OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes - Processing of Personal Data on Publications of Recorded Media

2025

TABLE OF CONTENTS

FOREWORD

The Constitution of Kenya, 2010, guarantees every individual the right to privacy under Article 31. The Data Protection Act, 2019, reinforces this right by setting out principles and obligations governing the collection, use, and disclosure of personal data. Among the most prevalent and sensitive forms of personal data are photographs, video recordings, and other recorded media, which can reveal intimate details of an individual's identity, location, and private life.

As Kenya embraces the digital superhighway under the Bottom-Up Economic Transformation Agenda (BETA), recorded media has become central to communication, entertainment, journalism, education, and social interaction. However, the ease of capturing, storing, publishing, and sharing recorded media has also amplified privacy risks, including identity theft, surveillance, harassment, reputational harm, and the misuse of children's images. In this context, the need for responsible and rights-based data processing cannot be overstated.

This Guidance Note has been developed to provide clarity to data controllers, processors, media entities, and individuals on their obligations when processing personal data for publication of recorded media. It underscores the lawful bases for processing, the need for verifiable consent, purpose limitation, data minimisation, accuracy, storage limitation, and accountability. It also emphasises the rights of data subjects—including the right to information, objection, erasure, rectification, and protection from automated decision-making.

The Office affirms that the processing of recorded media must always balance the public interest in information with the protection of individual rights and freedoms. Particular attention must be given to vulnerable groups, especially children, whose identities and locations require heightened safeguards. Compliance with this Guidance Note will not only fulfil statutory obligations but also foster public trust, protect human dignity, and promote responsible innovation in the digital and creative industries.

It is my expectation that this Guidance Note will serve as an authoritative resource for organisations, journalists, educators, cultural institutions, and content creators, guiding them to lawfully, fairly, and transparently process recorded media in a manner that respects the rights of all Kenyans.

Immaculate Kassait, MBS
Data Commissioner

DEFINITIONS

"Act" - means the Data Protection Act, No 24. of 2019;
"Artificial Intelligence"- AI is the ability of machines or computer systems to perform tasks that normally require human intelligence
"Augmented Reality"- is a technology that adds digital elements, like images or sounds, to the real world around you, enhancing what you see or experience in real time through devices like smartphones.
"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing of Personal Data.
"Data Handlers" means a data controller and or data processor.
"Data Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
"Data Subject" means an identified or identifiable natural person who is the subject of Personal Data. "Entity" or "Entities" means a natural (individual) or legal person, public authority, agency or other body that processes (handles) Personal Data.
"Further processing" of personal data refers to any operations performed on personal data for a purpose other than that which they were initially collected.
"Legitimate Interest" refers to a justifiable reason to process personal data for a data handler specific benefit or purpose. There should be a balance between the data handler's interest and the interest of the data subject.
"Machine Learning"- This is technology where computers learn from data and improve their performance on tasks without being specifically programmed for each task
"Processing" means any operation or sets of operations which is performed on Personal Data or on sets of Personal Data whether by automated means, such as:

a)collection, recording, organisation, structuring.
b) storage, adaptation or alteration.
c) retrieval, consultation or use.
d) disclosure by transmission, dissemination, or otherwise making available.
e) alignment or combination, restriction, erasure or destruction.

"Publication" means the act of making personal data available to the public, whether through print, electronic means or other forms of distribution.
"Recorded media" - any form of audio, video, or visual personal data that has been captured, stored, and reproduced using recording devices or technologies. It includes a wide range of formats and mediums, including audio, video, images and photographs, and multimedia presentations.
"The Office" means the Office of the Data Protection Commissioner as established under the Data Protection Act.
"Virtual Reality"- is a technology that creates a completely digital environment, replacing the real world around you. Using special devices like VR headsets, you are fully immersed in a simulated world where you can interact with the surroundings.

THE OFFICE

The Office of the Data Protection Commissioner is a government agency established to uphold and enforce data protection laws in Kenya. Its primary purpose is to protect the privacy, security, and fundamental rights of individuals concerning the processing of their personal data. The Office oversees the implementation and enforcement of the Data Protection Act, ensuring compliance by data controllers and data processors established in Kenya or targeting data subjects located within the country. Through its regulatory efforts, the Office strives to safeguard the confidentiality and integrity of personal data, promoting responsible and transparent data processing practices in both private and public sector organisations.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organisations processing personal data should respect individuals' 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 the Data Protection Act and attendant regulations. In addition, the Office also has a duty to raise public awareness about data protection issues and educate individuals about their rights and organisations on how to protect personal data. With the growing importance of data collection and data processing activities in our digital age, the Office is a critical institution in maintaining trust and confidence in our data-driven society.

The Office 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 ("BETA") and particularly its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, with its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation.

INTRODUCTION (BACKGROUND, PRIVACY CONCERNS)

2.1. BACKGROUND

Technology has facilitated the gathering of vast amounts of information on individuals. Evolving technologies have been used to capture behaviors in a broad range of applications. This has led to an evolution in the processing of personal data enabling the capturing, processing, and publishing of vast amounts of audio-visual and recorded information. The unauthorized disclosure of personal data by entities without sufficient protection measures can result in a range of consequences. These may include the fraudulent use of personal information for identity theft, targeted harassment or discrimination, and harm to an individual's reputation. Entities and individuals alike must prioritize the implementation of safeguards to prevent unauthorized access and misuse of personal data. Such measures are essential in mitigating potential risks and protecting the privacy and security of individuals. To address the evolving concerns, this guidance note on the processing of personal data for the publication of audiovisual and recorded media is intended to provide direction on the handling of personal data in the context of publication. This guidance is essential to ensure compliance with data protection regulations and to safeguard the privacy rights of individuals featured in audiovisual and recorded media. The processing of personal data for publication purposes carries inherent risks, and organisations and individuals involved in media production must understand and adhere to the applicable data protection principles.

This guidance note aims to address key considerations such as obtaining consent for the collection and use of personal data, including the processing of personal data relating to children, ensuring the security and confidentiality of the data, and respecting the rights of data subjects. It also provides practical advice on managing and protecting personal data throughout the production process, including storage, access control, and data retention. The guidance note emphasizes the importance of conducting data protection impact assessments to identify and mitigate potential risks to individuals' privacy. It highlights the need for transparency in informing individuals about the processing of their personal data and their rights in relation to such processing.

It addresses the specific considerations related to the publication of audiovisual and recorded media, including the identification and blurring of individuals, the use of pseudonyms, and the handling of sensitive personal data. It also underscores the importance of considering the potential impact on individuals' privacy and reputations when publishing audiovisual and recorded media. By following the principles and recommendations outlined in this guidance, data handlers can ensure that they process personal data in a lawful, fair, and transparent manner, while upholding the privacy rights of individuals featured in audiovisual and recorded media.

2.2. PRIVACY ISSUES AND CONCERNS

The use of recorded media raises several privacy concerns due to the potential for the collection, storage, dissemination, and sharing of personal data contained within audio, video,

or visual recordings. Recorded media may capture individuals in public or private settings without their knowledge or consent, potentially invading their privacy rights.
Recorded media may inadvertently capture personal information about individuals, such as their faces, voices, or identifiable characteristics, even if they are not the primary subjects of the recording. This can lead to unintentional exposure of personal data and privacy risks for individuals captured in the background of recordings.
This section highlights some of the privacy concerns in relation to the processing of personal data for publication of audio video and recorded media;

2.2.1. EMERGING TECHNOLOGIES

Emerging technologies are revolutionizing the way audiovisual and recorded media are produced, shared, and consumed. Tools like artificial intelligence (AI) and machine learning (ML) enable automated content generation, facial recognition, and emotion detection, enhancing media production and raising privacy concerns around unauthorized identification and surveillance.
Virtual reality (VR) and augmented reality (AR) provide immersive, interactive experiences but collect vast amounts of personal data, such as biometric and location data, which must be handled carefully.
The advent of 5G improves media delivery and real-time interaction, but it generates more personal data, requiring stronger data protection measures. Cloud-based production tools facilitate remote collaboration and scalable storage but introduce risks related to the security and privacy of unprocessed or sensitive content. The use of biometric data to gauge audience engagement or personalize experiences, along with high-resolution drones for filming, further amplifies the need for explicit consent and strict data handling protocols. These advancements, while exciting, demand careful consideration of data privacy and security to prevent misuse and protect individuals' rights.

2.2.2. USE OF SOCIAL MEDIA TO PROCESS PERSONAL DATA RECORDED USING RECORDED MEDIA

Social media is a powerful tool that allows individuals to connect with others and share information online. It has become an integral part of our everyday lives, revolutionizing the way we communicate and interact with the world. As social media continues to grow rapidly, it brings heightened privacy concerns related to the personal data of users on various platforms.

Social media platforms collect a large amount of user data, including sensitive personal information, which can be shared with third parties for purposes like targeted advertising. Many users are often unaware of, or do not fully understand, the privacy settings available to them, which can lead to the unintentional exposure of personal information to a much broader audience than they intended. This lack of transparency and control over personal data amplifies the risk of privacy breaches, highlighting the need for clearer privacy practices and user education on how to safeguard their information online.

2.2.3 PUBLICATION OF RECORDED MEDIA

Publication of personal data captured using recorded media is multifaceted and has become increasingly relevant with the advancement of technology. One of the primary concerns is whether individuals whose data is being captured have been informed of its publication. Without proper information, publishing personal data can infringe on privacy rights and potentially lead to legal consequences.

Publishing content that has been captured by audiovisual and recorded media with people's personal data could accidentally show who they are. Consequently, this could expose individuals to risks like identity theft or harassment.

Secondly, the nature of the captured personal data and its potential to reveal identifiable information about individuals is a significant concern. This includes not only visual images but also audio recordings, which may inadvertently disclose sensitive details about a person's identity or private life. The context in which personal data is captured and published plays a crucial role in determining its appropriateness. For example, recordings made in public spaces, such as on media platforms where individuals have a reduced expectation of privacy may be subject to different considerations than recordings made in private settings where individuals have a higher expectation of privacy.

Publication of personal data without adequate safeguards can lead to various harms, including identity theft, harassment, discrimination, and reputational damage. Therefore, it's essential to weigh the potential benefits of publication against these risks. There may be situations where the **public interest** in accessing or sharing certain information conflicts with individuals' rights to privacy. Balancing these competing interests requires careful consideration of the circumstances and potential impacts involved.

Example

After a physical altercation at the Musafi Hotel Lobby, management released CCTV footage to identify those involved, but this raises privacy concerns. The footage includes other guests who were not part of the fight, potentially exposing their identities without consent. Releasing such footage without proper notice or safeguards, like blurring faces, could infringe on privacy rights and lead to risks like identity theft or harassment. While the incident occurred in a public space, ethical and legal considerations still apply, and the hotel must carefully balance the need for public disclosure with protecting individuals' privacy.

Example

A documentary is being filmed in the village of Jijikuu, Kenya, focusing on the daily life and culture of the community. In the background, children from Jijikuu Primary School are visible playing on the school grounds. The documentary captures clear images of the children’s faces, school uniforms, and identifiable landmarks near the school, such as the signpost with the school's name.

If this video is published without safeguarding the children's identities, it could expose them to significant risks. The documentary will expose information about the location of the school or recognize the children in their local community. If the video circulates widely on social media, the children could become the target of unwanted attention, which could result in emotional harm, bullying, or even physical danger.

To avoid these risks, it is essential to blur the children's faces, remove identifying details, and seek parental consent before publication.

Once personal data is published, it is difficult to control its consequent use. Unauthorized **secondary use** of recorded media may violate a data subject's privacy rights and expectations. Additionally, collecting a large volume of recorded media overtime could lead to substantial data aggregation which in turn results in the profiling of individuals based on their social behaviors, preferences, or activities without their explicit consent.
Publishing of some content may capture location data which might enable tracking, this in turn reveals sensitive information of a subject's whereabouts without explicit consent

Example:

Jimbo App is a social media platform where users can post and share recorded media, such as pictures and videos. However, once these media files are shared, Jimbo can analyze them to determine various details about the users, such as their preferences, social behaviors, and activities, often without explicit consent. Over time, this practice may result in substantial data aggregation, which can lead to the profiling of individuals. In addition, some of the posted content may inadvertently include location data, potentially allowing Jimbo to track users' movements and reveal sensitive information about their whereabouts, further compromising their privacy rights.

SCOPE AND PURPOSE OF THE GUIDANCE NOTE

The guidance note addresses the processing of personal data for the publication of audio visual and recorded media, with the exclusion of intellectual property rights considerations. It provides direction in the handling of personal data within the context of creating, processing and publishing audio visual content, ensuring compliance with the Data Protection Act and the Data Protection Regulations.

It outlines the specific considerations and best practices for handling personal data in the context of creating and publishing audio visual and recorded content. This includes addressing issues such as obtaining consent, protecting the privacy rights of individuals featured in the media, and securely managing and storing personal data.

It also emphasizes the importance of conducting data protection impact assessments and implementing appropriate security measures to safeguard personal data throughout the production and publication process. By following this guidance, organisations can ensure that they are respecting the rights of individuals while engaging in the creation and dissemination of audiovisual and recorded media.

It addresses the necessity of implementing appropriate security measures to safeguard the privacy and confidentiality of minors' personal information. Furthermore, it offers guidance on the responsible use of minors' data, emphasizing the need to minimize potential risks and protect their best interests. Overall, this guidance note serves as a valuable resource for ensuring compliance with data protection regulations and upholding the rights of minors in the context of audiovisual and recorded media publication.

It offers practical advice on obtaining consent for the use of personal data in audio visual materials, as well as the secure storage and transfer of such data. The guidance aims to assist organisations and individuals involved in the production and distribution of audio visual and recorded media in understanding their responsibilities and obligations regarding the processing of personal data in this specific context.

APPLICATION OF THE DATA PROTECTION PRINCIPLES

The principles of data protection are provided under Section 25 of the Act and under Regulations 28 to 34 of the Data Protection (General) Regulations 2021. This section provides practical guidance on how data controllers and data processors processing personal data for the publication of audio, visual and recorded media can implement the principles into their processing operations.

4.1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

This principle requires that data controllers and data processors processing personal data for publication of recorded media, should be able to demonstrate the lawful basis being relied on, should ensure that the processing is transparent, and that the outcome of the processing is fair to the concerned data subject.

In determining the lawfulness of the processing, data controllers and data processors are to be guided by section 30 of the Act, which sets out the lawful basis that can be relied on to process personal data.

In general, fairness means that you should only handle personal data in ways that data subjects would reasonably expect and not use it in ways that have unjustified adverse effects on the data subjects. Data controllers and data processors are required to think not just about how they can use personal data, but also about whether they should use it.

The need for transparency is a fundamental aspect of data protection. When it comes to transparency, the expectation is that the data controllers and data processors must inform the data subject when personal data about them is being collect and processed, what the personal data will be used for, whether it will be shared with other entities and if so, the identity of those entities, as well as how long the information will be kept. To ensure that the principle of transparency is complied with, data controllers and data processors will be required to ensure that they find a way to provide the data subject with this information in a timely, clear, and accessible way including usage of multiple communication channels.

Example

A popular entertainment establishment in Nairobi Kenya hosts a lady's night out event every Wednesday night. With the aim of attracting more revelers to the event, the social media manager of the establishment proposes that they should advertise the event on their social media channels.

The content to be used in the advertisement will be videos taken of the lady revelers at the entertainment establishment.

For the entertainment establishment to be compliant with the principle of lawfulness, fairness and transparency they will be required to do the following:

a. Ensure that they have identified a lawful basis to support the publication of the pictures of the revelers on their social media platforms, in this instance, they may choose to obtain the consent of the ladies attending the event.
b. Ensure that the processing is transparent and fair. The entertainment establishment should ensure that the ladies attending the event are informed that their personal data is being collected (pictures or video footage), what that information will be used for, the lawful basis that will be relied on in the processing, as well as how long that information will be kept. The privacy notice is published on the entrance of the club, and they regularly make announcements in the course of the night. The privacy notice, however, does not serve as consent for publication, which needs to be obtained separately.

An effective way to provide transparent information is to place signs prominently before the entrance of the premises in the field of vision of the data subjects and reinforce this with further signs inside the area.

4.2 PURPOSE LIMITATION

This principle provides that a data controller or processor must ensure personal data is collected for explicit, specified and legitimate purposes and must not be used for purposes other than those specified at collection. In view of this principle, a data controller/processor must ensure that the personal data they are processing are:

(1) Adequate and sufficient to properly fulfil the stated purpose
(2) Relevant and has a rational link to that purpose; and
(3) Is limited to that specific intended purpose such that the controller/processor do not hold more than they need for the particular purpose

Purpose limitation means that the personal data collected for one purpose should not automatically be repurposed and used for other use cases - without the data subjects knowledge or consent.

Example

Waweza Church normally does a livestream of the sermons. This livestream focuses exclusively on the pulpit and the sermon, intentionally excluding the congregation from the camera's view. This deliberate choice ensures that the recording is used solely for broadcasting the sermon to interested parties, thereby aligning with its intended purpose. By not capturing images or identifiable features of the congregation, the church limits the scope of personal data collection and respects the privacy of individuals not directly involved in the sermon. This approach not only minimizes the risk of processing personal data of those present but also maintains transparency by clearly communicating the focused nature of the livestream to viewers.

It is important to note that, on matters of audio visual and recorded media, the data controller or data processor needs to not only focus on the technical capabilities, but also quality of the image produced, the field of vision offered, and the amount of data recorded. The data controller or data processor should thus consider the governance capabilities that complement the system (technical capabilities), such as a software that ensures clarity of the image produced and enables footage to be uploaded, stored, and audited.

In addition, personal data should be easily retrievable to enable data subjects to exercise their rights to access. It should also be able to blur or obscure third parties who may need such rights to be exercised. This ensures purpose limitation serves all the requirements above on adequacy, relevance and holding what is all round specific to fulfil the purpose of processing should be observed.

Example

Magerere, a land surveyor, uses a drone to capture images of land for boundary and topography assessment but ensures the drone is turned off when individuals are working nearby. This practice aligns with purpose limitation by focusing the recordings solely on the land, avoiding unnecessary capture of personal data, and respecting the privacy of individuals not relevant to the survey.

4.3. DATA MINIMIZATION

This principle requires that entities processing personal data should limit themselves to processing personal data necessary to achieve the purpose of processing. This means collecting only the minimum amount of data required to achieve the purpose for which it is collected.

To fulfil these requirements, the controller/processor must identify the minimum amount of personal data they need to fulfil their purpose. They should hold only that much information, but no more.

To comply with the data minimization principle, institutions should regularly review the data they collect and determine if it is necessary for the intended purpose. This will help to ensure that data is not collected unnecessarily, and that the institution is complying with data protection regulations.

Example:

Masimba County hosts a recorded public town hall meeting to discuss upcoming infrastructure projects. For publishing the recorded media, they only collect essential data from participants, such as their names and email addresses, to notify them when the recording is available. They avoid requesting personal information like home addresses or phone numbers, as it is not relevant to the purpose of sharing the recording.

4.4 ACCURACY

This principle requires data controllers and processors to ensure the accuracy of the personal data they process and be accountable for the processing of recorded media publication. Data controllers and data processors are expected to be put in place measures to ensure that that the data being processed is accurate and up to date. This can be achieved through implementing procedures that verify and validate the accuracy of the information being processed.

Example

The Daily Pulse, a local news website, publishes a story about the effectiveness of chief barazas meetings and includes a photograph to accompany the article. The website's editor mistakenly selects a photo from their archives, believing it depicts the event in question. Unfortunately, the photo chosen is of a political event in a different location, misrepresenting the context and participants in the story.

Upon realizing the error, The Daily Pulse immediately takes corrective measures. First, they replace the inaccurate photo with the correct one depicting the actual event. In addition, the website publishes a formal apology to its readers and clarifies the mistake. To further prevent future occurrences, the editorial team implements a verification procedure for selecting media to ensure accuracy before publication.

4.5 ACCOUNTABILITY

To ensure accountability, data controllers and data processors need to put in place appropriate measures, both technical and organisational, to safeguard against unauthorized access, variation, or loss. There is need to provide employees involved in the processing of personal data with periodic training on their responsibilities to ensure compliance with the requirements under the Data Protection Act and attendant regulations.
Once Data Controllers/Data Processors become aware of any inaccuracies, they should immediately take corrective measures which include correcting the inaccuracies, notifying subjects, and implementing safeguards to prevent re-occurrence. Data Controllers and Processors may also issue notifications/ disclaimers to affected data subjects

4.6 STORAGE LIMITATION

Data controller or data processor shall only keep the personal data in a form which identifies the data subject for as long as it is reasonably needed to fulfill the intended purpose. To comply with the principle of storage limitation the data controller or data processors must therefore develop clear internal procedures for data deletion and destruction, create a data retention schedule outlining what data to be retained and the period of retention. Where data will be kept for an unlimited period, data retention policy should provide realistic time frame for pseudonymization and anonymization together with the rationale behind each decision.

The entities in the audio-visual and recorded media industry should regularly review the personal data they hold, delete, erase or anonymize it when it is no longer needed for its original purpose. They should ensure that it is not possible to re-identify anonymized personal data or recover the deleted one. They should be able to demonstrate each and every action, including providing evidence that the personal data was deleted. For personal data shared with third parties, it is the responsibility of the concern data controller to inform the data processors/third party on principle of storage limitation these should form part of agreements between Data Controllers and Data processors.

Example

Ubunifu University has been experiencing a lot of exam malpractice's therefore affecting the quality of education in that institution. University administration together with examination office decided to install CCTV cameras in all their examination rooms to record and monitor student during exams time, the same recordings can be analysed by examination markers in case there is a sign of cheating in examination papers during marking. The university has an examination marking policy that states that all their exams must be marked, and results released within one month from the day the exams was done.

Below are the steps Ubunifu university can put in place to ensure that the principle of storage limitation is applied effectively

1. Implement a clear data retention policy outlining the duration for which the CCTV recordings can be retained considering the time required for exam marking and any potential appeals or investigations related to exam malpractices and any legal regulatory requirement.
2. Conduct regular audits and reviews of the CCTV storage system to ensure compliance with the data retention policy. This involves verifying that recordings are being deleted in accordance with the established timeframe and identifying any instances of non-compliance.
3. Implement an automated deletion process whereby CCTV recordings are automatically deleted after the specified retention period has elapsed, logs of deletion should be kept as evidence. This helps ensure compliance with the principle of storage limitation by preventing the unnecessary retention of data beyond the required timeframe.
4. Provide training and awareness programs for staff involved in managing CCTV recordings to ensure they understand the importance of storage limitation and adhere to the university's data retention policy.
5. Ensure that they have put in place enough technical and organisational measure to protect CCTV footage from unauthorised access.

4.7. INTEGRITY AND CONFIDENTIALITY

A data controller or data processor handling audiovisual and recorded media should ensure that they have put in place appropriate security measures to protect the personal data they hold. In upholding this principle, data controllers must ensure that audiovisual and recorded media is processed in a manner that ensures its security, protection against unauthorized or unlawful processing, against accidental loss, destruction or damage.

The data controller or data processor should ensure that only authorized persons have access to the recorded media for their processing tasks, and that the images and videos are stored securely and cannot be altered.

Example

Kiti Moto is contracted to take photographs and videos at a wedding in Nairobi. He does a splendid job and retreats to edit and compile the photographs and images for purposes of sharing them with his clients.

In processing the images and videos, Kiti Moto should ensure that he puts in place appropriate security measures to protect the recorded media against loss, destruction or damage. He should also ensure that only people who have authority can access the images and videos and that they are securely stored and cannot be altered by anybody.

APPLICATION OF THE LAWFUL BASIS OF PROCESSING PERSONAL DATA

Section 30 of the Act outlines the various lawful bases that data controllers or data processors can rely on in the processing of personal data.

The lawful bases include when the data subject has consented to the processing for one or more specific purposes, the processing is necessary for the performance of a contract, for compliance with any legal obligation, to safeguard the vital interests of the data subject or another natural person, for the exercise of official authority granted to the controller, and for the data controller's or data processor's own legitimate interests.

Data controller or data processor processing personal data for the publication for recorded media would rely on legal bases such as, consent, the necessity of processing for contract performance, compliance with legal obligations, to safeguard the vital interests of the data subject or another natural person, for the exercise of official authority granted to the controller, and legitimate interests pursued by the data controller or data processors or a third party.

5.1. CONSENT

The Act provides for consent as one of the lawful bases for processing personal data. When relying on consent as a lawful basis, the data controller or data processor is required to obtain express consent from the data subject before taking their photographs and recording videos that contain the data subject's identifiable images. There are instances where images are taken during events, and an individual may be identified in a crowd or a group scene, in such instance, the consent for the identifiable data subject must be obtained. There are instances where images are taken and the event is livestreamed and an individual can be identified in a crowd or a group scene, in such instances the data handler should obtain consent from all individuals who are identifiable in the livestream. This should be done by publicly notifying participants of the livestreaming areas and providing a mechanism for obtaining express consent from the participants.

The consent form should have the following bare minimums:

1. The name of the organisation
2. The names of other controllers and processors who will rely on the consent (other persons to whom the data will be shared)
3. The purposes of the processing - (why you need the data)
4. The type of personal data to be collected and used (what data you will collect)
5. The processing activities to be undertaken (what you will do with the data)
6. Whether the personal data will be subjected to automated decision-making
7. Whether there are any risks of data transfers where there are no appropriate safeguards to protect
8. Provision of the right to withdrawal of consent at any time
9. The consequences of providing, withholding, or withdrawing consent.

For collection and processing of audio-visual and recorded media, data controller or data processor must include notices at events informing the attendees that their photographs,

images, and videos may be taken and may be publicly shared on their website or social media sites. Additionally, the data subjects should be duly informed of the following:

1. At the entrance, there should be a clear consent form which should be filled in and signed by attendees who consent to their images being captured. The consent form should be different from the registration form. In the registration this notice must be included.
2. Give clear notice in writing that photography and audio visual will be at the event.
3. Include a notice regarding audio-visual and recorded media in the printed program or all publicity materials.
4. Provide a clear opt-out (example, those not consenting to processing to say so, or sit in a designated area within the event or wear stickers).

Regarding minors, data controllers and processors are mandated to seek parental consent from the child's parents or guardians prior to processing. In this regard, the parents/guardians must be informed when an identifiable image of the minors and the vulnerable will or has been captured, and a legal basis must be found before the image/recorded media is used in any way.

Example

A parent/guardian in school XYZ gave consent for use of the image of their minor, XYZ school engages Foto Kali for taking images for the minors. XYZ school uses the images for certain prospectus (based on the written, informed and clear consent). Later, the parent/guardian withdraws consent; the school does not need to take any action on all the prospectus that Foto Kali has already distributed. However, Foto Kali would need to stop or cancel production at that moment. If it is an image displayed on social media sites, such photo(s) must be pulled down as soon as possible.

Further, as a data controller/processor, you must inform the guardian/parent what you intend to do with the image of the minor/the vulnerable, including that they will be published on the internet/billboard/articles or any other publication. The image/video must be used strictly for the stated purpose.

Further, the Office has published Guidance Notes on consent that can be accessed here: https://www.odpc.go.ke/

5.2. PERFORMANCE OF A CONTRACT

Data controllers and data processors can rely on performance of a contract as a lawful basis for processing a data subject's recorded media. If publishing of recorded media forms part of a contractual agreement between a data subject and a data controller, then it is considered lawful to process their personal data for this purpose.

Example

Parapanda Agency hired Estelle as an influencer to promote a product for their client, with the contract specifying that videos and images of Estelle would be posted on the agency's social media pages for the duration of the one-year agreement. During this period, Parapanda, as the

data controller, lawfully processed Estelle's personal data, including her image and videos, based on the terms of the contract. This use of her recorded media was in line with the agreed-upon terms and conditions, making it a lawful basis for data processing under the performance of the contract.

However, once the contract ended, Parapanda was no longer legally allowed to use or publish any new images or videos of Estelle for marketing purposes as they no longer had a lawful basis. Importantly, photos and videos already taken and published during the contract period may remain on the agency's platforms unless the contract specifically includes provisions requiring their removal post-agreement.

5.3 LEGAL OBLIGATION

Processing of personal data to ensure compliance with a legal obligation is relied on as a lawful basis of processing where the processing is necessary to ensure that the data controller or data processors complies with a legal obligation placed on them by a law. In relying on this as a lawful basis to process personal data, the data controller or data processor must identify the law that places the obligation on them.

Further, the data controller or processor is also expected to identify the scope of information that the law requires to be processed, to justify the processing necessity. It is important to note that where the law does not provide for the processing of the specific sub-set of information, the expectation will be that the data controller / processors should limit themselves to what is provided. In this specific instance, the law must provide for the publication of personal data processed through audio, visual, or recorded media.

Example

The Kenya Broadcasting Corporation is a government agency established under the Kenya Broadcasting Corporation Act, CAP 221. The Act sets out the mandate of the corporation to include, providing of independent and impartial broadcasting services of information, education and entertainment, in English or Kiswahili or in such other languages as may be decided.

In complying with this legal obligation, the corporation may process personal data for the broadcasting of recorded media such as court proceedings, city council meetings, or public hearings.

The corporation relies on legal obligations as a lawful basis to process personal data to fulfill its duty of transparency and accountability to the public. This processing of personal data is necessary for the agency to comply with its legal obligations in making such recorded media publicly available.

By relying on legal obligations as a lawful basis, the agency ensures that the processing of personal data for publication of recorded media is done in a manner that respects individuals' rights and maintains the integrity of the public record.

5.4. VITAL INTEREST OF THE DATA SUBJECT

Vital interests cover those interests that are essential for someone's life. Therefore, this lawful basis is very limited and in general, only applies to matters of life and death. This basis is likely to be applied when the data controller needs to use a person's personal data for emergency medical care, but the person is unconscious or incapable of giving consent to the processing. Audio-visual and recorded media usually collect massive amounts of personal data which may reveal data of a highly personal nature and sometimes, sensitive data. For instance, if a video surveillance system is used to process sensitive data, the data controller must identify the legal basis for processing such data. If the processing is to protect the vital interest of the data subject or another natural person, the data controller would have to justify it and prove that it is an absolute necessity to safeguard the interest of a person and that the data subject is physically or legally incapable of giving his consent for the processing of his personal data. Additionally, the data controller is not allowed to use the system for any other reason other than the intended purpose.

Example

A surgeon is performing a life threating surgery on Murife and requires taking a photograph or a video recording of the patient for further consultation from a more experienced surgeon that is located in a different hospital. The recording is therefore live streamed to the surgeons and given that Murife is unconscious and cannot give consent, the surgeon can rely on the above legal basis to take the patient's photographs or videos.

There are also exceptional instances where the immediate protection of a child's vital interests necessitates action without prior parental consent, for instance where a child's health or safety is at immediate risk. In such instances, a person who is not a parent or a legal guardian such as a teacher, guided by their professional judgement, ethical considerations and legal obligations can act in the vital best interest of the child. However, in such a situation, the actions of the teacher should be promptly reported to the appropriate authorities and documented according to established procedures.

5.5. PUBLIC INTEREST

The Act provides that personal data may be lawfully processed if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
Entities in this sector may process personal data to safeguard the public interest. However, these entities must ensure that the processing of personal data is done in a way that respects individuals' rights and freedoms, and that appropriate measures are in place to protect the security and confidentiality of personal data.

Example.

As part of the Nyumba Kumi initiative, the chief working together with village elders have installed CCTV cameras in public areas to help prevent and deter crime which has been on the rise. The video recordings from these CCTV cameras capture personal data, including individuals' movements and activities, which is processed to safeguard public security. This processing is done under the lawful basis of performing a task in the public interest. The local chief and village elders ensure that all footage is securely stored, access is restricted, and measures are in place to protect individuals' rights and freedoms, ensuring the confidentiality and security of the recorded media in compliance with Data Protection Act. Clear signage is placed in the vicinity, notifying residents and visitors that they are being recorded

5.6. PERFORMANCE OF A TASK CARRIED OUT BY PUBLIC AUTHORITY

Performing a task carried out by a public authority serves as a lawful basis for processing personal data under certain circumstances. This is provided for under section 30 of the Act, which states that processing is lawful if it is necessary for the performance of a task carried out in the exercise of official authority vested in the controller.
Public authorities for example, the Kenya Yearbook Editorial Board are authorized to process personal data to ensure the carrying out of their mandate.
In simpler terms, if a public authority needs to process personal data to fulfill its official duties, they can do so under this lawful basis. However, it's crucial that such processing is done in accordance with the principles of data protection outlined as outline above, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
It's important for public authorities to ensure they have clear legal grounds and legitimate reasons for processing personal data under this basis, and they should also provide appropriate safeguards to protect individuals' rights and freedoms.

Example

The Kenya Yearbook Editorial Board (KYEB) is a State Corporation established through the Kenya Yearbook Editorial Board Order of 2007.

It is mandated to enhance Government communications and produce publications highlighting developments in all sectors. Kenya Yearbook Editorial Board's publications also promote awareness on the different initiatives by the country's stakeholders. Through its almanac, the Kenya Yearbook, and other sectors specific books and biographies, the Board aims to promote public awareness by ensuring that citizens and the international community understand and appreciate the Government's efforts in promoting development.

In performance of its mandate, the Kenya Yearbook Editorial Board will end up processing personal data for publication of recorded media and the lawful basis that it will rely on will be the performance of a task carried out by a public authority.

5.7. LEGITIMATE INTEREST

One of the legal bases for processing personal data under the Act is legitimate interest. Section 30(1)(b)(vii) of the Act lawfully allows processing, including audio visual and recorded media if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller or a third party, unless such interests are overridden by the data subject's legitimate interest or is unwarranted in any particular case having regards to the harm and prejudices to the rights and freedoms of the data subject. Therefore, the controller should consider that if the data subject objects in accordance with Section 26, the controller can only proceed with processing if it is a compelling legitimate interest which overrides the interests, rights and freedoms of the data subject.

The legitimate interest must be real and a present issue (i.e. it must not be fictional or speculative). A real-life situation of distress needs to be at hand, such as damage or serious incidents in the past, in the case of video surveillance. The controller may need to document relevant incidents (date, manner, financial loss) or records as the documented records can be strong case/evidence for the existence of a legitimate interest. Legitimate interest needs to be reassured at periodic intervals (biannually, annually depending on the circumstances). A legitimate interest assessment (LIA) can help demonstrate lawfulness and the need of processing.

Example

A supermarket wants to install video surveillance to prevent shoplifting and vandalism. Ideally, the cameras should only be filming the premises itself as it is not necessary to watch the neighboring premises. However, according to statistics, there is a high expectation of vandalism

and shoplifting in the area. Experience from neighboring supermarkets also shows a high level of vandalism.

This shows cause for legitimate interest in fixing surveillance cameras beyond the inside of the premises. It is thus not necessary that the damage must have occurred to the supermarket. If damage in the neighborhood suggests a danger or similar. However, the statistics must relate to the area in question and not just general and random statistics/records.

Example

Kazi Ngumu Limited publishes a notice in a newspaper stating that a former employee no longer works for them to prevent unauthorized business dealings. In this case, Kazi Ngumu Limited must ensure that the publication is necessary to protect its legitimate interest, such as safeguarding its reputation, while also ensuring that the notice does not harm the ex-employee's rights or reputation unnecessarily.

6. RIGHTS OF A DATA SUBJECT

Data subject rights are an essential component of data protection and privacy laws. These rights empower individuals to have control over their personal data and how it is used by institutions. The importance of data subject rights cannot be overstated, as they serve to uphold the fundamental right to privacy and the protection of personal information.

These rights are crucial in ensuring that individuals have a say in how their personal information is handled, and they provide a mechanism for individuals to hold organisations accountable for their data processing activities. By exercising these rights, data subjects can actively participate in the management and protection of their personal data, ultimately contributing to a more transparent and privacy-respecting digital environment.

When it comes to the processing of personal data for publication of audio visual or recorded media, this guidance note elaborates on how data subjects can exercise their rights and how institutions that are processing the personal data can ensure that data subjects are afforded the opportunity.

6.1. RIGHT TO BE INFORMED

The right of the data subject to be informed is a fundamental aspect to data protection. This right ensures that individuals have the right to be informed about the collection and use of their personal data. In compliance with this right, data controllers and data processors are required to provide clear and transparent information to data subjects about how their data will be collected and processed, for what purposes, by whom, how long the information will be kept and whether the information will be shared with any other third parties. Where data controllers and data processors provide this information to data subjects, it helps individuals make informed decisions about their personal data and empowers them to exercise control over their information.

Prior to the commencement of the processing, where reasonably practicable, data controllers or data processors are expected to ensure that this information is provided to the individuals, and this could be done using various means.

Example

A government institution is holding a public participation event with the aim of receiving views from the public on the proposed law that will greatly impact all the individuals in that specific area.

In line with the constitutional requirements of public participation, the government institutions advertise the venue and purpose of the event and the venue on TV stations, radio stations, and newspapers.

In the advertisement, the institution indicates that the proceedings will be recorded and broadcast on the national television channels and the print media. Also, the advertisement provides the purpose for the broadcast and the lawful basis in line with the institution's mandate.

By providing this information in the advertisement, the institution has been able to comply with the rights of individuals to be informed of the processing of their personal data.

6.2. RIGHT TO ACCESS PERSONAL DATA

The right to access personal data gives individuals the right to obtain a copy of their personal data from the entity processing it. This is a fundamental right that helps individuals to understand how and why data controllers and data processors are using their data and to ascertain the lawfulness of the processing.

In exercising this right, individuals have the right to obtain the following information from the data controller or data processor; a confirmation that the individuals' personal data is being processed, a copy of their personal information and any supplementary information in relation to the processing of their personal data, such as the identity of any other third parties their information may have been made available to.

In complying with this request, data controllers and data processors will be expected to provide information of a similar nature to the information that was provided to the individual at the point of collection, including; the purpose of processing, categories of personal data, identity of the third parties that have received the personal data, the retention period of the personal data and the source of the personal data, where the information was obtained indirectly.

Example

A university student consents to having their image used for a specific graduation photo album and program. However, later, they discover that their image was also captured in a promotional video for the school and shared online, a use they did not agree to. Concerned about this new use of their personal data, the student exercises their right to access and requests the university's records to confirm the processing of their image.

The student asks for a copy of the video, an explanation of how their image is being used, whether it has been shared with third parties, and how long the footage will be retained. In response, the university, adheres to the right to access by promptly providing this information, ensuring transparency and allowing the student to verify whether the extended use of their recorded media is lawful and within the scope of their original consent.

To exercise their right to access personal data in relation to the processing of personal data for the publication of recorded media, a data subject can submit a request to the data controller. This request should clearly state the specific personal data that the data subject wishes to access, as well as the purpose for which the data is being processed. The data controller is then obligated to provide the data subject with access to their personal data within a reasonable timeframe. This may include providing copies of the personal data and any relevant information about the processing activities. It is important for the data subject to be

aware of their rights in this regard, and to understand how to effectively exercise them to ensure transparency and accountability in the processing of their personal data for the publication of recorded media.

Note that in exercising this right, individuals are entitled to their own personal data. The only instance where an individual would be entitled to the personal data of another would be where they are acting as a parent or guardian of a child, or they have been appointed as a guardian by the court, or with the authorization of the individual

6.3. RIGHT TO ERASURE

In processing of personal data for the publication of recorded media, a data subject has rights, to which the data controller or data processor must give effect where applicable. Data subjects have, for example, the right to erasure ('the right to be forgotten') without undue delay if:

a) Personal data are no longer necessary in relation to the purposes for which they were processed.
b) The data subject withdraws consent and there are no other legal grounds for processing.
c) The data subject objects and there is no overriding legitimate grounds for processing.
d) The person data have been unlawfully processed

Example

A small fitness studio posts class photos on their social media to promote their sessions. One of the participants, Miady, had originally consented to appear in the photos, which were lawfully posted during the period when her consent was valid. Later, Miady requested that the studio remove any images of her from their social media platforms, stating that she no longer consents to the use of her image for promotional purposes.

While Miady is entitled to withdraw her consent at any time, it is important to note that the withdrawal of consent does not affect the lawfulness of the processing that occurred while her consent was still valid. In this case, the studio's posting of the photos during the period when Miady's consent was in place was lawful. However, once Miady withdraws her consent, the studio must comply by promptly deleting any images of her that are still being used, as the photos are no longer necessary for the original purpose, and she has exercised her right to erasure.

A data subject also has a right to rectification, without undue delay, of inaccurate personal data. If a data controller or processor becomes aware of any inaccuracies in the personal data being processed, they are obligated to ensure correct information is used for any further processing.

6.4 RIGHT TO RECTIFICATION

This means that individuals have the right to request corrections to inaccurate or incomplete information about them. They must implement a process and the technical capabilities to verify the request, correct the data, and confirm correction with the data subject.
In addition, this also applies to data the data controller passed on to third parties, they need a process to securely inform them of the correction. Overall, the right to rectification of personal data is important for ensuring that individuals have accurate and complete information.

Example.

A local newspaper published an article about a charity event and mistakenly uses a photo of Kamotho, a local teacher, instead of Kamotho, the event's organizer. The teacher submits a request for correction. The newspaper verifies the request, replaces the incorrect photo with the correct one, and issues a public correction in the next edition. Additionally, they notify any third parties or syndicates that may have received the original article with the wrong photo to ensure the error is corrected across all publications.

6.5 RIGHT TO DELETION

In the processing of personal data for the publication of audio-visual and recorded media, a data subject within the definition of the Act has rights under Section 26 (e) to the deletion of false or misleading data about them. Instances where one can request for deletion of their data can be;

1. The data subject's image or video was obtained without their consent.
2. Consent is withdrawn and there are no other legal grounds for processing.

Example

Okonkwo Bar and Restaurant normally takes photographs and videos of their clients and posts them on their social media pages. Wanjiku noticed that a photo of her was posted without her consent. She raised the issue with the entity, and they pulled down the image within 14 days as required under the General Regulations.

6.6. RIGHT TO OBJECT

Generally, the right to object applies to all data subjects in respect to processing of their personal data. However, where the data controller/processor demonstrates compelling legitimate grounds that override the rights and interest of the data subject, then the processing may continue based on those grounds. The controller or processor must however inform the

data subject of the reasons for declining the request for objection and the data subject's right to lodge a complaint to the Data Commissioner.

Nonetheless, the data subjects rights to object becomes absolute in as far as the processing relates to direct marketing which includes profiling to the extent that relates to such direct marketing. This means that the controller cannot continue processing the data subject's personal data for whatever reason if the use of the data subject's personal data is for direct marketing.

Example:

Vuvuzela, a popular prankster, posted a video on their platform showcasing one of his pranks in a crowded city park. Following this, one person in the video contacted Vuvuzela, requesting the removal of their appearance from the footage citing their right to erasure under Data Protection Act. Vuvuzela reviewed the request and recognized that the individual's personal data was not necessary for the intended purpose and in any case, the individual had withdrawn their consent for the use of their image, and there were no other legal grounds for processing the data. Vuvuzela promptly edited the video to blur the individual's appearance

6.7. RIGHT TO DATA PORTABILITY

The right to data portability as provided in Section 38 of the Act gives the data subject the right to apply to port or copy their personal data held by a data controller or a data processor to another. When data controller or data processor receives such request, they are required to comply with data portability requests, at reasonable cost and within a period of 30 days and provide the data subject with personal data concerning them in a structured, commonly used and machine-readable format and in a situation where the portability request is complex or numerous, the data controller or processor my request for extension of compliance time.

However, the right to data portability is subject to certain conditions and exceptions. The right shall not apply in circumstances where:

i. The request for data portability may affect the rights and freedom of others
ii. Data processed is based on other legal basis such as legitimate interest, public interest, or legal obligation.

In situations where the data controller or processor declines to comply with the request for data portability from the data subject, the office may decide on the same. The right to data portability in audio-visual and recorded media sector allows data subjects to move, copy or transfer personal data easily without hindrance from one data controller or processor to another and reuse it.

Example

Jay had a complex surgery at Niponye Hospital, and during his hospital stay, various audiovisual recordings and photographs were taken for medical documentation purposes. These recordings and photographs include videos of the surgery, medical imaging scans, and photos of Jay recovery progress.

After Jay's discharge from the hospital, he decides to seek a second opinion from another medical facility, "Salama Hospital," located in a different County. Under the data subject rights for data portability, Jay has the right to request a copy of his personal data, including the audiovisual recordings and photographs, from Niponye Hospital.

Jay submits a formal request to Niponye Hospital for his data portability rights. The hospital acknowledges the request and begins compiling Jay's medical records, including the audiovisual materials.

6.8. AUTOMATED INDIVIDUAL DECISION MAKING

Generally, every data subject has a right not to be subjected to a decision based solely on automated processing unless it is necessary for entering into or performing a contract between a data subject and a data controller; is authorized by law; or is based on the data subject consent.

Simply defined, Automated decision making means algorithmic decision made based on factual data, as well as digitally created profiles or inferred data. This therefore means that such decisions have a high likelihood of exposing the data subject to profiling or likely dangers/risks to their rights and freedoms.

In audiovisual and recorded media, personal data are almost always a subject of automated decision making. The guidelines provides that subject to the exemptions in Section 35 of the Act, before a data controller or data processor subjects a data subject to automated decision making, the controller/processor must ensure that:

1. The data subject is well informed about the logic involved.
2. The rights of the data subject to oppose profiling are present and made known
3. The data subject's consent is obtained in a clear written and well-informed manner
4. A data protection impact assessment is carried out by the data controller or data processor

Example 1

A publishing company uses an automated system to determine which authors' works to feature on their website based on various criteria such as sales data and reader reviews. Emma, an author whose book was not featured, learns that the decision was made entirely by the automated system without human review.

She expresses her concern about being subject to automated decision-making and asserts her right to not be subject to such decisions. The publishing company must comply by ensuring that her request is reviewed and considered by a person rather than relying solely on the automated system. This ensures that her right to avoid solely automated decisions is respected and that any decisions impacting her work are made with human oversight.

This approach prevents discrimination against authors like Emma and ensures that their rights are respected.

Example 2

Jimbo App uses facial recognition technology to automatically tag users in photos and videos posted by others. When a user uploads a video from a public event, the platform's automated system identifies and tags individuals who attended the event without seeking their explicit consent for this tagging process. Jimbo App must ensure that before applying such automated decision-making, individuals are informed about the technology used, how the tagging process works, and their right to opt out of being automatically tagged.

7.1. DATA PROTECTION POLICIES AND RETENTION SCHEDULES

As a data controller or processor, the law requires that you must have policies, procedures and regulations (documentation) in place to regulate the processing of personal data. The data protection legislations explicitly require controllers and processors to document their processing activities and maintain records on several things such as processing purpose, data sharing and data retention. These documents must be kept in writing. The data commissioner may, on request, require that the documents/records be made available.

Regulation 23 of the Data Protection (General) Regulations, 2021 obligates data controllers and processors to develop, publish and regularly update a data protection policy (some times known as privacy policy or notice). The policy is to serve as an external document notifying the data subjects on how their data is being used. This policy must be brought to the attention of all subscribers prior to the collection of their personal data or as soon as possible. The data protection policy should be provided to subscribers upon request and free of charge.

When drafting the data protection policy, the following several practical tips and consideration should be in place to ensure it effectively communicate to data subjects how their personal data will be used, these include:

1. The policy should be written in clear and plain language that is easy to understand. Technical or legal jargon should be avoided as much as possible to ensure that data subjects can easily comprehend what the policy says.
2. The policy should be transparent and comprehensive, covering all the relevant information that data subjects need to know about processing of their personal data. This include information about the rights of data subjects under the Act, the fact that personal data is being collected, the purpose for which the personal data is being collected, the third parties to whom the data may be transferred, and any safeguards in place to protect the data.
3. The policy should be accessible to data subjects. This can be achieved by making it available on the data controller's or data processor's website, or by providing a copy upon request.
4. The policy should be reviewed and updated regularly to reflect any changes in data processing practices or in relevant laws and regulations.
5. Visual aids such as infographics and diagrams can be used to help convey complex information.

To make the policy easy for the data subject to understand, the controller/processor may use questions and answers format or break down the policy into shorter sections with clear headings to make it more digestible for data subjects. Providing examples of how personal data may be used in practice can also help data subjects to understand the policy and the implications of sharing their personal information.

7.1.1. DATA RETENTION AND DISPOSAL SCHEDULE / POLICY

Other than the data protection policy, the controller/processor under Section 39 of the Act is required to have a data retention and disposal policy. Unlike the data protection policy, this policy is an internal document that the controller/processor develops to ensure its internal practices align with the Data Protection Act. The policy must be provided in simple and clean plain language and must be aligned to other legislative requirements on data retention and disposal.

7.2. DATA SHARING AGREEMENTS

A data controller or processor may be required to share or exchange the audio-visual and/or recorded media containing personal data, upon request by another data controller, data processor or a third party. However, data sharing must adhere to the principles of confidentiality, privacy, and informed consent. The data controller must establish clear data sharing agreements to allow them to share audio-visual and recorded media containing personal data. The person requesting audio-visual and recorded material that contains personal data must do so in writing. This can be through a letter or email, and the person should provide proof of the request. The request should also specify the reasons for requesting personal data, the duration for which personal data shall be retained and the requesting entity should have appropriate safeguards in place to secure the requested personal data from illegal disclosure.
A data sharing agreement must contain the type of information to be shared; in this instance, the specific audio-visual and recorded media to be shared. The agreement must also specify how the information will be shared and indicate the safety measures in place to ensure the information is shared securely and that it is shared with the right person. Further, the agreement should provide for the technical and organisational measures in place to ensure the security of the shared audio-visual and recorded media. The agreement should contain the intended retention period of the personal data and deletion procedures where the data subject can request deletion of personal data shared.

7.3. DATA PROTECTION IMPACT ASSESSMENTS

Section 31 of the Act requires the data controllers and data processors to carry out DPIA in a situation where a processing of personal data 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 data controller or data processor shall, prior to the processing, carry out a data protection impact assessment (DPIA). In instances where it is not clear whether DPIA is required, it is recommended that you carry out a DPIA nonetheless. DPIA will enable data controllers and data processors in audio-visual and recorded media industry to identify privacy risks and evaluate the effectiveness of the controls put in place to mitigate the risks. DPIA is a useful tool to help data controllers and data processors comply with the data protection laws.

Example

A marketing agency is planning to launch a promotional campaign for their new product. The campaign will involve capturing images and videos of people using the product in various settings, such as outdoor locations, events, and urban environments. The audio visuals will be used in online advertisements, social media posts, and on promotional materials. It is advisable to carry out and submit a DPIA to the ODPC

The Office has published a Guidance Note on Data Protection Impact Assessments, accessible via www.odpc.go.ke. This resource provides the required form for submitting a Data Protection Impact Assessment. The form should be submitted to the office 60 days prior to processing personal data.

7.4. REGISTRATION

The Act states that subject to prescribed mandatory registration thresholds or exemptions, no person shall act as a Data Controller or Data Processor unless registered with the Data Commissioner. Therefore, all Data Controller and Data Processors MUST register unless an Entity can clearly identify that they fall within an exemption.
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.

7.5. DUTY TO NOTIFY

Data controllers and data processors must inform data subjects about the collection and use of audio-visual and recorded media that contain their personal data. This duty to notify includes providing the data subject with information including their rights specified in the Act, information about the purposes of collecting and processing their personal data, disclose any third party who may receive and have access to their personal data and the safeguards adopted by the third party, description of the technical and organisational security measures in place to secure their personal data and if there are any consequences if the data subject fails to provide all or part of the requested data. Data controllers and processors should have all this information in a data protection policy which should be availed to the data subject before collection of their personal data.

In drafting the privacy policy, it is important to use clear and plain language that the data subject can easily understand. The policy should be comprehensive and covers all relevant information that data subjects need to know about the processing of their personal data, including their rights, the purpose of data collection, third-party recipients, and safeguards in place to ensure security of their personal data. The policy should be readily available and accessible to data subjects, for example, by providing it on the organisation's platform such as their website or upon request by the data subject. There should be regular reviews and updates

to ensure that the policy reflects any changes in data processing practices or relevant laws and regulations.

7.6. NOTIFICATION OF BREACHES

A data breach refers to a security incident where personal data is accessed, disclosed, or used by unauthorized individuals or entities. Unauthorized access can occur through various means such as hacking, malware, phishing attacks, physical theft of devices or files containing personal data.

Where a data breach occurs, a data controller must report personal data breaches to the Office without delay within 72 hours of becoming aware of them. 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 discovered, 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 affected, and the potential harm to affected data subjects. The entity must also provide information on any action taken to mitigate the harm and remedy any failure or shortcoming that contributed to the breach, and how affected individuals can mitigate potential harm.

Where there has been unauthorized access, data controllers 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.

7.7 PRIVACY BY DESIGN AND DEFAULT

Data protection by design is a concept that refers to the incorporation of data privacy and security measures into the design of products, services, and systems from the very beginning, rather than as an afterthought.
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 necessary 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 institutions in the audio-visual and recorded media sector to ensure that only data necessary to achieve your purpose is processed. Data protection by default requires entities to ensure that data protection issues have already been considered, and protection methods incorporated into existing systems and practices. This could be achieved by institutions in the audio visual and recorded media sector specifying the personal data required before the processing starts, appropriately informing individuals and only processing the personal data needed for the specific purpose.

APPENDIX: COMPLIANCE CHECKLIST

	Description	Yes	No	Comments/ Remedial Actions
1.	We respect the right to privacy as a fundamental human right as provided by Article 31(c) and (d) of the Constitution.			
2.	We have identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (DPA).			
3.	In publication of recorded media, we process sensitive data, we have identified permitted grounds under section 44 of the DPA			
4.	We restrict processing where the legal basis or legitimate interest ceases to apply.			
5.	We do not do anything generally unlawful with personal data or inconsistent purpose for processing.			
6.	If we are subject to mandatory registration, we have submitted to the Office of Data Protection Commissioner (ODPC) accurate and up to date information concerning our processing activities.			
7.	We have considered how the processing may affect the individuals concerned and can justify any adverse impact.			
8.	We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified			
9.	We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject			
10	We do not deceive or mislead people when we collect their personal data			
11.	We have clearly identified our purpose or purposes for processing and have clearly documented those purposes			
12.	We include details of our purposes in our privacy notices.			
13.	We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation			
14.	If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose, or we obtain specific consent for the new purpose.			

15.	We use technical measures to limit the possibility of repurposing personal data.			
16.	We can demonstrate the relevance of the data to the processing in question.			
17.	We periodically review the data we hold and delete anything we don't need.			
18.	We avoid the creation of more copies or entry points for data collection than is necessary.			
19.	We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
20.	We ensure the accuracy of any personal data we process and the reliability of our sources.			
21.	We have appropriate processes in place to check and verify the accuracy of the data we collect, and we record the source of that data			
22.	We carry out tests for accuracy at critical steps.			
23.	We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain			
24	We have a process in place to identify when we need to keep the data updated to fulfill our purpose properly, and we update it as necessary.			
25	We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of personal data.			
26	As a matter of good practice, we keep a note of any challenges to the accuracy of personal data.			
27	We know what personal data we hold and why we need it.			
28	We carefully consider and can justify how long we keep personal data.			
29	We have a policy with standard retention periods where possible.			
30	We regularly review our records with a view of identifying personal data that no longer requires to be retained and delete or anonymise such data.			
31	We have appropriate processes in place to comply with individuals' requests for rectification and/or erasure of false or misleading data about them.			

32	We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes			
33	We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards or valid consent from the data subject.			
34.	We checked and fulfilled all conditions set under part VI of the Act and General Regulations 2021			
35.	We have clearly identified our purpose/purposes for processing			
36.	We have documented those purposes			
37.	We include details of our purposes in our privacy notices			
38.	If one of the purposes is direct marketing, we make sure that the data subject is notified that direct marketing is one of the purposes for which personal data is collected or consented to the use of his/her data for the purpose of direct marketing and on any case, is provided with simplified opt-out mechanism.			
39.	We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.			
40.	If we plan to use personal data for a new purpose, we check that this is compatible with the original purpose, or we obtain specific consent for the new purpose.			
41.	Are personal data anonymized or pseudonymized where possible to protect individuals' identities?			
42.	Are procedures in place for notifying relevant authorities and affected individuals in the event of a data breach?			
43.	Are agreements in place to ensure third parties processing recorded media comply with data protection standards?			
44.	Is due diligence conducted to ensure third parties and contractors handling recorded media protect personal data appropriately?			