the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules.

(b) Transfers on the basis of an adequacy decision

Transfer of personal data to another country or a relevant international organization is based on an adequacy decision where the Data Commissioner makes a decision that —

'the other country or a territory or one or more specified sectors within that other country, or the international organization, ensures an adequate level of protection of personal data.'

In this regard, journalists, media practitioners and media enterprises should consult the list published by the ODPC on the countries, territories and specified sectors within that other country and relevant international organisation for which the ODPC has made a decision that an adequate level of protection is ensured.

(c) Transfers on the basis of necessity

Personal data may be transferred to another country or territory on the basis of necessity is only for any of the purposes outlined herein below:

i. for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
ii. for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
iii. for any matter of public interest;
iv. for the establishment, exercise or defence of a legal claim;
v. in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
vi. for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Any such transfer must be done after confirming there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.

(d) Transfer on basis of consent

Transfer of sensitive data on the basis of consent

Personal data can also be transferred on the basis of prior informed consent of the data subjects. Advisedly, this primarily applies as a basis of transfer in the event that none of the other bases of transfer of data discussed hereinabove. Transfer(s) of personal data to another country shall take place only on the condition that the data subject—

i. has explicitly consented to the proposed transfer; and
ii. has been informed of the possible risks of such transfers.

Transfer of sensitive data on the basis of consent

It worth noting that for sensitive data, transferring entities must:

i. Obtain informed consent of a data subject; and
ii. on obtaining confirmation of appropriate safeguards.

However, the ODPC has the residual and overriding power to prohibit, suspend or subject the transfer to such conditions as may be determined in order to protect the rights and fundamental freedoms of data subjects.

The Cabinet Secretary in charge of information, communication, and technology may set out when the processing of personal data may only be effected through a data centre or server located in Kenya. In line with this, Regulation 26 of the Data Protection (General) Regulations, 2021 lists instances where personal data should be processed through a server and data centre located in Kenya or there should be stored at least one serving copy of the concerned personal data in a data centre located in Kenya. The instances are when:

a. administering of the civil registration and legal identity management systems;
b. facilitating the conduct of elections for the representation of the people under the Constitution;
c. overseeing any system for administering public finances by any state organ;
d. running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018;
e. offering any form of early childhood education and basic education under the Basic Education Act, 2013; or
f. provision of primary or secondary health care for a data subject in the country.

Journalists, media practitioners and media enterprises may be engaged in international data transfers where it uses a cloud services provider, internet platform, or mobile phone applications to process personal data. Given this, journalists, media practitioners and media enterprises must ensure compliance with the above-cited conditions.

To determine the appropriateness of the data transfers, media enterprises should undertake a data transfer risk assessment that identifies:

- the type of personal data transferred,
- categories of personal data subject,
- types of entities involved in the transfer,
- Sector in which the transfer occurs,
- purpose of the transfer,
- format of the data,
- method of transfer,
- the technological and organisational security the importer has in place to protect the data,
- whether the data will be stored outside Kenya or whether there is remote access to data stored within Kenya,
- the movement of data when under the control of the importer, which countries the data will be held in,
- the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities
- any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards, and
- the possibility of data being forwarded by the importer to another entity.

6. DATA SUBJECT RIGHTS

Under this section we particularize and discuss the rights of data subjects as provided for under the DPA.

6.1. Right to be informed

This refers to the right to be informed of the use to which personal data is to be put. The DPA sets out what information should be provided to a data subject. A Journalists, media practitioners and media enterprises should inform a data subject of:

(a) the rights of a data subject.
(b) the fact that personal data is being collected.
(c) the purpose for which the personal data is being collected.
(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted.
(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data.
(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data.
(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory.
(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

The above information should be contained in privacy notices drafted by media enterprises respectively and provided to data subjects before their personal data is processed. A privacy notice may be made available in printed form, on posters, on media enterprises websites, on journalists,

media practitioners and media enterprises mobile phone applications, sent via email, or read to the data subject among other options.

6.2. Right to access personal data

This refers to the right to access personal data in the custody of journalists, media enterprises and media practitioners. A data subject may request to access the personal data that journalists, media enterprises and media practitioners have. Such a request may include a request for information on:

(a) the purposes of the processing,
(b) the categories of personal data concerned,
(c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, including recipients in other countries or territories,
(d) where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period, and
(e) where the personal data is not collected from the data subject, any available information as to the source of collection.

It is the right of the data subject to obtain confirmation of how journalists, media practitioners and media enterprises are treating their personal data. Where a data subject wishes to exercise the right to access their personal data, they may make a request under **Form DPG 2** as set out in the First Schedule of the Data Protection (General) Regulations, 2021.

Journalists, media practitioners and media enterprises must comply with the request for access to personal data from a data subject within **seven (7) days** of the request.

6.3. Right to Data Portability

The right to access personal data may be read together with the right to data portability.

A data subject has a right to receive their personal data in a structured and machine-readable format. For example, media enterprises could provide the data in printed format or PDF, Spreadsheet or Word/Document format.

A data subject also has a right to have their personal data transmitted to another data controller or data processor. For example, a data subject can request e-paper and website subscription data transferred to another data controller or data processor for personal use. A second scenario is a data subject may request a media enterprise to transfer video, text, or photos of the data subject to another data controller.

Where a data subject wishes to make a data portability request, they can do so through **Form DPG 4** as set out in the First Schedule of the Data Protection (General) Regulations, 2021. Journalists, media practitioners and media enterprises **have thirty (30) days** to comply with data portability requests at a reasonable cost.

Journalists, media practitioners and media enterprises may however decline to comply with a data portability request where:

(a) processing may be necessary for the performance of a task carried out in the public interest or the exercise of an official authority, or
(b) it may adversely affect the rights and freedoms of others.

Where a journalist, media practitioner or media enterprise declines to comply with the data portability request, they should provide the data subject with reasons in writing.

6.4. Right to object

This refers to the right to object to the processing of all or part of personal data. A data subject may object to the processing of their personal data unless media enterprises demonstrate compelling legitimate interest for the processing that overrides the data subject's interest, or for the establishment, exercise, or defence of a legal claim.

The right to object is an absolute right where the controller/processor intends to use ones personal data for direct marketing purposes. This means such an objection cannot be denied/refused.

Where a data subject wishes to object to the processing of their personal data, they may make a request under **Form DPG 1** as set out in the First Schedule of the Data Protection (General) Regulations, 2021. Journalists, media practitioners and media enterprises should comply with the request for objection within **fourteen (14) days** of the request without charging the data subject any fee.

Journalists, media practitioners and media enterprises may also reject the request for objection and provide reasons for the rejection to the data subject in writing.

6.5. Right to restriction

The right to restriction of processing of personal data means that journalists, media practitioners and media enterprises may at the request of a data subject restrict the processing of personal data where:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling them to verify the accuracy of the data,
(b) personal data is no longer required for the purpose of the processing, unless they require the personal data for the establishment, exercise, or defence of a legal claim,
(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead, or
(d) the data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor override those of the data subject.

For a request to restrict processing, a data subject is to make a request under **Form DPG 1** set out in the First Schedule of the Data Protection (General) Regulations, 2021. Journalists, media practitioners and media enterprises should comply with the request for restriction within **fourteen (14) days** of the request without charging the data subject any fee.

Journalists, media practitioners and media enterprises may reject the request for restriction of processing and provide reasons for the rejection to the data subject in writing.

6.6. Right to correction

The right to correction of false or misleading data includes the right of rectification for inaccurate, outdated, incomplete, or misleading data.

Journalists, media practitioners and media enterprises should ensure that they retain accurate, up to date and complete data. It is for this reason that media enterprises should put in place due diligence measures as far as personal data is concerned.

For a request for rectification, a data subject is to make a request under **Form DPG 3** set out in the First Schedule of the Data Protection (General) Regulations, 2021. The application may be supported by documentation to support the request for rectification. Journalists, media practitioners and media enterprises should comply with the request for correction within fourteen (14) days of the request without charging the data subject any fee. Journalists, media practitioners and media enterprises may reject the request for correction and provide reasons for the rejection to the data subject within seven (7) days.

6.7. Right to deletion

The right to deletion of false or misleading data means that controllers/processors may erase or destroy personal data where it is no longer authorised to retain the data, or the data is irrelevant, excessive or was obtained unlawfully. The right of erasure arises when:

(a) the personal data is no longer necessary for the purpose which it was collected;
(b) the data subject withdraws their consent that was the lawful basis for retaining the personal data;
(c) the data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing;
(d) the processing of personal data is for direct marketing purposes and the individual objects to that processing;
(e) the processing of personal data is unlawful including in breach of the lawfulness requirement; or
(f) the erasure is necessary to comply with a legal obligation.

An erasure request, a data subject is to make a request under **Form DPG 5** set out in the First Schedule of the Data Protection (General) Regulations, 2021. The application may be supported by documentation to support the request for rectification. Journalists, media practitioners and media enterprises should comply with the request for deletion within fourteen (14) days of the request without charging the data subject any fee.

For deletion, journalists, media practitioners and media enterprises may adopt technologies that facilitate deletion of data across multiple platforms.

Journalists, media practitioners and media enterprises may reject the deletion request and provide reasons for the rejection to the data subject. The right of erasure may not apply if data processing is necessary:

(a) to exercise the right to freedom of expression and information,
(b) to comply with a legal obligation,
(c) for the performance of a task carried out in the public interest or in the exercise of official authority,
(d) for archiving purposes in the public interest, scientific research, historical research, or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing, or
(e) for the establishment, exercise, or defence of a legal claim.

6.8. Right to file a complaint

A data subject has a right to file a complaint to the ODPC where they are aggrieved by a decision by journalists, media practitioners and media enterprises relating to their personal data. Under the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 the Data Commissioner may refer a complaint between a data subject and by journalists, media practitioners and media enterprises to mediation, conciliation, or negotiation. The Data Commissioner has published Alternative Dispute Resolution Framework to guide the mediation, conciliation, or negotiation process.

Where the Data Commissioner admits a complaint, the journalists, media practitioners and media enterprises shall be notified of the complaint and shall within **twenty-one (21) days**:

(a) make representations and provide any relevant material or evidence in support of its representations,
(b) review the complaint with a view of summarily resolving the complaint to the satisfaction of the complainant, or
(c) respond with the required information.

The Data Commissioner may carry out investigations on a complaint and inform the data subject and media enterprises of the outcome of the investigations. Upon conclusion of investigations, the Data Commissioner may:

(a) issue an enforcement notice to journalists, media practitioners and media enterprises,
(b) issue a penalty notice imposing an administrative fine where journalists, media practitioners and media enterprises fail to comply with the enforcement notice,
(c) dismiss of the complaint where it lacks merit,
(d) recommend prosecution, or
(e) make an order for compensation to the data subject by journalists, media practitioners and media enterprises.

Under section 63 of the DPA, an administrative fine may be up to five (5) million shillings or in the case of an undertaking up to one (1) per centum of such undertaking's annual turnover of the preceding year, whichever is lower.

Under section 34 (1) (a) of the Media Council Act, No.46 of 2013 a person aggrieved by any publication or conduct of journalists, media practitioners and media enterprises under the DPA may make a written complaint to the Complaints Commission setting out the grounds for the complaint, nature of the injury or damage suffered, and the remedy sought.

Under section 34 (4) of the Media Council Act, No.46 of 2013 a complainant shall disclose to the Commission the complainant's name and address; and other information relating to the complainant's identity that the Commission reasonably requires.

Under section 34 (5) of the Media Council Act, No.46 of 2013 the Commission may keep information provided by a complainant confidential if there are special circumstances or the Commission considers it is in the complainant's interests to do so; or accept an anonymous complaint concerning an issue of public interest, or where no identifiable person or group is affected.

6.9. Right to representation

This refers to the right conferred to a data subject in the case of a minor, to be represented a person with parental authority or by a guardian. Where a data subject has a mental or other disability, another person may be authorised to act as their guardian or administrator.

A data subject may also authorise any personnel to act on their behalf.

7. 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 ensure that journalists, media practitioners and media enterprises have an appreciable level of personal data protection.

7.1. Data Protection Training

Media enterprises should ensure 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, it promotes trust in how media enterprises process personal data, it improves media enterprises' culture of data governance, and keeps personnel up to date with emerging technologies in use for processing personal data. Data protection training will also ensure that personnel are well-versed in cyber-security strategies.

In addition to the training, media enterprises should also constantly sensitise their officers on emerging data governance compliance trends.

7.2. Privacy Assessment

Journalists, media practitioners and media enterprises need to evaluate their level of compliance with the provisions of the DPA. This evaluation is termed as privacy assessment or a readiness assessment. The assessment evaluates whether journalists, media practitioners and media enterprises have undertaken measures that are administrative, legal, technical, policy, economic, and political to comply with the DPA. The assessment will reveal current data protection capabilities.

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 organisation 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.

7.3. Budgeting

Budgeting for data governance compliance should be informed by findings from the privacy/readiness assessment. From the assessment, journalists, media practitioners and media enterprises will be able to determine the resources it requires to effectively build a privacy programme. Resources required to put in place organisational and technical measures to comply with the DPA include finances and personnel. It is important to note that compliance may require additional staff, technology, and infrastructure.

7.4. Assigning Responsibilities

7.4.1. Data Protection Officers

(a) Appointment of a Data Protection Officer: The DPA provides that a data controller or data processor may designate or appoint a Data Protection Officer (DPO). The use of the word 'may'

under the DPA indicates that it is not mandatory for a data controller or data processor to designate or appoint a DPO.

It is advisable for media enterprises to designate DPOs. The designated DPOs may be in house for larger enterprises and external DPOs for medium or small enterprises. Organisations can also have DPOs as external consultants on independent contractor basis. It is highly advisable that the office of the DPO is shielded from interference by having a seamless reporting structure in the organisation's organogram.

Under the DPA, a DPO may be a staff member who may fulfil other tasks and duties as long as they do not result in a conflict of interest with the DPO's tasks and duties.

(b) Qualifications of a DPO: The DPA indicates that a person may be designated or appointed as a data protection officer if that person has relevant academic or professional qualifications, which may include knowledge and technical skills in matters relating to data protection. A DPO ought to have received professional training or certification to act as a DPO.

(c) Role of a DPO

The DPA provides that the DPO shall:

- advise on data processing requirements provided under the DPA or any other written law,
- ensure that the DPA is complied with,
- facilitate capacity building of staff involved in data processing operations,
- provide advice on data protection impact assessment, and
- cooperate with the ODPC and any other authority on matters relating to data protection.

(d) Work plan for the DPO

The DPOs at first instance, shall seek to:

- Understand institutional operations,
- Identify departments to collaborate with,
- Identify departments that process personal data,
- Carry out preliminary privacy assessments,
- Establish a data protection committee,
- Review existing policies on data protection,
- Draft new policies where applicable,
- Draft privacy programme work plan,
- Plan data protection training and sensitisation, and
- Draft budgets for the establishment of a privacy programme,

The DPO appointed or designated by media enterprises needs to work in collaboration with other staff and third-party service providers.

7.4.2. Duties and Responsibilities of other Officers

Media enterprises shall ensure the allocation of duties and responsibilities to other Officers as follows:

(a) **Departmental Heads:** Each departmental head shall ensure compliance with the DPA within their department. Secondly, the departmental head shall ensure close collaboration with the DPO on matters relating to personal data protection within the department.
(b) **Chief Finance Officer:** The chief finance officer in collaboration with the DPO shall ensure that adequate financial resources are allocated to the privacy programme.
(c) Information Security Officer: The information security officer shall collaborate with the DPO to identify risks, vulnerabilities, and incidents that may lead to personal data breaches.
(d) **Human Resources Manager:** The human resources manager shall ensure all staff receive sensitisation training on compliance with the DPA. Secondly, the human resource manager shall initiate administrative proceedings where staff wilfully or negligently occasion non-compliance with the DPA.
(e) **Legal Manager:** The Legal Manager shall monitor any law reforms and court decisions relating to personal data protection. Secondly, they shall collaborate with the DPO and relevant departmental heads in the negotiation and drafting of contracts or agreements that require the processing of personal data.
(f) **Employees:** Employees should ensure they participate in data protection sensitisation sessions. Secondly, they should ensure that their day-to-day activities which include processing of personal data comply with the DPA. Thirdly, they should identify and report any risks, vulnerabilities, and incidents relating to personal data processing to their departmental heads and or the DPO.

7.5. Data Inventories

A data inventory is a list of all the personal data that journalists, media practitioners and media enterprises process. A data inventory is the systematic catalogue of the data assets. It provides a comprehensive picture of data resources, including how they are gathered, stored, accessed, and used. By creating and maintaining a data inventory, an organisation can gain a better understanding of their data environment and identify potential risks such as data breaches or failure to comply with the DPA.

A data inventory includes information about the type of data, its location, how it is used, who has access to it, and how it is secured. A data inventory will be critical in:

- Crafting an appropriate and comprehensive data protection strategy,
- Determination of which regulations apply to specific personal data processing operations,
- Classification of personal data (e.g. sensitive data),
- Ensuring data minimization,
- Carrying out data protection impact assessments,
- Registration with the ODPC,
- Responding to data subject requests or complaints,

- Responding to incidents and breaches that relate to personal data, and
- Ensuring effective use of personal data.

Due to the high volume of personal data processed, it is advisable that an organisation should use technology to formulate a data inventory. Below is an example of a data inventory for an identified activity.

Example	
Applicable Law	
Data subjects	
Data elements collected	
Sensitive data elements	
Mode of collection	
Legitimate use	
Departments handling the data	
Technology in use	
Location	
Risks	
Risk mitigation	
Third parties processing the data	
Retention period	

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

7.6. Data Retention

One of the key components of the data inventory example above is 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.

Journalists, media practitioners and media enterprises shall draft data retention schedules for different kinds of personal data depending on the above.

Sample data retention table:

Record Type	Retention Period	Disposition
By-line lists	Permanently	Archive
Camera footage	Permanently	Archive
Clip libraries	Permanently	Archive
Website Articles	Permanently	Archive
e-Paper Materials	Permanently	Archive
Press releases	Permanently	Archive
Social media posts	5 years	Deletion
Website analytics	5 years	Archive
Active user login details	Permanently	Shred/encrypt user data after 7 years of inactivity
Obituaries	10 years	Deletion

7.7. Data Protection Policies

Media enterprises shall formulate in-house data protection policies that are inward-looking. The data protection policies should include:

(a) the nature of personal data collected and held,
(b) how a data subject may access their personal data and exercise their rights in respect to that personal data and any exemptions applicable,
(c) complaints handling mechanisms,
(d) lawful purpose for processing personal data,

(e) obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients,
(f) the retention period and schedule, and
(g) the collection of personal data from children, and the criteria to be applied.

In addition to the listed issues, the data protection policies may also include:

- Definitions of key data protection terms,
- The roles and responsibilities of personnel,
- Procedures for collecting personal data from data subjects, including obtaining consent and providing notice to data subjects about the purposes for which their data is being collected,
- Procedures for processing personal data, including data minimisation, accuracy, storage limitation, and security measures,
- Security measures in place to protect personal data from unauthorised access, use, or disclosure, including encryption, access controls, monitoring, and incident response procedures,
- Staff data protection training and sensitisation, and
- Procedures for monitoring compliance with the policy, conducting audits, and enforcing the policy through disciplinary actions if necessary.

7.8. Privacy Notices

Privacy notices are outward-looking stemming from the duty to notify data subjects of personal data processing operations. The notification is usually in the form of a privacy notice. The DPA sets out what information should be provided to a data subject through a privacy notice as follows:

(a) the rights of a data subject specified,
(b) the fact that personal data is being collected,
(c) the purpose for which the personal data is being collected,
(d) the third parties whom personal data has been or will be transferred to, including details of safeguards adopted,
(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data,
(f) a description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data,
(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory, and
(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

The above information should be contained in a privacy notice drafted by media enterprises and provided to data subjects before their personal data is processed. The privacy notice may be made available in printed form, on posters, on websites, on mobile phone applications, sent via email, or read to the data subject among other options.

7.9. Data Subject Rights Management

Journalists, media practitioners and media enterprises should set up a data subject rights management framework. This framework will respond to data subject requests made to a media enterprise. The framework will include:

(a) Designation of officers to oversee managing data subject rights and data subject requests. Ideally, the officers in charge will be the DPOs.
(b) Providing notices to data subjects.
(c) Providing access to data subjects.
(d) Setting up a verifiable process to record consents of data subjects.
(e) Verification of the identity of data subjects when they make requests.
(f) Responding to data subject requests:
    i. Understanding the request.
    ii. Discovering what personal data, the organisation holds in relation to the data subject.
    iii. Consultation with relevant departments.
    iv. Informing and collaborating with third parties who have access to the personal data in question.
    v. Informing the data subject of the decision on the request.
(g) In the event of a complaint by a data subject, media enterprises should at first instance seek to address the complaint through negotiation with the data subject.

7.10. Data Protection Impact Assessment

Data protection impact assessments (DPIA) should be carried out where a personal data processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context, and purposes.

The process to carrying out a DPIA involves:

1) Identify the need for a DPIA This is pegged on the data risk level in the organisation. Processing operations that may be high risk to the rights and freedoms of data subjects include:

(a) automated decision making with legal or similar significant effect that includes the use of profiling or algorithmic means or use of sensitive personal data as an element to determine access to services or that results in legal or similarly significant effects;
(b) use of personal data on a large-scale for a purpose other than that for which the data was initially collected;
(c) processing biometric or genetic data;
(d) where there is a change in any aspect of the processing that may result in higher risk to data subjects;
(e) processing sensitive personal data or data relating to children or vulnerable groups;

(f) combining, linking or cross-referencing separate data sets where the data sets are combined from different sources and where processing is carried out for different purposes;
(g) large scale processing of personal data;
(h) a systematic monitoring of a publicly accessible area on a large scale;
(i) innovative use or application of new technological or organisational solutions; or
(j) where the processing prevents a data subject from exercising a right.'

2) Describe the personal data processing. Indicate the steps in the collection, storage, transformation, analysis, and dissemination of data.

For example, a data subject personal data shall be collected using web cache, prompts, push notifications, a website form, interviews, surveys, observation, video/photo recording, studio Interviews, secondary data collection e.g. Government reports, court documents and publicly accessible data.

Identify and list the data elements being processed and whether they include sensitive personal data.

3) Consult. Involve all departments involved in the data processing the DPIA is being undertaken.

4) Assess necessity and proportionality. Identify the lawful or legitimate reasons for processing the personal data in question.

For example, in cases where a journalist working on an exposé needs to reveal links between different players (data subjects) implicated in an alleged scandal or crime, e.g. where a public official has listed family/allies as directors in a firm cited in an investigative report.

5) Identify and assess risk. In this step, identify and assess the risks associated in the personal data processing operations being assessed.

Some of the risks may include surveillance, leaks, and possible bias, due to technology or software limitations, where Artificial Intelligence is deployed in analysing data.

Indicate whether the risks would result in high risk to the rights and freedoms of the data subjects in question. The risks could be for example, risk to the right to privacy and equal protection.

6) Identify measures to mitigate risk.

Examples of strategies to mitigate risks include implementing appropriate security controls. Security controls may involve access control, encryption, firewalls, CCTV, and intrusion detection, and prevention systems.

Mitigation strategies may also include data protection training or sensitisation for employees, reviewing data protection policies, regular assessments/reviews, executing contracts with data processors etc.

7) Incorporate the issues identified into the DPIA template set out in the Third Schedule of the Data Protection (General) Regulations,2021.

8) Sign off, record outcomes, and integrate outcomes into an implementation plan.

9) Consultation with ODPC.

The DPA requires an organisation to consult the Data Commissioner prior to a personal data processing operation if the data protection impact assessment indicates that the processing of the data might result in high risk to the rights and freedoms of the identified data subjects. An organisation shall submit the data protection impact assessment report to the Data Commissioner.

An organisation is required to consult the Data Commissioner on the data protection impact assessment report prior to processing of personal data. The submission of the report to the ODPC shall be done **sixty (60) days** prior to the processing of the data in question.

Where the Data Commissioner identifies that the personal data processing operations may cause harm to the data subjects, or violate provisions of the DPA, the Data Commissioner may provide written advice.

If an organisation does not receive communication from the Data Commissioner within **sixty (60) days** from submission of the data protection impact assessment report, they may commence the personal data processing operations.

10) Keep data processing operations under review. Media enterprises shall constantly review their data processing operations and make further consultations to the Data Commissioner where necessary.

7.11. Online Archives

Journalists, media practitioners and media enterprises shall ensure retention and publication of a full online news archive. Where possible, stories that are later shown to be inaccurate or unfair should be linked to subsequent corrections.

7.12. Confidential Sources

Journalists, media practitioners and media enterprises naturally protect the identity of their sources. However, a data subject of a story can request for access to information a journalist has on them.

There is need for clarity on this so that reporter's privilege is safeguarded as has been the practice in journalism. A request for information needs to be weighed against the obligation on the part of the journalists to protect confidential sources.

7.13. Information Security

Journalists, media practitioners and media enterprises shall ensure a high level of security, both physical and online security for the data that it holds. The respective organisation shall also incorporate cyber hygiene training into its data protection training and sensitisation of staff.
Tips for ensuring a heightened level of security include:

(a) Ensure physical security: use CCTV, guards, lock and key, safes, access control, adopt a clear desk policy etc.
(b) Have an ICT policy.
(c) Have a device use policy.
(d) Ensure security of WIFI and designate WIFI for staff and WIFI for use by visitors.
(e) Keep all software or platforms in use up to date and ensure devices only use approved software and platforms.
(f) Monitor staff accounts for any suspicious activity that may put data at risk.
(g) Ensure email security.
(h) Verify information and intended recipients before sending emails.
(i) Beware of online scams.
(j) Block downloads from untrusted sites and platforms.
(k) Have a cloud security policy.
(l) Have a working remotely policy.
(m) Ensure network infrastructure security.

7.14. Security Audits and Assessments

To ensure heightened security, media enterprises should undertake periodic security audits and assessments which will involve:

(a) Review of policies and procedures: review policies and procedures related to data security, such as access controls, data classification, incident response, and data retention.
(b) Evaluating technical controls: evaluate controls, such as firewalls, intrusion detection and prevention systems, antivirus software, and encryption to identify any weaknesses or vulnerabilities in the organisational technical defences.
(c) Conduct vulnerability scans and penetration tests: these will identify vulnerabilities and weaknesses in systems and networks. This can include testing for common vulnerabilities, such as unpatched software, weak passwords, and misconfigured systems.
(d) Conduct interviews and surveys: interviews with staff and surveys of employees may provide insight into the organisational culture and attitudes towards data security. This can help identify areas where training or awareness-raising may be needed.
(e) Analyse incident response procedures: evaluate incident response procedures to ensure that they are effective and up to date. This may also include reviewing incident reports and conducting a table top exercise to test responses to a simulated data breach.
(f) Report and remediation: the assessment should conclude in a report that identifies any vulnerabilities and risks identified, as well as recommendations for remediation.

7.15. Incident and Data Breach Management

The DPA requires for notification and communication in case of a personal data breach. 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 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.

Under Regulation 38 of the Data Protection (General) Regulations 2021 a notification to the Data Commissioner shall include the information in the table below:

Incident and data breach register	
Breach ID	
When organisation became aware of breach	
Date breach occurred	
Time breach occurred	
Classes of data compromised	
How breach occurred	
Nature of breach	
Cause	
Who is responsible for the breach	

Data subjects affected	
Risk and potential harm to data subjects	
Action to be taken by data subjects to reduce harm	
Remediation measures undertaken	
Notification to data subjects	
Notification to ODPC	
Remediation measures – long term	
Lessons learnt	
Contact of DPO	

Journalists, media practitioners and media enterprises may adopt the following strategy to deal with incidents and data breaches:

- Create an inventory with at-risk assets.
- Ensure compliance with the DPA.
- Develop a Disaster/ Incident Recovery Plan and Procedures whose objective shall be to maximise the effectiveness of contingency operations.
- Have incident response stakeholders meet on a regular basis to identify potential risks.
- Assign roles and responsibilities:
    - DPO: incident response planning, risk assessments, compliance monitoring, notifying the Data Commissioner and law enforcement if required.
    - IT department: investigating the breach, determining the extent of the damage, and taking steps to mitigate the effects of the breach. IT should also identify vulnerabilities that led to the breach and develop a plan to prevent similar incidents in the future.
    - Legal department: reviewing contracts and agreements with vendors and partners to identify any potential liability issues.
    - Human resources department: communicating the breach to employees, and contractors.
    - Public relations department: developing messaging and communication plans for external stakeholders.
    - Third party vendors: where the data breach involves third-party vendors, they should be involved in the response strategy to help assess the impact of the breach and take steps to mitigate the effects.
- An organisation may seek external advice to confirm you have the right approach to the data breach.

- Conduct practice drills and hold table top exercises with all stakeholders to test response plans.
- Document a reporting process if a data breach occurs.
- Learn from each incident and update the response plan accordingly.

Journalists, media practitioners and media enterprises will apply the provisions of the Computer Misuse and Cybercrimes Act, 2018 alongside the provisions provided above in Incident and Data Breach Management.

7.16. Data Sharing Agreements

Where journalists, media practitioners and media enterprises share data with each other, they ought to enter into data sharing agreements which will include clauses on:

(a) Scope and purpose of data sharing.
(b) Compliance with relevant statutory requirements.
(c) Data use.
(d) Confidentiality of the data.
(e) Security of the data.
(f) Incident and breach management.
(g) Data ownership.
(h) Intellectual property.
(i) Liability of parties.
(j) Data access.
(k) Data retention period.
(l) Destruction of data.
(m) Termination.
(n) Return of data.
(o) Amendment of the agreement.
(p) Dispute resolution.

7.17. Vendor Risk Assessment

When onboarding vendors through the public procurement processes, it is important that journalists, media practitioners and media enterprises expressly indicate whether the vendor will be processing any personal data for/ or on behalf of the organisation. In this process, the organisation shall inquire if:

- The vendor has put in place measures to comply with the DPA.
- The vendor will process personal data for/or on behalf of the organisation.

Where the above inquiry is in the affirmative, journalists, media practitioners and media enterprises shall enter into contracts with their respective vendor. Such a contract will in most cases be a data controller vs data processor contract, and should contain the following information:

a) processing details including—
   (i) the subject matter of the processing,
   (ii) the duration of the processing,
   (iii) the nature and purpose of the processing,
   (iv) the type of personal data being processed,
   (v) the categories of data subjects, and
   (vi) the obligations and rights of the parties.
b) instructions of the organisation.
c) duty of the data processors (vendor) to obtain a commitment of confidentiality from any person or entity that the data processors (vendor) allow to process the personal data.
d) security measures subjecting the data processor (vendor) to appropriate technical and organisational measures in relation to keeping personal data secure.
e) provision stipulating that all personal data must be permanently deleted or returned on termination or lapse of the agreement, as decided by the data controller, and
f) auditing and inspection provisions by the organisation.

For vendor risk assessments journalists, media practitioners and media enterprises should:

- Continuously review vendor compliance with the DPA,
- Have an up-to-date inventory of vendors involved in processing of personal data, and
- Have vendor ratings or scores.

7.18. Digital Platforms

The DPA requires every data controller/processor to implement appropriate technical and organisational measures which are designed to implement the data protection principles in an effective manner; and to integrate necessary safeguards for that purpose into the processing.

Journalists, media practitioners and media enterprises shall implement elements of privacy by design and by default as set out in Part V of the Data Protection (General) Regulations, 2021 to ensure lawfulness of processing personal data, transparency, purpose limitation, integrity, confidentiality, availability, data minimisation, accuracy, storage limitation, and fairness in processing.

Journalists, media practitioners and media enterprises shall ensure privacy by design and by default for their mobile phone applications and digital platforms. Key considerations in ensuring privacy by design and by default for mobile phone applications and platforms include:

- **Data minimisation:** collect and retain only the minimum amount of personal data necessary to provide the services requested by customers. Unnecessary data collection should be avoided.
- **Consent and transparency:** obtain clear and informed consent from customers before collecting their personal data.
- **Permissions:** mobile phone application shall only request permissions that are necessary for the application's core functionality.

- **Secure applications and platforms:** adopt robust security measures to protect a customer's personal data.
- **User control and access:** provide users of their applications and platforms with control over their personal data. This will be achieved through easy access to update or delete user information where applicable.
- **Default privacy settings:** configure privacy settings to their most privacy-friendly options by default.
- **Cookie banners:** DPA requires that media enterprises must inform users about their data protection and privacy practices through cookies and obtain user consent. The banner informs users that the website uses cookies and seeks their consent before collecting their personal data**.**
- **Terms and conditions for use:** a media enterprise shall on its digital platforms set out the guidelines on user accounts, user conduct, intellectual property, content usage, third-party links, disclaimer, warranties, liability, governing law, changes to terms, and contact information.

7.19. Direct Marketing

The DPA provides for principles to be complied with when engaging in direct marketing and commercial use of personal data. To ensure compliance with the DPA, journalists shall adopt the following strategies:

- **Data brokers:** journalists, media practitioners and media enterprises shall not procure or obtain personal data from data brokers who have not obtained the personal data in compliance with the DPA.
- **Obtain consent:** obtain valid and informed consent from individuals before engaging in direct marketing activities.
- **Opt-in mechanism:** implement an explicit opt-in mechanism where individuals expressly indicate their willingness to receive marketing communications.
- **Opt-out mechanism:** provide clear and easy-to-use unsubscribe options in all marketing communications. Honour opt-out requests promptly and ensure that individuals are removed from marketing lists as requested.

7.20. Record Keeping

Journalists, media practitioners and media enterprises shall ensure it keeps comprehensive records of:

(a) Training and sensitisation of employees on data protection.
(b) Data policies formulated, reviewed, and enacted.
(c) Privacy notices formulated, reviewed, and enacted
(d) Consent forms (where applicable) formulated, reviewed, and executed.
(e) Resources allocated to compliance with the DPA: financial, human resources, equipment, etc.
(f) Appointment of data protection officers.

(g) Data inventory.
(h) Inventory of reasons for processing personal data.
(i) Inventory of assets used to process personal data.
(j) Inventory of third parties with whom personal data is shared.
(k) Strategies on ensuring correctness and security of data.
(l) Complaints by data subjects: complaints made, complaints resolved, and time taken to resolve the complaints.
(m) Requests by data subjects: requests made, requests resolved, requests denied, and time taken to resolve the requests.
(n) Data breaches and incident management: number of incidents, number of notifications to ODPC, time taken to identify breaches and incidents, and number of incidents fully addressed.

The above records shall also constitute metrics for monitoring and evaluating the level of compliance with the DPA.

7.21. Registration with ODPC

Journalists, media practitioners and media enterprises shall ensure that they are registered with the Office of the Data Protection Commissioner. The application form is available at the Office of the Data Protection Commission (odpc.go.ke). Information required on the registration portal includes:

(a) Particulars and contacts of the DPO,
(b) Description of personal data processed,
(c) Description of the purpose for processing personal data,
(d) Description of sensitive personal data processed,
(e) Description of the purpose for processing sensitive personal data,
(f) Description of risks and vulnerabilities related to data processing, and
(g) Description of measures to mitigate risk and vulnerabilities related to data processing.

8. IMPLEMENTATION OF THE GUIDE

To implement this guide, journalists, media practitioners and media enterprises will be required to:

(a) Familiarise themselves with this Guide.
(b) Sensitise or train employees on data governance as provided for under this Guide.
(c) Ensure that this Guide informs in-house policies and procedures.
(d) Implement monitoring, evaluation, and learning strategies for data governance.
(e) Put in place review and accountability measures.
(f) Ensure continuous improvement of data governance practices.

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