REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes - Processing for Journalistic Purpose

2025

TABLE OF CONTENTS

FOREWORD

Article 33 of the Constitution of Kenya, 2010 guarantees the freedom of expression, including freedom of the media, while Article 31 secures the right to privacy. The Data Protection Act, 2019 was enacted to operationalise Article 31, ensuring that all personal data is in accordance to the principles of data protection. For media practitioners, authors, and artists, this dual framework presents both an opportunity and a responsibility: to contribute to democratic discourse, cultural enrichment, and public accountability, while safeguarding the dignity and rights of individuals.

The use of personal data in journalism, literature, and artistic work serves vital public purposes, including informing society, exposing wrongdoing, advancing knowledge, and celebrating creativity. However, it also presents privacy challenges ranging from intrusive reporting and misuse of sensitive data to the handling of vulnerable groups such as children and persons with diminished capacity. In the digital age, the risks are magnified by the ease with which recorded information can be published, replicated, and disseminated globally.

This Guidance Note provides clarity on the lawful bases for processing personal data for journalistic, literary, and artistic purposes. It outlines the scope of allowable exemptions under Section 52 of the Data Protection Act, emphasizing that these exemptions are not absolute and must satisfy the specific conditions set out in the legislation. It further outlines compliance obligations such as registration, transparency, safeguards for sensitive data, data minimisation, accountability, and the conduct of Data Protection Impact Assessments.

The Office of the Data Protection Commissioner (Office) emphasizes that media freedom and data protection are not mutually exclusive. Responsible processing of personal data is essential to sustaining public trust, protecting vulnerable persons, and promoting ethical standards in journalistic, literary and artistic practice. Compliance with this Guidance Note will enable practitioners to balance the public's right to know with the individual's right to privacy, thereby advancing democratic values while upholding the law.

It is my expectation that this Guidance Note will serve as a vital reference for journalists, editors, authors, artists, and media organisations. By following its principles, they will contribute to a media and cultural environment that is not only vibrant and diverse, but also uphold the individual's right to privacy and be accountable to the people of Kenya.

Immaculate Kassait, MBS
Data Commissioner

DEFINITIONS

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

"Anonymisation" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

"Alternative methods" means the use of covert news gathering techniques, including but not limited to hidden cameras or microphones;

"Child" means an individual who has not attained the age of eighteen years

"Data" means information which –

a) is processed using equipment operating automatically in response to instructions given for that purpose;
b) is recorded with the intention that it should be processed using such equipment.
c) is recorded as part of a relevant filing system.
d) where it does not fall under paragraphs (a), (b), or (c), forms part of an accessible record; or
e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

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

"Media Practitioner" (for this guidance notes) means any person who practices their trade in journalistic, literary and artistic work and includes but is not limited to, media content-hosts, continuity announcers, anchors, presenters, photojournalists, camerapersons, graphic designers, content producers, a publisher engaged in publication and the manager or proprietor of a magazine or broadcasting station.

"Office" means the Office of the Data Protection Commissioner as established in section 5 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"**Pseudonymisation**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"Public interest" concerns matter which may reasonably be judged to have an impact on the population as a whole, or groups of citizens. It includes but is not limited to detecting or exposing crime or serious impropriety, corruption or professional incompetence that affects members of the public; protecting public health or safety; or preventing the public from being misled by an action or statement of an individual or organisation or any other situation that may be determined from time to time by the media council.

"Public figure" refers to any person who occupies a position or office through which they regularly interact with citizens personally or through the media, and whose name and/or appearance are known to significant numbers of persons with whom they have no personal relationship.

"Regulations" means the Data Protection (General) Regulations, 2021; the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021; and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

"Journalistic purposes" means the collection, processing, and intended dissemination of information to the public through any means, with the intent of publication and contributing to public debate, informing society, holding powers accountable, or providing cultural, educational, or social value.

"Journalist" refers to any person recognised as such by the Media Council of Kenya upon fulfilling the Council's accreditation criteria.

"Literary Purposes" - means, irrespective of literary quality, novels, stories and poetic works, plays, stage directions, film sceneries and broadcasting scripts, textbooks, treatises, histories, biographies, essays and articles, encyclopedias and dictionaries, letters, reports and memoranda, lectures, addresses and sermons, charts and tables, computer programs; and tables and compilations of data including tables and compilations of data stored and embodied in a computer or a medium used in conjunction with a computer

"Artistic work" means a variety of creations, regardless of artistic quality, including paintings, drawings, etchings, lithographs, woodcuts, engravings, and prints. It also includes maps, plans, and diagrams; sculptures; photographs that are not part of audio-visual works; architectural designs in the form of buildings or models; and works of artistic craftsmanship that are pictorial in nature.

THE OFFICE

The Office of the Data Protection Commissioner is a government agency established to protect the privacy and security of personal data in our increasingly digital world. The Office is mandated to oversee the implementation and enforcement of the Data Protection Act, 2019, which regulates the processing of personal data by both private and public organisations in Kenya.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organisations respect their privacy rights. The Office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches, and imposing sanctions on entities that violate data protection laws. In addition, the Office is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the Office is a critical institution in maintaining trust and confidence in our data-driven society.

The Office of the Data Commissioner is uniquely positioned to facilitate both the government and private sector entities in achieving the Government's strategic goals under the "Bottom-Up Economic Transformation Agenda" and its digital superhighway initiative. As the digital landscape continues to expand, the need for robust data protection mechanisms becomes increasingly paramount. The Office, with its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation. Kenya remains at the forefront of digital transformation while upholding stringent data protection standards. The Office serves as a key stakeholder and regulator in guiding the nation's digital journey, ensuring that as we advance technologically, the rights and privacy of individuals are safeguarded.

INTRODUCTION

The processing of personal data for journalistic, literary, and artistic purposes is governed by the Media Council Act, 2013, the attendant regulations, the Data Protection Act, 2019, the Copyright Act, and other applicable regulations. To support compliance with the Act and the rules, the Office has developed this guidance note for such processing. This guidance aims to give effect to Article 31 (right to privacy) and Article 33 (freedom of expression) of the Constitution of Kenya, by clarifying the balance between freedom of expression and personal data protection in journalistic, literary, and artistic activities. This guidance note outlines the compliance requirements and provides information on the interpretation and implementation of the Act and the regulations as they relate to processing personal data for journalistic, literary, and artistic purposes.

While the Act includes exemptions for journalism, literature, and art, it's essential to recognize that not all data processing in these categories automatically qualifies for the exemptions under Section 52. Such exemptions often follow a rigorous assessment of the public interest involved. This assessment evaluates whether the need to inform the public and contribute to democratic discourse outweighs the potential impact on individuals' rights to privacy. Thus, the exemption provided in the Act is not absolute.

It is essential to recognize that even when certain data processing activities do not meet the stringent criteria for public interest exemptions, they can still be classified as being undertaken for journalistic purposes. Therefore, Media practitioners must reasonably and responsibly research and present it in a way that complies with the standard provisions of the Act.

PRIVACY CONCERNS

Privacy concerns in the media realm are multifaceted, encompassing traditional practices and digital challenges. With increased journalism's reliance on digital platforms, protecting individuals' rights amid algorithmic curation and data monetization is crucial, requiring ongoing adaptation to ensure responsible reporting while upholding free speech principles.

Here are some of the key privacy concerns in this sector: -

Private life disclosure: During their business, media practitioners may disclose intimate private matters of an individual. Journalists must carefully weigh the relevance of disclosing individuals' private information, considering whether it contributes to the public interest. Generally, pictures and information of a purely personal nature are not considered to contribute to a debate of public interest.

Public Figures: While private individuals unknown to the public may seek privacy protection, public figures are often subject to a different standard. Nonetheless, even public figures retain a reasonable expectation of privacy in purely private matters. Intrusion into their private lives must be justified by a clear public interest, such as exposing hypocrisy or criminal behavior. The public's right to know must outweigh the individual's privacy rights, and the extent of intrusion should be proportionate to the public interest served.

Voluntary disclosure: For data subjects, voluntary disclosure of personal information might nevertheless weaken the degree of protection to which that person is entitled.

Example

Mti Moja, a social media influencer, posts his exorbitant lifestyle on his platforms. A journalist wrote an article on him (accompanied by photographs) referring to his extravagant financial difficulties and exorbitant tastes. Mti Moja claimed a violation of privacy, without success, since he had already disclosed information about the lavish lifestyle on social media, from which the journalist drew information.

Vulnerable Groups: Privacy concerns arise when reporting on vulnerable groups. Vulnerable groups should be given greater protection due to their limited or impaired capacity to provide informed consent.

Cybersecurity breaches: Media practitioners can be vulnerable to cybersecurity breaches, which can expose users' personal data, including confidential sources, and leave them vulnerable to harm, identity theft, and other forms of fraud.

Sensitive Categories of Data: Mishandling or publication of sensitive personal data can infringe upon privacy rights, causing harm to individuals and undermining trust in the media.

Methods of obtaining information: Investigative journalism may necessitate alternative means of obtaining information. Such methods must be justified in the public interest and adhere to the Media Council of Kenya's codes of conduct and data protection laws.

Investigative Journalism: While investigative journalism may require the collection of personal data without consent, this should be guided by public interest and necessity, subject to proportionality and editorial accountability.

LEGISLATIVE FRAMEWORK

The processing of personal data for journalistic, literary, and artistic purposes in Kenya is governed by:

The Constitution of Kenya 2010

a) **Article 31 (c) and (d)** guarantee the right to privacy regarding information relating to individual's family or private affairs unnecessarily required or revealed, or that of their communication, infringed**.**
b) **Article 33** guarantees freedom of expression, which includes freedom to seek, receive, and impart information and ideas.
c) **Article 34** provides for freedom of the media, which guarantees freedom and independence of electronic, print, and all other types of media, as the services are critical in a democratic society.

Data Protection Act, 2019 - The Act provides for a lawful basis of processing Journalistic, literary, art, or scientific research. Processing for journalistic purposes can be exempted from complying with some provisions of the Act based on the nature and purpose of the publication.

The Media Council Act of 2013 gives effect to Article 34(5) of the Constitution by establishing the Media Council of Kenya to set media standards and ensure compliance with those standards as set out in Article 34(5) of the Constitution and for connected purposes.

The Code of Conduct for Media Practice 2025 gives effect to the Media Council Act of 2013 and provides guidelines on the code of practice for journalists.

The Copyright Act, 2001 (revised 2022) provides for the definitions of what may be regarded as literary or artistic material.

The Access to Information Act, 2016 stipulates conditions for the fulfilment of the right to access to information that may include information about a person, i.e., personal data.

Notwithstanding the list of Acts, the forms of expression, particularly the boundaries, are not regulated solely through legal provisions but also subject to ethical considerations and a code of practice. The understanding of the balance between freedom of expression and privacy rights can be found in the Constitution of Kenya, as well as in universal human rights standards.

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

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

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

Media Council of Kenya Codes of Practice and Ethics.
Provide guidelines for responsible journalism by promoting accuracy, fairness, integrity, and respect for privacy and human dignity. They require journalists to verify facts, avoid bias and conflicts of interest, protect sources, and refrain from spreading hate speech or discrimination, ensuring ethical and accountable media practice in Kenya.

PRINCIPLES OF DATA PROTECTION

6.1 Lawfulness, Fairness, and Transparency

Media practitioners must act lawfully, fairly, and transparently, documenting a lawful basis and, where appropriate, obtaining consent.

The principle of transparency requires media practitioners to be open and honest in notifying data subjects of their identity and the purpose of processing, unless this is not practicable.

This principle, therefore, calls for media practitioners, whenever practicable, to provide data subjects with extensive information, including their rights, contact details, sources, retention period, purpose of processing, categories, and recipients. However, a specific exemption applies in a journalistic context where such notification (transparency) would defeat the purpose of processing (e.g., investigative journalism), provided that a substantial public interest justification exists (Section 52 (1)(b)(c) read with 52(2) and 25(a).

As such, where covert methods of data collection (e.g., hidden cameras, undercover reporting) may be justified (there is a compelling public interest), media practitioners must justify that no less intrusive alternative methods exist. The method is proportionate to the harm being exposed. Such practices should be documented and reviewed internally to ensure accountability.

The principle of fairness is based on the notion of proportionality; for example, a journalist may evaluate the need to broadcast some aspects of a data subject and eliminate details about their family affairs in the published content. In applying this principle (fairness), if the only reason for the intrusion of privacy is curiosity, and it does not carry any real value, such publication of private information is not justified. This invasion contradicts the fundamental values of privacy, freedom, autonomy, and dignity.

Example:
HabariMedia, a prominent television station in Kenya, offers a digital streaming service featuring live broadcasts and on-demand content through its website and mobile app. For subscribers, the station relies on explicit consent to collect personal data, such as email addresses and preferences. In contrast, for suppliers and employees, data processing is based on the performance of a contract.
HabariMedia provides clear information about how user data is used, informing subscribers that their data may be used to enhance content recommendations and ensuring that personal data is not used for unrelated purposes without further consent. The station also publishes an easily accessible privacy policy that details data collection, usage, and user rights, allowing both subscribers and suppliers to manage their data preferences. Through these practices, HabariMedia exemplifies lawfulness, fairness, and transparency, while fostering trust with users and suppliers.

Example:
Mwandishi undertakes a project to write a biography of a prominent politician, aiming to capture their life story and contributions to the nation.
To demonstrate lawfulness, Mwandishi obtains explicit consent from the politician before collecting personal information and anecdotes. The politician is fully informed about how their experiences will be represented and published, ensuring compliance with data protection regulations.
The writing process is transparent and respectful. Mwandishi communicates the objectives of the biography and the criteria for including personal stories, allowing the politician to provide input on how they wish their narrative to be portrayed. This approach ensures that the politician's perspective is honored and that they feel comfortable with the representation of their life.
Transparency is further emphasized through a detailed agreement that outlines the project's terms. This includes how the biography will be distributed, the intended audience, and the rights the politician retains over their personal stories.

By adhering to these principles, Mwandishi fosters trust with the politician while creating a meaningful biography that honors their contributions and resonates with the public.

6.2 Purpose Limitation

The purpose limitation principle is a crucial aspect of data protection for processing of personal data for journalistic, literary and artistic purposes. This principle requires media practitioners to ensure that personal data is collected for explicit, specified and legitimate purposes, and must not be used for purposes other than those specified at collection without the data subject's consent. To contextualize, this means that they should not use information for non-journalistic purposes. However, they can still re-use information for other stories in future or keep it as a general journalistic research archive as keeping a news archive is part of the end-to-end process of journalism, so there is no change in purpose.

If a media practitioner is using data for a purpose that is different from the initial purpose at the point of collection or which would have an unjustified impact on the data subject(s), consent from data subjects should thus be considered.

Example:
Mwanahabari, a freelance journalist, is documenting the nightlife in Nairobi city. In her reporting, Mwanahabari conducts interviews with party revelers who frequently go out to a popular club in Nairobi to gather information for her article. In doing so, Mwanahabari must use the personal data she collects solely to produce her journalistic piece. She cannot share the personal data with third parties, unless prior consent or other lawful basis exists, or use it for any other unrelated purposes, such as direct marketing.

6.3 Accuracy

Media practitioners must take reasonable steps to verify the correctness of personal data before publishing it. Further, they should also take particular care to distinguish between facts, opinions, and speculation to avoid any undue harm to the privacy of any individual.
In other words, you will need to assess the personal data required to report news or stories and balance it against the level of intrusion into the life of the data subjects and the potential harm this may cause.

Example:
Magazetini, an online news outlet, publishes stories sourced from freelance writers. To ensure the accuracy of personal information in the stories, Magazetini has introduced a pre-publishing checklist for content writers to follow, which helps remove errors, inconsistencies, and biases. Additionally, it has employed a fact-checker to verify the authenticity of the data and cross-check it against multiple reliable sources. Magazetini has adopted a policy of not publishing stories [or news items] that contain unverifiable personal data.

6.4 Data Minimization

Data minimization is a critical aspect of data protection for processing personal data for journalistic, literary, and artistic purposes. This principle speaks on the processing of personal data to only what is necessary for a specific purpose.
You should collect personal data that is adequate, relevant, and limited to the purposes intended. Avoid collecting excessive information that may be unnecessary but gather enough information for their journalistic purposes.
The following specific considerations can assist media practitioners in complying with this principle;

a) Only collect personal data that is relevant in fulfilling your journalistic activities and wider journalistic purpose.

Example:
Mwanahabari, a journalist is tasked with collection of public views regarding a contentious bill on deforestation in the country. In interviewing any citizens, Mwanahabari must ensure that she only requests for the individuals giving their views to state their names. In the event that Mwanahabari requests for identification numbers, marital status, place of birth or any other unnecessary details during the collection of public views, that would amount to a violation of the principle of data minimization.

b) Decide why you need the data and what you'll use it for.

Example:
Mwanahamadi, a news anchor, is tasked with interviewing Msemakweli, an Advocate of the High Court, on the impact of a trending judicial decision. In seeking personal details of Msemakweli, Mwanahamadi must refer to the reasons for the collection of the personal data. If the interview is being broadcasted on television, the name of the Advocate and her profession may be highlighted. Mwanahamadi should not disclose any other details of Msemakweli, such as her contact information or email address, as this data would be unnecessary for achieving the purpose of the interview.

c) Media practitioners should keep in mind what they are trying to achieve through personal data processing and aim to collect only the data they need to do that efficiently.

Example:
Mheshimiwa is vying for a seat as a member of the parliament of Kenya. Broadcasting her agenda and manifesto is one of her key campaign strategies. She approaches Ubunge Radio Station for assistance in broadcasting her manifesto. Before broadcasting Mheshimiwa's manifesto, Ubunge radio requests her personal data, including her marital status, level of education, family history, ethnicity, financial details, number of children, and health status. However, in line with the principle of data minimization, Ubunge radio only needed to broadcast Mheshimiwa's, education level and career history. His ethnicity, family history, number of children, and health records are too intrusive and contrary to the principle or data minimisation.

d) Identify if there is a need to collect personal data and if there are less intrusive ways of achieving the purpose.

Example:
Msema Kweli is an international journalist seeking to produce a documentary on sexual harassment in a renowned African organisation. Despite collecting the personal data of victims of sexual harassment in the organisation, she will be required to redact the names of the victims to protect them from stigmatisation and other ensuing consequences, especially if a suit has not been instituted for the same. The personal data will not be required at the documentary-making stage. Still, it may be necessary to obtain witness statements if a lawsuit is instituted against the organisation. He also assured the victims that their faces would be blurred and their voices altered upon release of the documentary. Msema Kweli should thus balance between the publication of personal data of the sexual harassment victims and the possible impact it would have on exercising their rights and freedoms.

e) Review the data you keep regularly to make sure you do not keep it longer than you need to.

Example:
For the preparation of the story, a journalist has collected official records as well as other personal details relating to an official. Many of these documents were used for referencing; however, following the lapse of the statutory period within which the media/journalist may be sued, these documents are no longer needed.

6.5 Confidentiality & Integrity

Data Controllers and/or processors must process personal data in a manner that ensures its security, including protection against unauthorized or unlawful processing against accidental loss, destruction, or damage. Therefore, all technical procedures used to gather, process, store, use, or distribute data should utilize robust security safeguards, for which threshold standards must be established. This may involve data encryption, security keys, two-factor authentication, and password requirements.

Moreover, data controllers and/or processors should conduct periodic data security audits and ensure that personal data is safeguarded from unauthorized access and changes. This can be achieved by implementing robust organisational and technical measures, such as policies and procedures for information security and access controls.

Example:
A freelance journalist working on an investigative piece about corporate corruption must ensure the confidentiality and integrity of personal data. He protects the sources of his story by using pseudonyms and encrypted communication tools like Signal or ProtonMail. Sensitive files are securely stored in encrypted drives or secure cloud services, and physical documents kept in a safe location. The journalist must ensure the facts are not distorted and ensure a balanced and ethical report that protects the integrity of personal data.

Example on Literary Works
Mwandishi, a freelance journalist, is working on a story that explores the lives of sex workers in a specific town in Kenya. This piece aims to provide a genuine and nuanced portrayal of the women involved in this trade, shedding light on their experiences and challenges. To protect the identities of the individuals featured in the story, she uses pseudonyms instead of their real names. This approach not only helps safeguard their privacy but also allows readers to engage with their narratives without compromising their safety or dignity. By prioritizing confidentiality, Mwandishi ensures that the focus remains on their stories rather than their identities, fostering a more empathetic understanding of their lives.

6.6 Storage Limitation

This principle requires that personal data should not be kept for longer than is necessary for the purposes for which it is processed in accordance with the subsisting government policy and legislation. Data controllers and/or processors must have appropriate internal policies and procedures in place to ensure that personal data is securely stored and only kept for as long as necessary. The said policies should have a specified retention period, as per the laws governing the relevant media practitioners, or otherwise provide for reasonable and justifiable retention periods based on the processing activity and the identified purpose for processing.

Furthermore, media practitioners must evaluate and document the duration for which they anticipate retaining the collected data. In this regard, media practitioners must establish a retention policy or schedule to assist in recording standard retention periods.

Guidance:
This principle of storage limitation only applies to personal data collected and not the story itself. The storage and/or archiving of stories will adhere to self–regulation, the codes of practice, Act and regulations. Journalistic materials containing personal data should be securely stored for as long as necessary to serve the journalistic purpose for which they were collected. Once the journalistic purpose is fulfilled or no longer relevant, it should be securely destroyed in compliance with relevant laws on the destruction of records.

Example:
A news organisation has a policy to archive articles for only five years after publication. After this period, older articles are either deleted or anonymized to protect the identities of sources and individuals involved. This approach not only reduces the amount of data stored but also helps ensure that sensitive information doesn't remain accessible indefinitely.

Example:
A publishing house has a policy that manuscripts submitted for review will be retained for a maximum of two years. If a manuscript is not accepted within that time frame, it is deleted from their system. This ensures that the publisher does not keep unnecessary submissions on file, thereby simplifying their data management and reducing the risk of potential data breaches.

6.7 Accountability

Accountability involves proactively safeguarding personal data. The accountability principle requires Media practitioners to ensure compliance with relevant laws and regulations related to the collection, use, and disclosure of personal data.

Media practitioners should thus have policies and procedures in place to govern the collection, use, and disclosure of personal data. These policies and procedures should be regularly reviewed and updated to ensure compliance with evolving legal and regulatory requirements.

Guidance:
To demonstrate compliance with the Act and Regulations, media practitioners should adopt and implement data protection policies and data protection by design and by default approaches; maintain records of processing activities and implement appropriate security measures, appoint a data protection officer where possible, enter into data processor agreements with third parties involved in the processing and conduct data protection training for employees.

LAWFUL BASIS FOR PROCESSING FOR JOURNALISTIC, LITERARY & ARTISTIC PURPOSES

Section 30 of the Act outlines several lawful bases for processing personal data, which include processing data for journalistic, literary, and artistic purposes which often involves processing personal data in the interest of public knowledge and democratic accountability, even when there is no direct relationship with the individual concerned. While processing personal data for journalistic purposes, media practitioners would likely rely on the following lawful basis:

a) Consent of a data subject
b) Legitimate interest of a data controller
c) Protection of the vital interests of a data subject
d) Public interest
e) Journalistic, Literary, and Artistic purposes

Media practitioners must ensure that the further processing for journalistic purposes is not inconsistent with the original purpose of collection and the identified journalistic purpose. Further to the above, a media practitioner must be able to demonstrate compliance with the relevant laws affecting processing by media practitioners, such as the Media Council Act and applicable Codes of Conduct.

7.1 Consent of a Data Subject

A media practitioner can seek the consent of a data subject to process their personal data for journalistic, literary, and artistic purposes. While relying on consent, a media practitioner must meet the conditions outlined in Section 32 of the Act. This section requires that the media practitioner prove they have obtained the data subject's consent for processing and specify the purpose. When seeking consent, the media practitioner must inform the data subject of:

a) The purpose of each processing operation;
b) The type of personal data collected and used;
c) The right to withdraw consent;
d) The consequences of providing, withholding, or withdrawing consent.

Consent must be given voluntarily, be specific to the processing purpose, and come from a data subject with the capacity to consent. For vulnerable groups (e.g., minors, mental incapacitation, etc), consent must be obtained from the child's parents or legal guardians. The consent should not be inferred from silence or pre-ticked boxes.

Example:
Filamu, an independent filmmaker, seeks to document the practice of rice farming in Mwea with an aim to publish. The documentary will be aired in a weekly show on one of the local media stations. Understanding the importance of consent, she researches local norms and regulations. Filamu approaches community leaders for guidance and visits farms to engage with farmers, addressing their concerns and sharing her vision to share their story. She presents consent forms in both local and English languages, ensuring transparency and emphasizing participants' rights to privacy. Filamu's respectful approach fosters trust, enabling her to create an authentic documentary while respecting farmers' privacy.

7.2 Legitimate Interest

Another basis is the legitimate interests of a data controller, which, in the case of journalism, literary and artistic work, can include the media practitioner's interest in creating and publishing news stories. When relying on the lawful basis of 'legitimate interests', media practitioners should not cause unwarranted harm to the person concerned. Legitimate interests can include a media organisation's commercial and journalistic interests in gathering and publishing material, as well as the public interest in freedom of expression and the right to know. This basis requires a balancing test to ensure that the interests of the media do not unjustifiably override the rights and freedoms of the individuals whose data is processed. A media practitioner relying on legitimate interest should conduct the following assessment:

(1) Identify Legitimate Interests: The process clarifies whether the interests pursued are legitimate and necessary for journalistic work. This includes determining whether the story makes a meaningful contribution to public debate or knowledge.
(2) Necessity and Proportionality: Assessing legitimate interest ensures that the processing of personal data is strictly necessary for journalistic, literary, and artistic purposes and that no less invasive means could achieve the same objective. This is key to minimizing potential harm or intrusion into individuals' privacy.
(3) Balancing Test: The assessment is essential for conducting a thorough balancing test between the media practitioner's interests and the individuals' rights and interests. This helps safeguard against abuses and ensure that journalism, literature, and the arts serve their purpose responsibly.

Example:
WenyeMitambo news group covers the Olympics, leveraging commercial interests for advertising and sponsorships while maintaining journalistic integrity in reporting competitions, athlete profiles, and investigative stories. They balance revenue generation with accurate, engaging coverage, fostering audience engagement and community participation.

7.3 Public Interest

Media practitioners frequently rely on the public interest as the lawful basis for processing personal data. This acknowledges that the value of public knowledge and informed citizenry can, in certain circumstances, outweigh an individual's right to privacy. Media practitioners are responsible for determining whether the publication is in the public interest.

(1) Validating the Public Interest Claim: The assessment confirms that journalistic, literary, and artistic activity genuinely serves the public interest. This is crucial for maintaining the integrity of journalism as a pillar of democracy. Not all stories that attract public attention qualify as being of public interest, especially when they delve into private matters without a clear societal benefit.

(2) Balancing Rights: It helps to weigh the public interest against the potential impact on the privacy rights of individuals. This balancing act ensures that the pursuit of a story does not unjustifiably infringe on personal rights, adhering to both legal and ethical standards.

Public interest, as outlined by media practitioner guidelines, includes but is not limited to:

(a) detecting or exposing crime or serious impropriety, corruption, or professional incompetence that affects members of the public;

(b) protecting public health or safety; or

(c) preventing the public from being misled by an action or statement of an individual or organisation.

Example:
Mwadime, an investigative journalist at a local station, is delving into a counterfeit gold syndicate that has targeted foreign nationals for fraud. Throughout his inquiry, he thoroughly examines the backgrounds of those implicated in the scheme. The findings of his investigation are then broadcast during prime-time news, featuring the names and photographs of the individuals involved in the syndicate. Mwadime justifies his investigation and the subsequent publication of the story on the grounds of public interest.

When relying on public interest, some publications may be exempt from certain data protection principles, such as having a lawful basis for processing, data minimization, the adoption of safeguards, ensuring data accuracy, and registration with the Office. Section 9 of this guidance note outlines the conditions for exemptions.

7.4 Processing for Journalistic, Artistic & Literary

Processing personal data is considered lawful when it serves essential journalistic, literary, or artistic purposes. This basis underscores the importance of freedom of expression and the dissemination of information in journalism, academia, the arts, and literature.

This legal basis applies particularly when media practitioners intend to publish journalistic, literary, or artistic works, even when the content may not be deemed of broad public interest. The objectives behind such works may range from entertainment to informational purposes,

often targeting specific audiences rather than the public. This basis enables media to explore and share diverse narratives while respecting the privacy of individuals and adhering to the code of ethics for journalism.

Example 1:
Mwanahabari is a news agency that is established to ensure Citizens are informed on current affairs. Mwanahabari is known for its comprehensive coverage of political news, including government actions, policies, and related events. They adhere to journalistic standards, ensuring that information is accurate, fair, and sourced appropriately, which supports their processing of personal data in accordance with the framework of journalistic activities.

Example 2 on Intent to Publish:
An investigative journalist gathers data for months on a new public health policy's impact, planning to publish their findings in a major newspaper to spur public debate on healthcare efficacy. Despite rigorous data collection, interviews with health professionals, and securing personal testimonials, the article's publication is indefinitely postponed due to sudden, relevant policy changes by the government. This decision to delay aims to incorporate these developments for a more comprehensive report. Although the article might never be published, the journalist's intent to publish throughout the investigation anchors their work firmly within "journalistic purposes." This intent, guiding the collection and processing of data even without final publication underscores the commitment to informing the public and contributing to significant societal discourse.

Example 3:
Mwandishi, an author, writes a historical novel that delves into the life of a notable musical figure in a particular Kenyan community. Through rich storytelling, he explores their struggles, achievements, and the impact they had on the nation's cultural landscape. Drawing upon historical records and anecdotes, Mwandishi creates vivid portrayals of this figure without seeking consent from their descendants or family members.
The novel aims to educate readers about Kenya's musical heritage while celebrating the contributions of this iconic artist. In this context, processing the historical data serves a literary purpose, allowing Mwandishi to illuminate important narratives that shape Kenya's identity and engage readers in a compelling exploration of its cultural history.

Guidance on continuous assessment of lawful basis considerations

Continuous assessment for determining the lawful basis for processing personal data in journalism emphasizes an ongoing evaluation rather than a one-time decision. This approach is crucial due to the evolving nature of publications and data protection obligations.

Key aspects of continuous assessment: -

1. Adaptability to changing circumstances:

- New information can shift the balance between public interest and privacy rights, necessitating adjustments in data processing.
- Changes in a data subject's status or consent can affect the justification for processing their data.

2. Ensuring compliance and ethical integrity:

- Legal and Ethical Standards: Ongoing assessment ensures alignment with evolving data protection laws and best practices in ethical journalism.
- Risk Management: Proactive evaluation helps identify risks related to data breaches or misuse, reducing potential legal and reputational harm.

3. Implementation strategies:

- Documentation and Review Processes: Formal documentation of data processing decisions allows for reassessment as needed.
- Training and Awareness: Regular training for journalists on data protection laws reinforces the importance of continuous assessment.
- Feedback Mechanisms: Collecting feedback from data subjects and the public can highlight privacy concerns and inform assessments.

4. Balancing public interest with privacy rights:

- Public Interest Monitoring: Regularly evaluating the public interest value of information ensures that journalism serves societal purposes while justifying the impacts on privacy.
- Internal Data Protection Impact Assessments: Conducting assessments helps identify risk changes and guide data processing adjustments to protect individuals' rights.

COMPLIANCE OBLIGATIONS

7.1 Registration

Media Practitioners must be required to register as data controllers or data processors if they fit the criteria defined in the Act and Regulations.
The Office has published a Guidance Note on Registration of Data Controllers and Data Processors, which is accessible through *www.odpc.go.ke*. The Guidance Note includes a step-by-step guide on how to complete the registration process, and the information required during the registration process is available here.

7.2 Duty to Notify

Media practitioners handle personal data in their various journalistic processes and are therefore expected to adhere to the principles outlined in the Act. While there exist journalistic processes where exemption to principles can be justified, Media practitioners are expected to adhere to these principles while processing. One of the key principles under Section 29 of the Act is transparency. This principle guides media practitioners in processing personal data fairly and transparently. To achieve this, they are required to comply with the duty to notify.
Media practitioners, where applicable, need to notify the data subjects of their rights specified in the Act. Section 29 of the Act guides that data subjects be informed why their personal data is being collected, the purpose of collection, disclose any third parties who may receive the data and the safeguards adopted, provide the contacts of the data controller or data processor and disclose whether any other entity may receive the data, describe the technical and organisational security measures taken to ensure data confidentiality and integrity, state if the data is being collected according to any law and if it is voluntary or mandatory, and outline the consequences if data subjects fail to provide all or part of the requested data. The Act provides that the above information should be provided to data subjects to enable them to understand how their personal data is used.

Media practitioners, driven by their own self-regulation or efforts to comply with the Act's provisions, have implemented various mechanisms that align with their duty to notify data subjects. Some of the commonly noted mechanisms include developing data protection and privacy policies that clearly define the rights of data subjects, consent mechanisms, privacy notices during data collection, online disclosures, email communications, and public awareness campaigns, among others. The Office guides that Media Practitioners should study the provisions of Section 29 of the Act and align the various mechanisms accordingly.

Example:
A journalist, Mr. Bidii, working for XYZ media house was researching on a feature on social economic impact of the high cost of living to the residents of Nairobi. The feature was to appear on both print and Audiovisual channels of the media house. Mr. Bidii and his team interviewed many data subjects of varying social and economic stratus across the many localities, took pictures and videos. The process involved collecting various data sets of both personal and sensitive data of subjects such as name, age, economic status, job, family size, images, voice recordings among others. Mr. Bidii and the team provided a consent form that data subjects read and signed.
In such a scenario, before a data subject consents to any processing of their personal data they must be informed of various items; what data is being collected, why is it being collected, how long will it be stored, will it be shared by any other party, mechanisms available to exercise their rights, contact person, among others. This is an obligation of the data controller or processor who in this case is the media practitioner who should deliver this information in a language and format that can easily be understood by the data subject. The consent must be unequivocal, free, specific, voluntary, and informed.

There are situations where media practitioners may be exempted from exercising their duty to notify the data subject at the point of collecting their personal data. Examples of such scenarios include, among others;

1. Emergencies such as accidents, natural disasters, etc., where the priority would be to save lives and report or publish the crisis as it unfolds. In such emergencies, it will be impractical for a media practitioner to notify data subjects of their rights.
2. Public events that attract huge crowds, such as political rallies and crusades.
3. Matters of public interest.
4. Where it would prejudice journalistic integrity or investigative outcomes, provided this is justified and documented.

7.3 Handling of Sensitive Data

The processing of sensitive personal data for journalistic, literary, and artistic purposes is a common practice. Sensitive personal data includes information about an individual's health, race, ethnicity, religion, biometric data, and sexual orientation, among others.
To process sensitive personal data for journalistic, literary, and artistic purposes, media practitioners must meet certain conditions set out in the Act. Media practitioners should not process sensitive categories of personal data unless:

i. There is a lawful basis for the processing, and they must adhere to the principle of data protection during the processing of any sensitive personal data.

Guidance:
Media practitioners cannot process purely private matters of a data subject, such as an individual's sexual life, without the explicit consent of the individual or in public interest as provided for in the Media Council Code of Conduct, 2025.

ii. Where consent is the lawful basis relied upon, media practitioners should ensure the consent is explicitly obtained from data subjects, and obtained before processing sensitive personal data. This means that the data subject must give clear, unambiguous, and specific consent for their data to be processed.

Example:
Publishing health information of a data subject without consent will result in a violation of the right to privacy and other laws and regulations.

In certain circumstances, media practitioners may process sensitive personal data without consent when:

i. A data subject has manifestly made the sensitive data publicly available.
ii. Processing of sensitive personal data is necessary to protect the vital interests of the data subject where data subjects are physically or legally incapable of giving their consent.

Guidance:
Media practitioners cannot process purely private matters of a data subject such as an individual's sexual life unless with explicit consent of the individual unless it is justified in the public interest.

7.4 Processing personal data for vulnerable groups.

Processing personal data for journalistic, literary, and artistic purposes, particularly when dealing with vulnerable groups such as minors, requires careful consideration and adherence to legal guidelines, as the publication of children's photos raises significant data protection concerns. A child's image is considered personal data, and its unauthorized use or distribution can infringe on the child's right to privacy. Media practitioners thus must respect children's rights, and this entails adhering to the best interest of the child principle by ensuring that their rights are protected and their dignity upheld in such processing. It is essential to obtain explicit consent from parents or guardians before publishing or sharing any photographs of children, especially in the public domain. Parental/guardian consent essentially means that a parent or guardian has permitted their child's data to be collected and used for specific purposes. Without parental/guardian consent, a media practitioner would not be able to legally collect or process personal data about minors for journalistic, literary, and artistic purposes. Respecting parental or guardian consent in such cases is essential for upholding the rights and protecting children's privacy, as well as ensuring compliance with the Act and regulations.

To ensure that parental consent is genuine, it is vital to verify the authority of parents or guardians. Verification can be accomplished in various ways, such as requiring a signed consent form, verifying the parent or guardian's government-issued identification, or utilizing electronic signatures. It is also essential to ensure that the person giving consent is the child's parent or guardian.

Guidance:
Before conducting interviews with minors, the journalist should obtain consent from the parents or legal guardians, informing them about the purpose of the interviews and how their child's information will be used. This consent ensures that parents are aware of their child's involvement in the journalistic, literary, and artistic piece and have agreed to the collection and processing of their child's data for this specific purpose.

Example:
Mwanahabari News is covering a story about a community event, which involves interviewing community members, including minors. Mwanahabari captures photographs and videos of the event, including close-up shots of attendees, some of whom are children, to publish these visuals alongside the article on the news outlet's website and social media platforms. In this scenario, the Mwanahabari is required to obtain parental/guardian consent before publishing the personal data of minors, which includes their visual representation.

Furthermore, in cases where parents or guardians made harmful, sensitive, or other inappropriate comments about children under their responsibility, journalists should pay attention to the best interests of the child. They should only publish such information when there is a compelling public interest, by avoiding mentioning the name of the child. This will prevent a lifelong link with harmful or embarrassing remarks or opinions. In such cases, where the name of the child is not cited and images are not shown, journalists should also avoid publishing additional information indirectly identifying the child (for example, photographs of the parents or the precise location of the family, etc.).

Moreover, when dealing with persons with mental incapacity, there is a need for greater protection due to the implicit susceptibility. Media Practitioners should refrain from taking advantage of the vulnerability of these people to extract information.
Furthermore, media practitioners should pay special attention when reporting on or interacting with individuals who have mental incapacity, as there is an even greater imperative for protection due to their inherent vulnerability. Therefore, media practitioners must exercise utmost caution and sensitivity in such processing for journalistic, literary, and artistic purposes, refraining from exploiting the vulnerability of these individuals to gather information and do reporting.

7.5 Rights of a Data Subject

Right	What does this mean?	Are there limits to this right?
Right to be informed.	Right to be provided with extensive information, including all their rights, contact details, source, retention period, purposes, categories, and recipients.	Whenever practicable, media practitioners should inform data subjects of the collection of their personal data and the purpose for which it will be processed.
Right of access	Right to access personal data within seven days and for free. It must be possible to make electronic subject access requests.	Provide any information you are able without undermining your journalistic, literary, and artistic activities; specific data can be withheld if disclosure adversely affects the rights and freedoms of other data subjects. For example, it is improbable for a journalist to disclose information identifying a

		confidential source in response to an individual's request for their own personal data.
Right to rectification (of inaccurate data)	A data subject may request correction of any personal information held to ensure that the data is accurate, true, or complete. Rectification of personal data should be within 14 days.	Some practical examples of relevant accountability measures you could take include: a) a policy setting out the process to follow when an inaccuracy is reported; b) an online form to make it easy for people to report inaccuracies; and c) reporting on inaccuracies and correcti

		ons in one place, as well as individual stories It is best practice to restrict the processing of personal data while verifying accuracy.
Right to erasure "To be forgotten''	A data subject may request erasure if; • the data is no longer necessary for the purpose for which it was initially collected, • An individual withdraws their consent, • individual objects to the processing of their data, • the processing of data is for direct marketing and the individual objects, • The processing has been unlawful. The data controller or processor should respond within 14 days. If a data controller has shared this data with a third party, they must take reasonable steps to inform the third party about any rectification or erasure requests. Additionally, over time, media or publishers may become data controllers and must notify data recipients of such changes to ensure proper rectification or erasure.	Right does not apply if processing is necessary for freedom of expression or information. There is a significant public interest in preserving news archives, as they play a crucial role in providing access to information about past events and the historical context of the present. This consideration is generally a compelling reason to avoid erasing personal data

		from these archives. If there are grounds for erasure, media practitioners should: a) Assess whether it is feasible or proportionate to reach out to the recipients of the personal data. b) Inform the third-party recipients of the data about the decision to erase. If requested, inform the individual about who received their data. If personal data has been published online, take

		reasonable steps to notify other controllers processing that data to remove any links, copies, or replications.
Right to restrict processing.	Right to request that processing be restricted where data cannot be deleted as it is required for legal reasons. This is a more limited right than the right of erasure. It allows controllers to restrict the use of data to a specific purpose, such as handling legal claims.	You should have processes in place to restrict personal data when necessary. Methods include: a) Temporarily moving data to another system b) Making data unavailable to users c) Removing published data from a website If you've shared the data with others, inform them of the restriction unless relying on a

		journalistic, literary, or artistic exemption. Consider whether it's feasible to contact each recipient. If asked, inform the individual about who has received their data. Typically, restrictions are temporary, so notify the individual before lifting them. When a request is declined, the controller/processor shall communicate in writing to the person and provide reasons for the objection.
Right to data portability	This enables individuals to easily transfer data from one controller or processor to another. The request should be acted on within thirty (30) days of receipt and upon payment of any reasonable charge.	The right to data portability only applies to personal data that an individual has personally provided, where the processing is based on consent or the performance of

		a contract, or where processing is carried by automated means (i.e., excluding paper files)
Right to object to processing.	Right to object to the processing of all or part of their data; generally, or for a specified purpose, the objection is absolute where processing is for direct marketing. A controller should respond within 14 days.	The right does not apply where there are legal claims requiring data use, and when data controllers demonstrate a compelling legitimate interest that outweighs an individual's privacy interests for the continued processing of personal data.
Right to withdraw consent	Data subjects have a right to withdraw consent as easily as they gave permission.	This right is balanced against the public interest in freedom of expression and the media's role in reporting. If consent is withdrawn, journalists should consider the implications for ongoing reporting. They may need to

		evaluate whether they can continue processing the data under other legal bases, such as legitimate interests. The withdrawal of consent should only apply to further processing of the personal data.
Right not to be subject to a decision based solely on automated decision making.	Data subjects have a right not to be evaluated or subject to decisions based solely on automation where decisions have legal or significant effects.	The right does not apply if the decision is based on explicit consent, necessary for a contract, or authorised by law.

7.6 Engagement of Data Processors

When media practitioners engage with vendors or service providers (data processors) for cloud-based solutions, data management, or even security services, it is crucial to consider the special context of processing for journalistic, literary, and artistic purposes. These entities, acting as data controllers, must ensure that their engagement with data processors upholds the stringent requirements of the Act and regulations, particularly in safeguarding the rights of data subjects while balancing the freedom of expression and information essential to journalism, literary, and artistic purposes.

The Act mandates that any engagement with a vendor or service provider to process information on behalf of a media practitioner must be governed by a written contract. This contract must explicitly state that the data processor will act solely on the instructions of the controller, adhering to the principles and obligations pertinent to journalistic purposes or in the attainment of journalistic endeavours. Importantly, the contract must underscore the commitment to protect personal data confidentiality, recognizing the sensitive balance

between public interest and individual privacy rights inherent in journalistic, literary, and artistic endeavors.

Specifically, the contract between a media practitioner (data controller) and a data processor should detail the subject matter of processing, the type of personal data involved, the nature and purpose of processing, and the duration. Given the context of journalistic work, the contract should emphasize security measures tailored to protect journalistic sources and data integrity. It should outline the conditions under which the controller must grant prior authorization for certain processing activities, reflecting the unique ethical and legal considerations specific to journalism.

Additionally, the contract must include obligations for the data processor to ensure employee confidentiality and support the media practitioner in fulfilling their duties under the Act, particularly in responding to inquiries regarding data protection rights. The agreement should also specify procedures for the deletion or return of personal data upon contract termination, provisions for conducting audits and inspections to ensure compliance, and clarify liability for non-compliance or actions beyond the controller's instructions.

7.7 Data Protection Impact Assessment (DPIA)

The carrying out of a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". Furthermore, when alternative methods like covert recording are used, media practitioners must conduct a DPIA to proactively identify and mitigate risks. In cases where it is unclear whether a DPIA is required, it is recommended that a DPIA be carried out nonetheless, as it is a valuable tool to help data controllers and/or data processors comply with data protection law. In addition to the above, the Act requires all data controllers and processors to implement appropriate technical and organisational measures and integrate suitable safeguards to ensure the adequate protection of personal data of data subjects.

The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke. The Guidance Note includes the form in which a Data Protection Impact Assessment (DPIA) should be submitted, as well as guidance on when it should be submitted.

7.8 Notification and Communication of Breach

Data Controllers must report personal data breaches to the Office without delay, within 72 hours of becoming aware of the breach, while also notifying the affected data subjects. Where there has been unauthorised access, players within the telecommunication sector are required to communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established.

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

mitigate the damage and remedy any failure or shortcoming that contributed to the breach, as well as how affected individuals can mitigate potential harm.

7.9 Privacy by Default and by Design

The Data Protection Act, in section 41, outlines the requirement for data controllers and data processors to implement appropriate technical and organisational measures to ensure effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the Act requires that only essential personal data is processed, considering the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by design is an approach that ensures data controllers and data processors consider privacy and data protection issues at the design phase of any system, service, product, or process, and then throughout the lifecycle. Data protection by default requires media practitioners to ensure that only data necessary to achieve a specific purpose is processed. Data protection by default requires media practitioners to ensure that data protection issues have already been considered and that protection methods have been incorporated into existing systems and practices. This could be achieved by media practitioners specifying the personal data required before processing starts and appropriately informing individual data subjects, and only processing the personal data needed for specific purposes.

Applying appropriate security measures to personal data processed, and its processing environments both at rest and in transit, is vital to ensure the personal data is protected to the highest standards. This can be achieved through putting in place robust organisational and technical measures, such as policies and procedures for information security and access controls, as explained below:

7.9.1 Technical Safeguards

Consent Management Platforms (CMPs) Section 32(1) of the Act explicitly addresses the need for data controllers and Data processors to seek consent from data subjects before processing personal data. CMPs help journalists obtain explicit consent from users for data processing activities. The platforms also enable data subjects to manage their preferences and provide transparency on matters of data collection and processing.

Anonymisation and Pseudonymisation Tools

Sections 37(2) and 39(2) of the Act provide that a data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymize the data to ensure that the data subject is no longer identifiable. In that case, Journalists often need to protect the identity of sources and individuals mentioned in their reports. Anonymisation and Pseudonymisation tools help redact or replace personally identifiable information (PII) to maintain privacy.

Example:
Suluu is an international journalist seeking to produce a documentary on sexual harassment within a renowned African organisation. Despite Suluu collecting the personal data of victims of sexual harassment in the organisation, she will be forced to redact the names of the victims to protect them from public ridicule and other ensuing consequences, especially if a suit has not been instituted for the same.

Guidance:
Media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except where a court has ordered disclosure after a full and fair public hearing.

a) **Secure Communication Tools:** Media practitioners should utilize secure communication tools to safeguard sensitive information and maintain the integrity of confidential correspondence with sources. This can be achieved via:
    a. **Encryption of data at rest and in transit:** Secure messaging applications, such as Signal, ensure that communications remain confidential, protecting data from integrity threats. The use of end-to-end encryption also prevents parties from later denying their involvement. Data encryption is a critical process of securing data from unauthorized users by converting readable data into an unreadable form using encryption algorithms and encryption keys.
    b. **Use of Secure Submission Platforms**: Platforms like SecureDrop provide a secure and anonymous means for whistleblowers to submit information, thereby preserving data integrity and non-repudiation.
    c. **Timestamps:** The use of timestamps provides evidence of when messages or data were sent, which is crucial for data subject integrity and non-repudiation.

Example:
Ujana Media House procures a Customer Relationship Management (CRM) software that contains inbuilt tools for end-to-end encryption, generation of audit trails, and log reports to comply with the technical measures for securing personal data in their custody.

b) **Data Retention and Deletion Solutions:** Section 39(1) of the Act requires organisations to manage data retention and deletion. Data management platforms can help automatically delete data when it's no longer needed or archive it for compliance purposes.

Example:
An art gallery decides to keep digital records of artworks for a maximum of ten years after an exhibition ends. After that period, images and detailed descriptions of the artworks are removed from their database. This practice allows the gallery to manage storage costs effectively and focus on current and future exhibitions without being burdened by outdated records.

Example:
Ujana Media House procures a data management software to provide alerts and notifications on the expiry of data retention periods. After this, Ujana Media House's ICT personnel determine whether the data should be deleted, archived, anonymized, pseudonymized, or retained altogether. The software system enables Ujana Media House to exercise control over the deletion of personal data in its custody, thereby promoting the rights of data subjects not to be subjected to automated decision-making that is likely to result in infringement of their rights and freedoms.

c) **Data Inventory and Classification:**

Media practitioners should identify and classify the types of data they collect and store. This includes categorizing data as public, private, sensitive, or confidential.

Example:
Ujana Media House, through its ICT team, develops a data mapping tool for internal mapping of personal data in the media house's custody. The data mapping tool categorizes data into public, personal, enterprise, and sensitive. Through these categories, individual employees dealing with personal data provide input on the purpose for processing the data, the mode of storage (whether manual or electronic), the storage period, the lawful basis for processing, the employees with ownership of the data, and the technical and organisational measures in place to secure the data. Through data mapping, Ujana Media House can track the movement of personal data from its initial state to its ultimate erasure.

d) **Archiving Solutions:** Archiving platforms are used to store historical content, including old articles, videos, and broadcast recordings. Archiving solutions ensure that data is accessible for historical or legal purposes without cluttering the active storage systems.

7.9.2 Organisational Safeguards

e) **Data Retention Policies:** Media practitioners should establish data retention policies that outline the duration for which different types of data will be stored. This ensures that data is only retained for as long as necessary.

f) **Legal Compliance:** Media practitioners should have a legal department or consultants to ensure compliance with data retention and deletion requirements specific to their jurisdiction.
g) **Regular Audits and Monitoring:** Regular audits should be conducted to ensure that data is being managed in accordance with the defined retention and deletion policies. Monitoring solutions may help detect and address non-compliance.
h) **Access Control and Identity Management:** Media practitioners should implement robust access controls and identity management systems to ensure that only authorized personnel can access sensitive data.

Example:
Ujana Media House has developed an Incident response plan, data protection policy, and other organisational policies relevant for the protection of the personal data held in their databases and manually. Through the organisation's policies on data security, Ujana Media House ensures that data stored manually is also as secure as data stored in electronic databases.

EXEMPTIONS

8.1 Introduction

Media practitioners process personal information for journalistic, literary, and artistic works to exercise their right to freedom of expression. However, there is a delicate balance between freedom of expression and data protection. This section offers guidance on when exemptions for journalistic, literary, and artistic purposes would apply.
Section 52 of the Act provides the criteria for application of the exemption of processing personal information for journalistic, literary, and artistic purposes as follows: -

a) Processing of the personal information must only be for journalistic, literary, and artistic purposes;
b) The processing activities must be carried out with the intention to publish;
c) The media practitioner must reasonably believe publication is in the public interest, and where there is intrusion into private life, the public interest must justify the extent of the intrusion.
d) The media practitioner can demonstrate that their processing of personal information complies with any self-regulatory or issued code of ethics in practice; and
e) The media practitioner must also reasonably believe that compliance with the relevant provision is incompatible with journalism.

The above criteria must be met for the exemption to apply. Therefore, media practitioners must maintain records of exemption decisions, detailing how each criterion is met, including the public interest justification and why compliance with the specific data protection provisions is incompatible with journalistic, literary, and artistic purposes. Furthermore, media practitioners relying on this exemption should demonstrate robust policies and procedures,

compliance with relevant industry codes of practice, awareness of the Act's requirements, and appropriate record-keeping for particularly controversial decisions.

Despite the exemptions discussed in this section, processing of personal information for journalistic, literary, and artistic purposes must generally comply with the requirements of the Act. Relying on exemptions for journalistic, literary, and artistic purposes does not preclude a media practitioner from adhering to the following compliance obligations:

a) Registration with the Office;
b) Having a lawful basis for processing;
c) Minimizing the collection of data to only what is sufficient to achieve the purpose;
d) Ensuring data quality and accuracy;
e) Ethical considerations; and
f) Implementing security measures to secure personal data.

8.2 Exemption for Journalistic, Literary & Artistic purposes

A key factor that distinguishes processing personal information for journalistic purposes is the intent to publish, meaning that the primary objective behind collecting and handling such data is to share it with the public. Additionally, the actual publication of the information is not required for the activity to qualify as journalistic. Even if the content does not ultimately get published, the intention to make it available to the public is sufficient to categorize the processing as journalistic. Therefore, the actual publication of the information is not a prerequisite for an activity to be considered for journalistic purposes.

For data processing to qualify for the journalistic exemption, it must be in the public interest.

Guidance on Public Interest threshold for Journalistic Purposes

Setting a very high threshold for assessing public interest in the context of processing data for journalistic purposes is crucial for the application of the data protection exemption. This ensures that data protection exemptions for these purposes are applied judicially, safeguarding individuals' privacy while allowing for the freedom of expression in a democratic society. The application of the threshold for public interest involves the following criteria to ensure that only journalistic activities that genuinely serve the public good can justify the processing of personal data under exemptions.

Significant Contribution to Democratic Processes: The information should make a meaningful contribution to public debate, democratic governance, or oversight of public institutions. This includes investigative journalism that exposes corruption, promotes transparency, and enables public accountability.

Urgency and Necessity: There should be a clear and compelling need for the information to be disseminated to the public without delay, due to its relevance to pressing social, economic, or environmental issues or its critical impact on public health and safety.

Absence of Alternative Means: The public interest assessment must demonstrate that the information cannot be disseminated in a less intrusive manner that respects individuals' privacy rights.

Proportionality and Minimization: The processing of personal data should be proportional to the journalistic aim being pursued. This means that any intrusion into personal privacy is outweighed by the public's interest in the information. Data minimization principle should be applied, ensuring that only the necessary data for achieving the journalistic purpose is processed.

Ethical Considerations and Integrity: The intent behind the publication should be guided by journalistic integrity and ethics, avoiding sensationalism or exploitation of personal stories for commercial gain. The focus should be on issues of genuine public concern rather than topics that merely satisfy curiosity without serving a public interest.

Transparency and Accountability: There should be a transparent process for determining public interest, with documented justifications for decisions made. Journalists and media organisations must be accountable for their choices, including the readiness to defend the public interest basis of their work if challenged.

Applying this high threshold ensures that exemptions for journalistic purposes are not used to justify the invasion of privacy in cases where the interest of the public is more about curiosity rather than a substantive need to know. This approach upholds the integrity of journalistic work, ensuring that it remains a vital tool for informing the public on matters of significant concern, promoting democratic values, and facilitating informed public discourse.

Example:
Where Gossip Columns Might Meet the Threshold:
Reporting on a celebrity involved in a charity scandal, where their actions may impact public trust or the use of public funds.
A public figure's statements or actions regarding significant societal issues, such as climate change advocacy, where their influence could sway public opinion or policy.

Example:
Where Gossip columns do not meet the threshold for public interest:
A gossip column that reports on a well-known actress frequently visiting a particular grocery store and purchasing luxury items, alongside details like her shopping list, her favorite shopping and dining places. This information is personal and involves tracking her shopping patterns and preferences; it lacks significant public interest.
The story doesn't expose any wrongdoing, public service, or broader societal implications. Instead, it merely focuses on her personal choices in a private setting. This could raise ethical concerns about privacy and the responsible use of personal data, as it does not contribute meaningfully to public discourse.

8.3 Literary and Artistic Works

Literary work includes novels, stories and poetic works, plays, stage directions, film sceneries and broadcasting scripts, textbooks, treatises, histories, biographies, essays and articles, encyclopedias and dictionaries, letters, reports and memoranda, lectures, addresses and sermons, charts and tables, computer programs; and tables and compilations of data including tables and compilations of data stored and embodied in a computer or a medium used in conjunction with a computer.
Artistic material refers to any visual representation, such as a painting, drawing, map, photograph, sculpture, engraving, or video.

Processing activities for literary and artistic works cannot be performed without respecting the ethical and professional standards in place, particularly the Copyright Act. The person who publishes literary or artistic works must ensure that the publication is within the scope of the exemption provided in sections 51 and 52 of the Act.

ANNEX A

Checklist for Compliance

Description	Questions	Yes	No	Comments/Remedial Actions
Lawful basis for processing	We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.			
	We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable and less intrusive way to achieve that purpose.			
	We have documented our decision on which lawful basis applies to help us demonstrate compliance.			
	We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.			
	Where we process sensitive data, we have also complied with sections 44, 45, and 46 of the Act.			
Compliance Obligations	We have reviewed the criteria for registration for controllers and processors and have taken the necessary steps to comply.			
	We have ensured that you have complied with the principles of data protection as per section 25 of the Act.			
	We have implemented data protection by design or by default in our processing.			

Public Interest	We have carried out a public interest assessment.			
	Our processing activities comply with the criteria outlined in this guidance note on public interest assessment.			
	We have a specific criterion for determining processing activities that fall under the public interest.			
	We can justify the publications that are classified as public interest.			
Exemptions	We have reviewed the criteria for registration for controllers and processors and have taken the necessary steps to comply.			
	We have complied with the non-exempt principles listed in section 51 of the Act, which include (lawful processing, data minimization, data quality, and safeguards)			
	Our processing activities fall under journalistic, literary, and artistic purposes.			
	We intend to publish our work.			
	We believe that publication is in the public interest.			
	We are part of a sector or industry that has self-regulation and a code of conduct.			
	We believe that complying with Data Protection principles will impede the required outcome of your journalistic, literary, and artistic activities			