

**ARTICLE 19**

# **Balancing free expression and data protection: The journalistic exemption in Kenya**

NOVEMBER 2024

**SUPPORTED BY**



First published by ARTICLE 19, November 2024

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices.

Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our nine regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on five key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

E: [kenya@article19.org](mailto:kenya@article19.org)

W: [www.article19.org](http://www.article19.org)

Fb: @article19easternafrik

T: +254 727862230

Tw: [@article19eafric](https://twitter.com/article19eafric)

A19/EAF/2023/[978-9966-084-21-7]

© **ARTICLE 19 Eastern Africa, November 2024**

This publication was produced with the financial support of the European Union (EU) and the German Federal Ministry of Economic Cooperation and Development (BMZ) under the Our Data, Our Voice project, implemented by the GIZ Digital Transformation Center (DTC) Programme. The publication contents are the sole responsibility of GIZ DTC and ARTICLE 19, and do not necessarily reflect the views of the EU or the BMZ.

This work is provided under the Creative Commons Attribution-NonCommercialShareAlike 4.0 license.

You are free to copy, distribute, and display this work and to make derivative works, provided you:

- give credit to ARTICLE 19;
- do not use this work for commercial purposes;
- distribute any works derived from this publication under a license identical to this one.

To access the full legal text of this license, please visit:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used. ARTICLE 19 bears the sole responsibility for the content of the document.

# Contents

<b>Executive summary</b>	<b>4</b>
Report recommendations	4
<b>Abbreviations</b>	<b>1</b>
<b>Glossary</b>	<b>1</b>
<b>Introduction</b>	<b>1</b>
Research methodology	1
Report structure	1
<b>1 Free expression and data protection</b>	<b>2</b>
Media freedom, the right to free expression, and access to information	2
Data protection	3
The nexus between free expression and data protection	4
<b>2 The journalistic exemption</b>	<b>6</b>
What is the journalistic exemption?	6
Scope of the exemption	6
Criteria for applying the exemption	9
Processing for the purpose of journalism	9
Processing with the aim of publication	10
Reasonable belief that publication is in the public interest	10
Compliance is incompatible with journalism	11
Compliance with codes of practice	11
<b>3. Survey: data protection awareness and practice in the media sector</b>	<b>2</b>
Methodology	2
The respondents	3
Awareness about data protection	6
Digital security practices	8
Training and resources	11
<b>Recommendations</b>	<b>14</b>
<b>Notes</b>	<b>15</b>

## Executive summary

This report provides an overview, based on desk research, of the legal and policy frameworks relating to privacy, freedom of expression, data protection, and the journalistic exemption in Kenya and beyond. It explores the scope of, and justifications for, the journalistic exemption from data subjects' data protection and privacy rights. It examines the need for greater specificity on the scope of the exemption, including by contrasting it with the European Union and United Kingdom's comparable legislation.

The second section goes on to consider the media's obligations to comply with areas of the Data Protection Act, even when relying on the journalistic exemption from certain provisions. Section 2 therefore first lays out the media's responsibility and obligation to comply with data protection principles of data security and accountability. Section 2 then goes on to detail the findings of a survey ARTICLE 19 conducted of Kenyan media practitioners' awareness and practices regarding data protection issues in relation to journalism. The findings of this survey can inform media leaders of the need for increased training and support on the issues covered in this report.

Our desk and survey research shows that:

- overall that the journalistic exemption plays a crucial role in balancing the right to privacy with the right to free expression, free media, and the public's right to access information.
- The scope of the journalistic exemption in Kenya needs to be clearly defined so that the media sector may know which provisions of data protection legislation may be derogated from provided that the criteria are met.
- Further work is needed to increase levels of awareness in the media sector of data protection obligations and of the journalistic exemption in Kenya, and training and other support is needed to strengthen data protection-related compliance in the media sector.

## Report recommendations

Kenya's Office of the Data Protection Commissioner should give effect to both freedom of expression and the right to privacy, and not unduly limit the right to free expression and access to information in the context of journalism.

Specifically, the ODPC should:

- Clarify and define the scope of the journalistic exemption under the Data Protection Act 2019 including which derogations are permissible under the exemption.
- Clarify that the journalistic exemption extends to work that involves material that is newsworthy and in the public interest.
- Require media organisations to publish and review their editorial policies relating to personal data protection and privacy, and to train staff on their policy.

- Encourage digital media practitioners to comply with the Code of Conduct for Digital Media Practitioners.

Kenyan media organisations should:

- Publish and regularly review policies relating to personal data protection and privacy.
- Train new staff – and retrain existing staff – on the policies, particularly in areas of balancing between privacy and free expression.

Kenyan digital media practitioners should commit to comply with the country's Code of Conduct for Digital Media Practitioners.

## Abbreviations

ACHPR	African Commission on Human and Peoples' Rights
CATI	computer-assisted telephonic interview(s)
CFREU	Charter of Fundamental Rights of the European Union
DPA	Data Protection Act (Kenya)
EU	European Union
GDPR	General Data Protection Regulation (EU)
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office (UK)
ODPC	Office of the Data Protection Commissioner (Kenya)
OSCE	Organization for Security and Co-operation in Europe
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations

## Glossary

For the purposes of this report, the following terms have these meanings:

**Data subject.** The individual whose data is being processed, for example website visitors, clients, employees, and contractors.

**Personal data.** Information relating to an identified or identifiable natural person, which may include name, age, sex, etc.<sup>1</sup>

**Processing.** Any action performed on data, whether automated or manual. Examples include gathering, recording, organising, structuring, storing, utilising, and deleting data.

**Sensitive personal data.** Data that reveals a natural person's ethnicity, health status, social origin, personal beliefs, genetic or biometric data, property details, marital status, family details (including names of the person's children, parents, or spouse(s)), or sexual orientation.

# Introduction

## Research methodology

This report is the outcome of a combination of desktop and survey research ARTICLE 19 undertook between January 2023 and July 2024. The desktop research focused on the legal and policy frameworks relating to privacy, freedom of expression, data protection, and journalistic exemption in Kenya. We drew on decided cases, and legal and policy frameworks, in both Kenya and other jurisdictions, to explore the scope of the journalistic exemption from data subjects' right to privacy and to protection of personal data, and the justifications for this exemption.

The desk research also included study of the data protection policies of media houses in Kenya to understand media industry practice regarding data protection and free expression. Additionally, ARTICLE 19 undertook a survey to collect quantitative data on Kenyan media practitioners' awareness of the data protection framework and current data protection practices through computer-assisted telephonic interviews (CATI) and focus group discussions between 9 and 13 January 2023.

## Report structure

We have structured the report as follows.

**Section 1** looks at the legal framework for data protection, freedom of expression and the journalistic exemption, and illustrates the need for further detail to be provided by Kenya's Data Protection Commissioner on the scope of the exemption.

- Chapter 1 contextualises the journalistic exemption through a review of the legal framework, in Kenya and beyond, relating to media freedom, the right to free expression and to access to information, and data protection and privacy, and considering how free expression and data protection relate to one another in this framework.
- Chapter 2 focuses on the journalistic exemption, its scope, and its application criteria in Kenya. It brings in comparisons and case examples from the European Union (EU), United Kingdom (UK), and other jurisdictions, to show how the exemption can and should be applied in practice, and to underline the need for further specificity to be provided on the scope of the Kenyan exemption.

**Section 2** looks at the obligations of media practitioners to comply with data protection requirements and the levels of knowledge and good practice currently within the media industry.

- Chapter 3 considers the media's responsibility and obligation to comply with data protection principles of data security and accountability.
- Chapter 4 details the methodology and results of our media sector data protection awareness survey.

The recommendations section provides practical proposals for a Guidance Note on data protection and the journalistic exemption.



# Section 1: The legal landscape

# 1 Free expression and data protection

The right to free expression is entrenched in various human rights instruments including Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

Article 19 of the ICCPR states:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Article 9 of the African Charter on Human and Peoples' Rights states that 'Every individual has the right to receive information' and 'to express and disseminate [their] opinions within the law'.<sup>2</sup>

## **Media freedom, the right to free expression, and access to information**

A free, independent, and pluralistic media is one of the most fundamental tenets of a democratic society. The media plays a key role in investigating and sharing information and ideas on issues of public interest, keeping the public informed, and enabling the public to fully participate in society, economically, socially, and politically.

The Organization for Security and Co-operation in Europe (OSCE) states that free media is important because 'no nation can hope to develop democratically without the free expression, publication and distribution of ideas and opinions'.<sup>3</sup> With this realisation, Principle 11 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa places an obligation on the state to promote a pluralistic and diverse media that facilitates the free flow of information and ideas and make these accessible in local languages.<sup>4</sup>

The right to freedom of expression and access to information is a key enabler of media freedom and of the practice of journalism centred on freedom to investigate, know, speak, and inform.

The Charter of Fundamental Rights of the European Union (CFREU) requires that, while exercising the right to freedom of expression and access to information, media freedom and pluralism shall be promoted.<sup>5</sup> General Comment 34 of the United Nations Human Rights Committee explores the relationship between free expression and media freedom, stating that free expression allows the free press to comment on public issues without censorship or restraint and to inform public opinion, while citizens have a corresponding right to receive media output.<sup>6</sup>

The Declaration of Principles on Freedom of Expression and Access to Information in Africa states that the right to express oneself through practising journalism should not be subject to

undue legal restrictions,<sup>7</sup> further emphasising journalism as a key mode of exercising the right to free expression. In addition, the Declaration of Principles places an obligation on the state to promote a diverse and pluralistic media to facilitate citizen access to information.<sup>8</sup>

The freedom and independence of the media is guaranteed under Article 34 of Kenya's Constitution of 2010.

### Data protection

Data protection is part of the broader framework of the right to privacy. The right to privacy is key to maintaining the dignity of a person by allowing each individual a space free of intrusion from either the state or other individuals. While privacy relates to the protection of private affairs, data protection involves the regulation of the processing of personal data that may be in either the public or the private domain. It refers to the processes and procedures that ensure data is processed fairly, transparently, and securely.

Data protection creates obligations for data controllers and data processors and rights for data subjects.

The rights of the data subject include, among others:<sup>9</sup>

- a) Right to access data held about them by data controllers or processors and to be informed of the purpose of processing;
- b) Right to object to the processing of all or part of their personal data, for example to object to use of data for commercial purpose or profiling;
- c) Right to rectification of inaccurate or misleading data;
- d) Right to erasure, that is, the deletion of data where it is inaccurate, misleading, no longer necessary, irrelevant, or unjustifiably made public; and
- e) Right to data portability, which includes the transmission of data on an individual held by one controller or processor to another.

Several international frameworks such as the ICCPR and the UDHR provide for the right to privacy prohibiting arbitrary or unlawful intrusion into a person's family, home, or correspondence and unlawful attacks on their honour or reputation.<sup>10,11</sup>

In addition to international frameworks, regional frameworks also provide for the right to privacy and data protection. In Europe, the Charter of Fundamental Rights of the European Union (CFREU) provides for both the right to privacy (respect for private and family life)<sup>12</sup> and the right to data protection. The latter ensures data is processed for a lawful purpose and gives individuals data protection rights overseen by an independent authority.<sup>13</sup>

The African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) provides a regional framework for the regulation of personal data. It provides for the creation of independent national bodies to oversee the implementation of any legislation on data protection at the national level, principles of data protection, rights of data subjects, and

obligations of data controllers.<sup>14</sup> The Declaration of Principles on Freedom of Expression and Access to Information in Africa also requires that data be processed for a lawful purpose according to the principles of data protection and provides data subjects with data rights.<sup>15</sup>

In Kenya, Article 31 of the Constitution provides for the right to privacy, which includes individuals' right not to have:

- a) their person, home, or property searched;
- b) their possession seized;
- c) information relating to their family or private affairs unnecessarily revealed; and
- d) the privacy of their communications infringed.

In 2019, Kenya enacted the Data Protection Act (DPA 2019) to provide a legal framework that further gives effect to Article 31(c) and (d) by regulating how personal information is collected and processed, establishes data protection rights, and creates the office of the Data Protection Commissioner to oversee implementation of the Act.

### **The nexus between free expression and data protection**

Freedom of expression is not absolute and is subject to certain limitations prescribed under Articles 19(3) and 20 of the ICCPR. Such limitations or restrictions are justifiable where they are:

- a) Provided by law – the law must be accessible and precise, overseen by an independent body, and include safeguards against abuse;<sup>16</sup>
- b) In pursuit of a legitimate aim – the restriction must have a genuine purpose, which may include protecting the rights and freedoms of others, and the protection of national security and public order; and
- c) Necessary and proportionate – where the least restrictive means is employed.

Equally, the 2021 Report of the Special Rapporteur on the right to privacy pointed out that the enforcement of an individual's right to privacy and data protection may be limited by another individual's right to legitimate free expression and vice versa. A balanced approach is thus necessary to facilitate the full enjoyment of both rights.<sup>17</sup>

The Constitution of Kenya broadly provides for the right to free expression,<sup>18</sup> free and independent media,<sup>19</sup> access to information,<sup>20</sup> and the right to privacy.<sup>21</sup> However, these rights to free expression and free media do not extend to propaganda for war, incitement to violence, advocacy for hatred, or hate speech.<sup>22</sup> Additionally, when exercising these rights every person is required to respect the rights and reputation of others.<sup>23</sup>

Article 24 of the Constitution provides for the factors to consider when determining if a limitation to a right is reasonable and justifiable.<sup>24</sup> Among these factors is the need to ensure the enjoyment of a right by one individual does not prejudice the enjoyment of the rights of others. This balancing test is needed to ensure the right to data protection and privacy does not unduly

limit the right to free expression and vice versa. Under Kenyan law, therefore, the rights to freedom of expression and to privacy are not absolute.

While developing the Global Principles on Protection of Freedom of Expression and Privacy, ARTICLE 19 noted that while freedom of expression and privacy are often mutually reinforcing, they sometimes come into conflict, 'including where privacy claims may be used without justification to prevent the dissemination of information about individuals in order to restrict reporting on matters of public interest and to avoid public scrutiny or deliberately mislead others.'<sup>25</sup>

On data protection specifically, the Global Principles note: 'data protection legislation can be misused or abused to prevent, end or restrict the legitimate public dissemination of accurate personal information in order to enable individuals to *control their reputation* at the expense of freedom of information, the right to truth and wider public interest' (emphasis added).<sup>26</sup>

ARTICLE 19 has noted the growing use of data protection rights and legislation to protect reputation at the expense of public access to information already in the public domain, for example while analysing the decision in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (2014) ('Costeja judgment'),. This use of requests for erasure of information that, although truthful, is 'no longer relevant, or excessive', brings into conflict the public right to know and to access information, and the right to erasure, which individuals may abuse to protect their reputation.<sup>27</sup>

## 2 The journalistic exemption

### What is the journalistic exemption?

As we have seen, every person including all members of the media has a responsibility to ensure they respect other people's right to privacy and data protection while exercising their right to free expression. In tandem, data protection, while protecting the rights of the data subject, should not unduly limit or interfere with the freedom of the media.

Data protection legislation in some countries therefore provides for an exemption from compliance with certain provisions where necessary in order to reconcile the right to protection of personal data with the right to free expression and access to information where data processing is carried out for a journalistic purpose. This is known as the journalistic exemption.

This concept precedes the enactment of the Kenyan data protection law of 2019. For example, in the EU the General Data Protection Regulation (GDPR) allows member states to create national legislation that allows for derogations or exemptions from certain provisions of the GDPR. This can occur where data processing is for journalistic, artistic, or literary purposes and is intended to reconcile the right to protection of personal data and the right to free expression and access to information.<sup>28</sup> Prior to the GDPR, the 1995 EU Directive on the protection of individuals with regard to the processing of personal data provided for this exemption.<sup>29</sup>

Part VII of Kenya's data protection legislation, the DPA 2019, allows for the exemption from compliance with certain provisions of the law where necessary for various reasons and special purposes, including the facilitation of journalism, literature, or art. Specifically, the DPA states:<sup>30</sup>

52. Journalism, literature, and art:

1. The principles shall not apply where:

- a) Processing is undertaken by a person for the publication of a literary or artistic material;
  - b) Data controller reasonably believes that publication would be in the public interest; and
  - c) The controller reasonably believes that in all circumstances, compliance with the provision is incompatible with the special purposes.
2. Subsection (1) (b) shall only apply where it can be demonstrated that the processing is in compliance with any self-regulatory or issued code of ethics in practice and relevant to the publication in question.
3. The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Journalism, Literature, and Art.

### Scope of the exemption

The journalistic exemption applies to personal data relating to an identified or identifiable natural person. Unlike the EU's GDPR,<sup>31</sup> Section 52 of Kenya's DPA 2019 provides only the criteria for applying the journalistic exemption but does not specifically list out the scope of the exemption

in Kenya. This leaves confusion and requires inference to be made regarding the exemption's exact scope. Table 1 compares how the applicable legislation in the EU, the UK (the law dates from before the UK left the EU and refers to the GDPR), and Kenya defines the scope of the exemption.

**Table 1. Scope of the journalistic exemption: EU, UK, and Kenya compared**

EU GDPR, Article 85	UK Data Protection Act 2018, Schedule 2, Part 5 ('Exemptions etc based on Article 85(2) for reasons of freedom of expression and access to information), Section 26(9) <sup>32</sup>	Kenya DPA 2019, Section 52
<p>Exemptions/derogations from the following chapters:</p> <ul style="list-style-type: none"> <li>• II. Principles of data protection law</li> <li>• III. Rights of the data subject</li> <li>• IV. Controller and processor</li> <li>• V. Transfer of personal data to third countries or international organisations</li> <li>• VI. Independent supervisory authorities</li> <li>• VII. Co-operation and consistency</li> <li>• IX. Specific data processing situations</li> </ul>	<p>'For the purposes of this paragraph, the listed GDPR provisions are the following provisions ... (which may be exempted or derogated from by virtue of Article 85(2) of the GDPR) –</p> <p><u>(a) in Chapter II of the GDPR (principles) –</u></p> <p>(i) Article 5(1)(a) to (e) (principles relating to processing);</p> <p>(ii) Article 6 (lawfulness);</p> <p>(iii) Article 7 (conditions for consent);</p> <p>(iv) Article 8(1) and (2) (child's consent);</p> <p>(v) Article 9 (processing of special categories of data);</p> <p>(vi) Article 10 (data relating to criminal convictions etc);</p> <p>(vii) Article 11(2) (processing not requiring identification);</p> <p><u>(b) in Chapter III of the GDPR (rights of the data subject) –</u></p> <p>(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided);</p> <p>(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);</p> <p>(iii) Article 15(1) to (3) (confirmation of</p>	<p>Provides criteria only; lists no specific details of exemption scope.</p>

	<p>processing, access to data and safeguards for third country transfers);</p> <p>(iv) Article 16 (right to rectification);</p> <p>(v) Article 17(1) and (2) (right to erasure);</p> <p>(vi) Article 18(1)(a), (b) and (d) (restriction of processing);</p> <p>(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);</p> <p>(viii) Article 20(1) and (2) (right to data portability);</p> <p>(ix) Article 21(1) (objections to processing);</p> <p><u>(c) in Chapter IV of the GDPR (controller and processor) –</u></p> <p>(i) Article 34(1) and (4) (communication of personal data breach to the data subject);</p> <p>(ii) Article 36 (requirement for controller to consult Commissioner prior to high risk processing);</p> <p><u>(d) in Chapter V of the GDPR (transfers of data to third countries etc), Article 44 (general principles for transfers);</u></p> <p><u>(e) in Chapter VII of the GDPR (co-operation and consistency) –</u></p> <p>(i) Articles 60 to 62 (co-operation);</p> <p>(ii) Articles 63 to 67 (consistency).'</p>	
--	---	--

As the table shows, the EU GDPR states the provisions which may be exempt, while the UK Data Protection Act provides further information on the exact derogations possible under UK national law. Both laws thus provide for the scope of their exemptions.

In Kenya, however, the act provides the criteria for applying the journalistic exemption (see further below), but no specific sections are listed that may be exempted or derogated from. As a



result, journalists and editors must infer where they can apply the exemption, provided they believe it necessary and are in compliance with the criteria for journalistic exemption.

Section 30 of Kenya's DPA 2019 states that a data controller or processor may process information, even without the consent of the data subject, where the processing is necessary for journalism, literature, or artistic purposes. Section 39(d) also specifies that a data controller or data processor is not subject to limitations on the retention of personal data if the retention is for journalistic purposes.

It is important for the Kenyan Data Protection Commissioner to provide more clarity on the scope of the journalistic exemption, and on the exact provisions for which derogations are possible under the journalistic exemption, to ensure certainty, transparency, and consistency (see Conclusions and recommendations). This could be done through the code of practice provided for in Section 52(3).

### Criteria for applying the exemption

Section 30 of the DPA sets out that a data controller or processor may lawfully process personal data for the purpose of journalism.

Section 52(1) of the DPA sets out the criteria or test to meet in order to apply the journalistic exemption. This test includes that:

- The processing is done with the aim of publication of the journalistic material;
- The data controller reasonably believes publication is in the public interest; and
- The data controller also reasonably believes compliance with the data protection principles of the DPA is incompatible with journalism.

Additionally, Section 52(2) specifies that *'Subsection (1)(b) shall only apply where it can be demonstrated that the processing is in compliance with any self-regulatory or issued code of ethics in practice and relevant to the publication in question.'*

Below we discuss the interpretation of these criteria. Illustrative examples from other countries are included to show how comparable criteria have been interpreted in other jurisdictions and therefore how such provisions could be interpreted in Kenya:

### Processing for the purpose of journalism

To apply this exemption, one must process data for the purpose of journalism. While in other jurisdictions journalism is mentioned specifically as a special purpose,<sup>33</sup> under the DPA 2019 'literary or artistic material' can be interpreted widely to include journalism. Journalism as defined under Kenyan law includes the collecting, writing, editing, and presenting of news or news articles in newspapers, magazines, radio, television broadcasts, the internet, or any other medium.<sup>34</sup>

The emphasis here is on the purpose of processing for journalism. A broad interpretation of ‘the purpose of journalism’ should be adopted, especially where the publication aims to inform the public or contribute to public debate (see Conclusions and recommendations).

This should be interpreted to mean the writing of newsworthy material or material in the public interest and does not necessarily mean who publishes the news, because this exemption applies broadly beyond journalists to media practitioners and other non-media persons including civil society organisations.<sup>35</sup>

For example, in *Steinmetz and others v. Global Witness*, the UK Information Commissioner’s Office (ICO) found that Global Witness, a civil society organisation, could rely on the journalistic exemption under the UK Data Protection Act in order to process data concerning Steinmetz and others and investigate and publish a story on corruption at the company BSG Resources. In particular, the ICO stated: ‘non-media organizations may be able to invoke the exemption if their purpose in processing the specific information is to publish information, opinions or ideas for general public consumption. It is our view that this constitutes a journalistic purpose even if they are not professional journalists and publication is part of a wider campaign.’<sup>36</sup>

### **Processing with the aim of publication**

The exemption applies where processing, which includes the collection, use, or storage of data about a person, is undertaken with the intention of making the resulting journalistic material accessible to the public.

In the UK’s *Steinmetz* case, the ICO held that not all personal data collected needs to be published, and the exemption would still apply even where that data is collected and analysed to write a story, even though the personal data is not in the end included in the story.

### **Reasonable belief that publication is in the public interest**

Section 52 of the DPA requires the data controller to consider relevant factors including an individual’s right to privacy and data protection, the public right to access information, and the right to press freedom. The test is subjective, and the controller is called upon to exercise their own judgment, which should in all circumstances be reasonable.

In the UK, the ICO has stated that a controller may be required to demonstrate their decisions were reasonable and performed to achieve a public interest that is set out in law <sup>37</sup> Although this obligation is placed on the data controller, it may be delegated to data processors as the controller sees fit.

While Kenyan law does not define public interest, the country’s Data Protection Act (General) Regulations 2021 state that public interest includes lessening or preventing a serious threat to life, public health, or public safety, locating a person reported missing, and taking appropriate action in relation to unlawful activity or serious misconduct.<sup>38</sup>

In *Biriuk v. Lithuania*, the European Court of Human Rights found that, although the press has a duty to inform the public on matters of public interest, this should not result in harm to an individual. In this case, the biggest daily newspaper in Lithuania had published sensitive personal data about the plaintiff, Biriuk, revealing her HIV status. The court found after examining the facts of the case that publication of the plaintiff's health status did not serve any public interest, was not likely to contribute to public debate, and was merely to boost the newspaper's sales.<sup>39</sup>

### **Compliance is incompatible with journalism**

The data controller is required to demonstrate a reasonable belief that compliance with some of the provisions of the DPA is incompatible with journalism. Such situations may include the disclosure of journalistic sources and third parties who provide information to the media such as whistleblowers, or investigative journalism practices requiring journalists to operate covertly. The Code of Conduct for the Practice of Journalism allows journalists to obtain information through subterfuge where no other means is possible.<sup>40</sup>

In the previously mentioned *Steinmetz* case, for example, Global Witness refused to comply with a data access request from Steinmetz, as doing so would have been incompatible with the exposé they intended to publish.

### **Compliance with codes of practice**

As mentioned above, Kenya's DPA also specifies that exemption from the principles of processing personal data on the basis that the data controller reasonably believes that the publication is in the public interest, only applies where the processing is demonstrably in compliance with any applicable self-regulatory codes or codes of ethics. Kenya has a framework of relevant standards and codes:

- **The Media Council Act** sets and regulates media standards in Kenya. Section 3 states that, when exercising the right of free expression through journalism, media enterprises, journalists, media practitioners, and consumers of media services should be guided by the following principles:<sup>41</sup>
  - a) Reflect the interest of all in society;
  - b) Be accurate and fair;
  - c) Be accountable and transparent;
  - d) Respect the personal dignity and privacy of others;
  - e) Demonstrate professionalism and recognition of the rights of others; and
  - f) Be guided by the 'National Values and Principles of Governance' as expressed by Article 10 of the country's Constitution.
- **The Code of Conduct for the Practice of Journalism** further expounds on these principles and applies to journalists, media practitioners, and media enterprises. The

code provides for fair and accurate reporting, with any false, misleading, or inaccurate reporting corrected immediately,<sup>42</sup> protection of confidential sources, especially where those sources may suffer harm,<sup>43</sup> and respect for individuals' privacy, which should not be interfered with except in the public interest.<sup>44</sup>

- **The Code of Conduct for Digital Media Practitioners** is a self-regulatory set of guidelines published by the Media Council of Kenya for digital media practitioners, including online publishers, influencers, bloggers, and vloggers.<sup>45</sup> The code makes explicit reference to the need to balance between free expression and privacy by encouraging content creators to ensure disclosure of personal information does not cause unnecessary harm to individuals or their families. Additionally, the guidelines allow for the disclosure of certain information where this is in the public interest, such as data about a person's health, sexuality, religion, or tribe.
- **Editorial guidelines.** Journalists in our survey (see Section 2 below) also mentioned relying on editorial guidelines provided by media houses to balance between privacy, data protection, and free expression, especially when determining when material is in the public interest.<sup>46</sup> The Nation Media Group's editorial policy and guidelines highlight elements to guide practitioners on this balance.<sup>47</sup> These include protecting the confidentiality of sources, the use of subterfuge only in cases of public interest, and recording interviews and conversations with the knowledge of the subject unless in very limited circumstances. Other media houses likely have similar editorial policies, although few such guidelines are in the public domain.

## **Section 2: The media and data protection obligations**

### 3. Survey: data protection awareness and practice in the media sector

ARTICLE 19 undertook a media sector data protection awareness survey in Kenya under the survey title 'Our Data, Our Voice' (Figure 1) between 9 and 13 January 2023. The purpose of the survey was to ascertain levels of awareness of data protection and current data protection practices among Kenyan media practitioners.

Questions covered topics including awareness of data protection legislation in Kenya, digital security practices and media organisations' in-house policies. The results show that further work is needed to increase levels of awareness of data protection obligations in Kenya, and training and other support is needed to strengthen data protection-related compliance in the media sector.



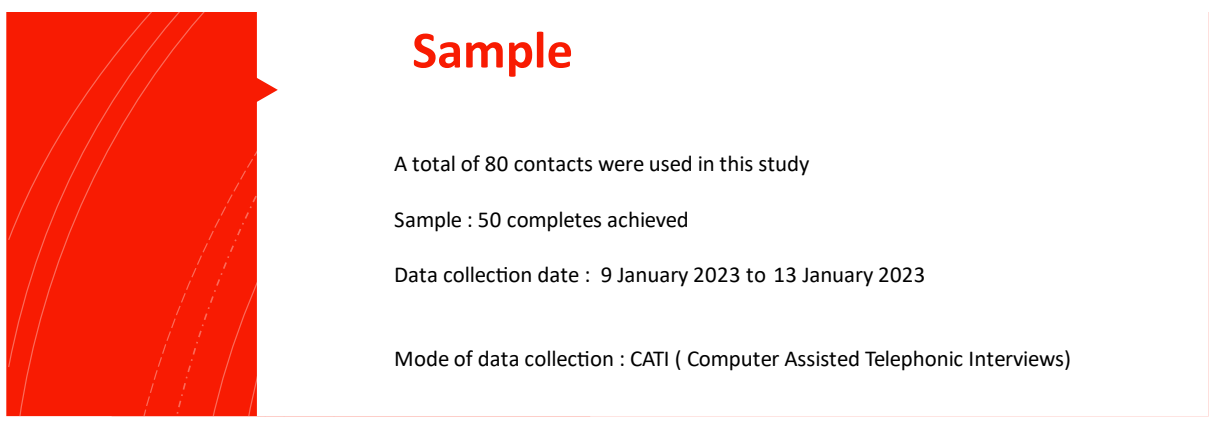
*Figure 1. 'Our Data, Our Voice' survey title page*

#### Methodology

ARTICLE 19's survey used a primary data collection approach. Undertaken among a sample of media practitioners the survey employed quantitative methodology to collect data through computer-assisted telephonic interviews (CATI) integrating phone calls with an online survey. CATI is a research methodology whereby an interviewer or moderator works through a computerised questionnaire script with each respondent during a phone call or online video call.

CATI software enables researchers to ask different types of questions in a set sequential order. This technique guarantees accuracy in questionnaire administration. The interviewer can give explanations when questions are unclear, to improve the response rate.

To select survey respondents, we used simple random sampling from a contact list of mobile telephone numbers. The sample frame contained different types of media practitioners in Kenya such as journalists, online creatives, bloggers photographers. Some of the respondents were drawn from marginalised communities to ensure the study was inclusive. We achieved a total sample of 50 completed surveys out of the 80 contacts we approached (Figure 2).



*Figure 2. Survey sample and other details*

## The respondents

We undertook the survey among 50 media practitioners from more than ten media organisations countrywide, mostly those based in Nairobi, Kakamega, and Mombasa (Figures 3 and 4).



*Figure 3. Media organisations with practitioners included in the survey*

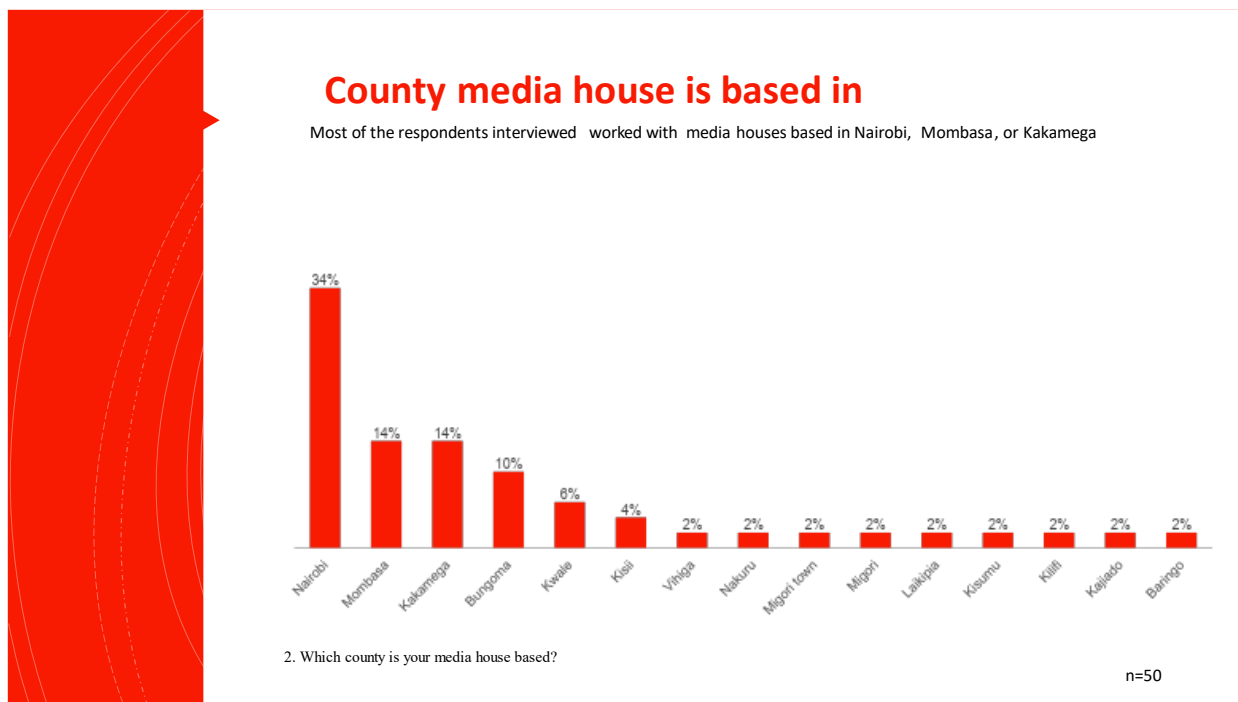


Figure 4. Geographical location in Kenya of media organisations in survey

Interviewees included diverse media practitioners in Kenya (Figure 5).

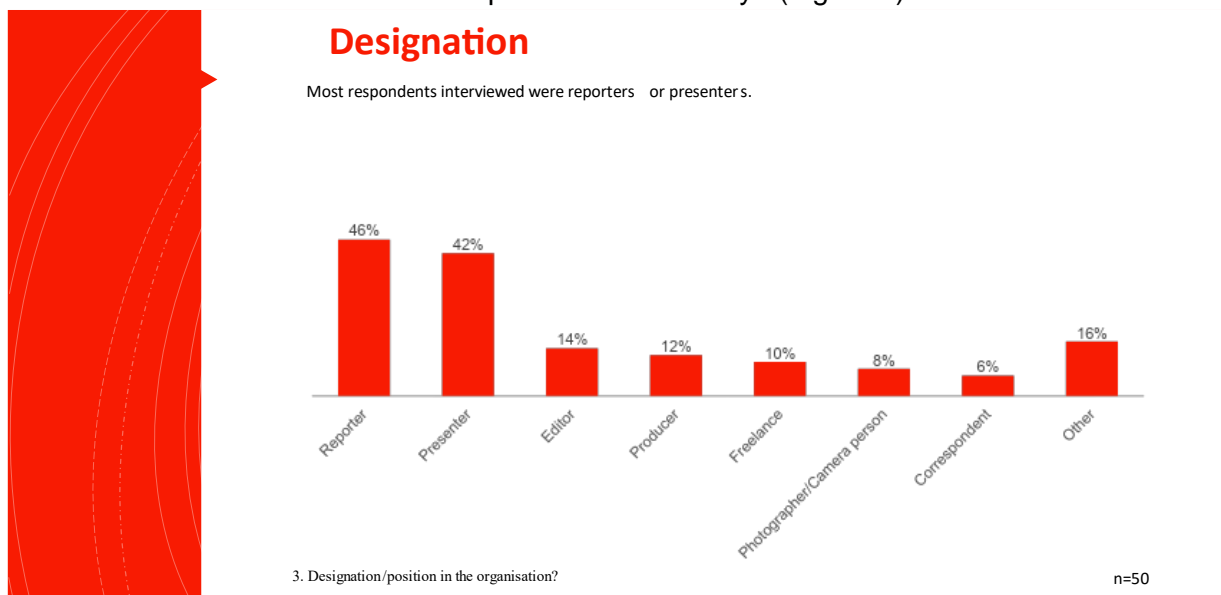


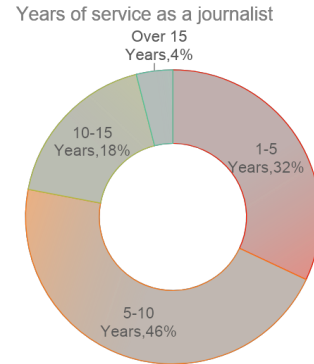
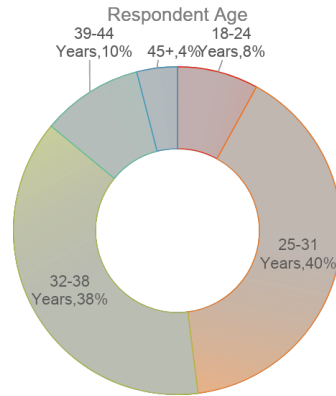
Figure 5. Interviewee designations (media roles)

To be representative, the respondents were aged between 25 and 38, and most had worked in the media for between one and ten years (Figure 6).



## Respondent age and years of service

About 78% of those who took part in the study were between the age of 25 and 38 years old. Only 22% of the respondents to the survey had served for over 10 years.



4. What is your age range?  
5. For how long have you worked as a journalist?

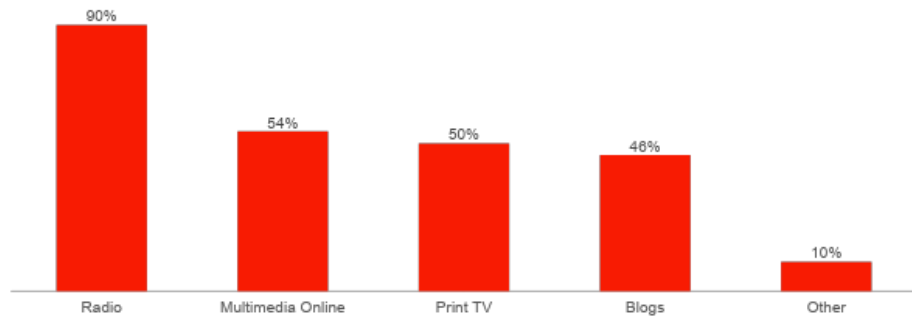
n=50

Figure 6. Age of respondents and number of years as a media practitioner

The media practitioners interviewed worked in diverse media, including radio, online multimedia, print and TV, and blogs (Figure 7).

## Type of media

Over 50% of the survey participants contribute to radio, multimedia online, or print or TV outlets. Most of the media practitioners work across different platforms.



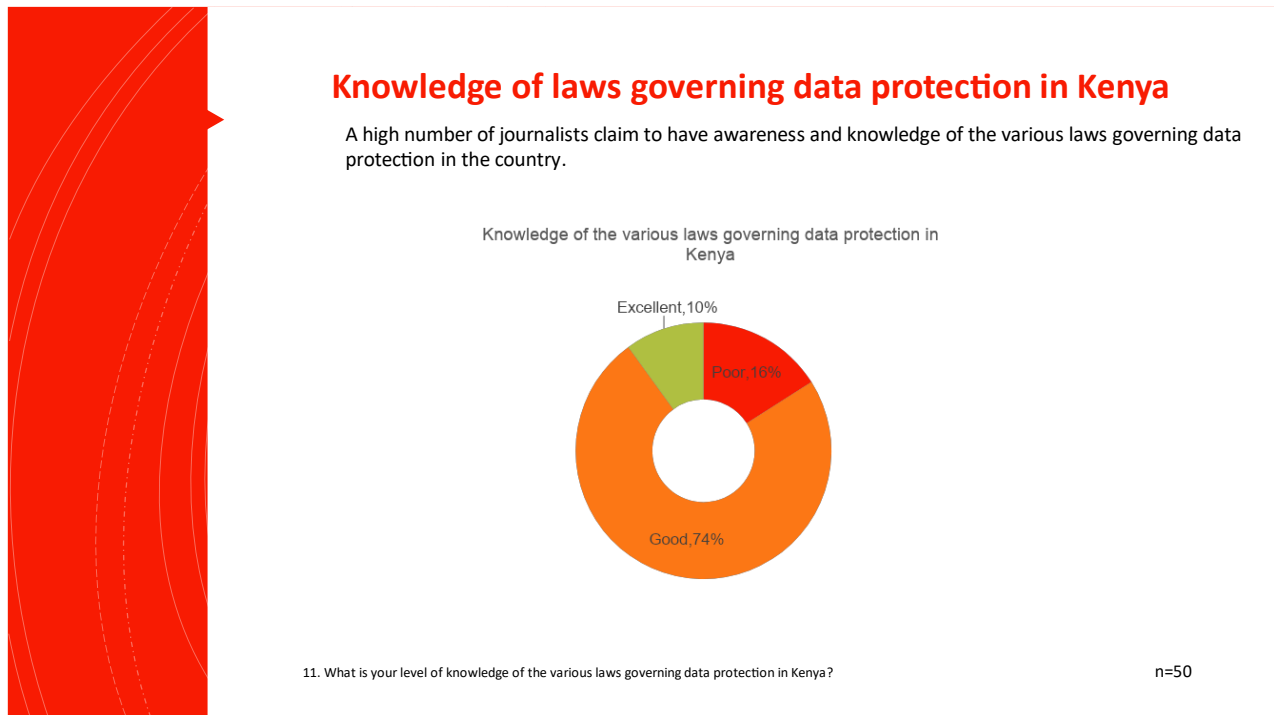
6. Which type of media platforms do you work with or contribute to (You can select more than one)

n=50

Figure 7. Respondents' work by media platform type

## Awareness about data protection

The survey aimed to find out the level of awareness of data protection among media practitioners. Of the 50 respondents surveyed, 10% claimed to have excellent knowledge of laws governing data protection in Kenya, 74% said they had good knowledge, and 16% admitted to having poor knowledge (Figure 8). Despite this claim, when we probed further, the findings showed that actual levels of knowledge were very different.



*Figure 8. Respondents' claimed knowledge of data protection laws in Kenya*

To probe further, respondents were then asked:

- If they were aware of the DPA 2019.
- If they were aware of the journalistic exemption under the DPA 2019.
- If they were aware of the Office of the Data Protection Commissioner (ODPC) in Kenya.
- If the answer to (c) above was yes, if they were aware of the roles of the Data Protection Commissioner.
- If the answer to (d) was yes, what specific roles of the ODPC they were familiar with?

Figure 9 shows the results of questions (a) to (d).

## Data Protection Act 2019

There is still low awareness of the complete Data Protection Act 2019, its clauses, the existence of the Office of Data Protection Commissioner and its roles.

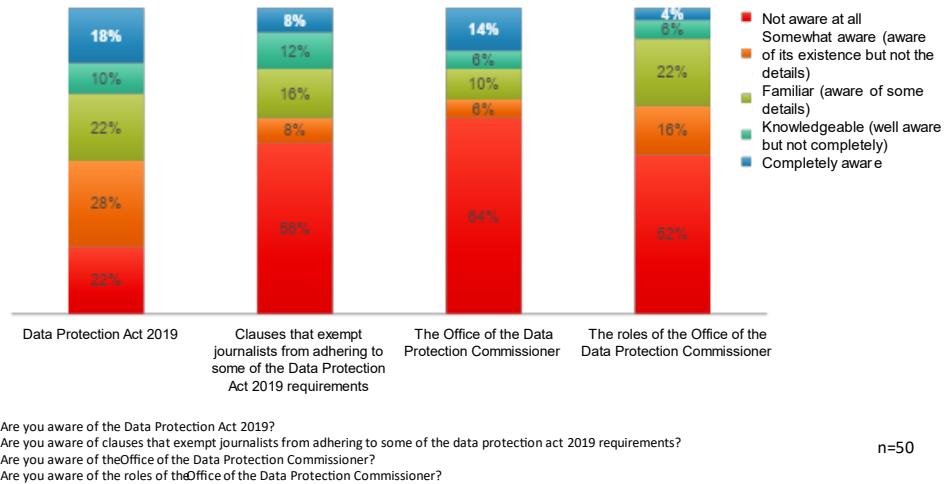


Figure 9. Respondents' knowledge of the DPA 2019 and ODPC

Question (e) was answered by 32% of respondents (16 people), who said they were at least familiar with the roles of the ODPC. Most of these respondents knew the ODPC is responsible for investigating complaints of infringement of the right to data protection (Figure 10).

## Awareness: Roles of the Office of the Data Protection Commissioner

The Office of the Data Protection Commissioner receives and investigates complaints of infringement of rights under the Act. It also exercises oversight on data processing operations.

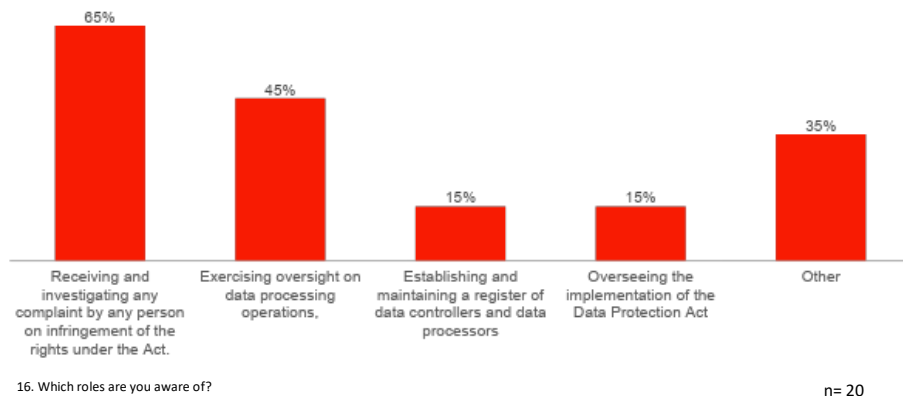


Figure 10. Respondents' awareness of the roles of the ODPC

Although 74% of respondents claimed to have excellent or good knowledge of laws governing data protection in Kenya (Figure 8), as Figures 9 and 10 show, awareness is actually still low. For example:

- At least 22% of the respondents were not aware of the existence of the DPA 2019 and 28% aware of its existence but not of the contents.
- At least 56% of respondents were not aware of the journalistic exemption under the DPA.
- 64% of respondents were not familiar with the ODPC , and a further 68% were not aware of the roles of the ODPC.

We combine these findings in Figure 11. The image on the right in Figure 11 shows the average level of actual awareness (on a scale of 1 being not aware at all to 5 being completely aware) among the respondents who claimed excellent, good and poor knowledge of the laws governing data protection in Kenya.

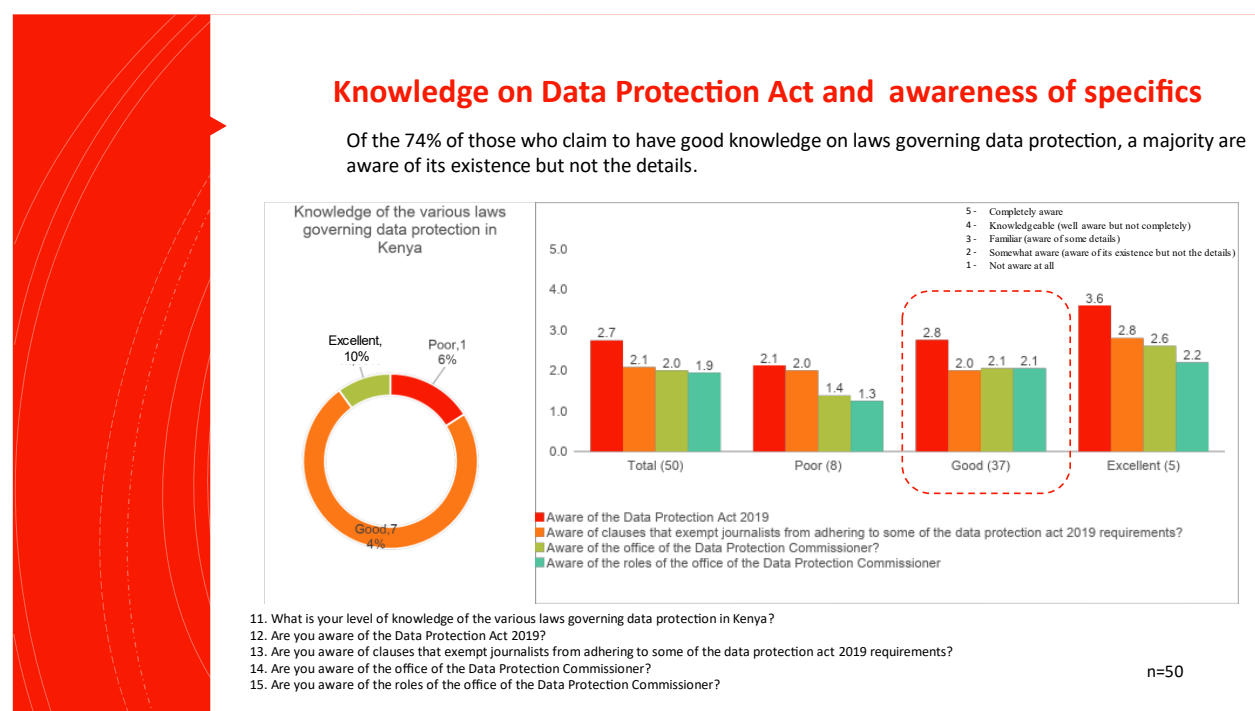


Figure 11. Respondents' awareness of the specifics of data protection in Kenya

## Digital security practices

The survey also sought to understand digital security practices among Kenyan media practitioners. This is because media practitioners are not exempt from obligations to maintain data security while processing data for the purposes of journalism. Poor personal digital security habits could lead to an infringement of the data protection and privacy rights of others.

The survey results found that a majority of respondents had been exposed to digital security threats, and 63% had faced online intimidation. The survey showed that 6% of respondents had had their emails hacked; 3% had had their phones tapped; and 3% stated they had been victims of cybercrime. Although the precise nature of the intimidation was unclear from the survey, this may have affected some respondents' ability to conduct journalism. (Figure 12).

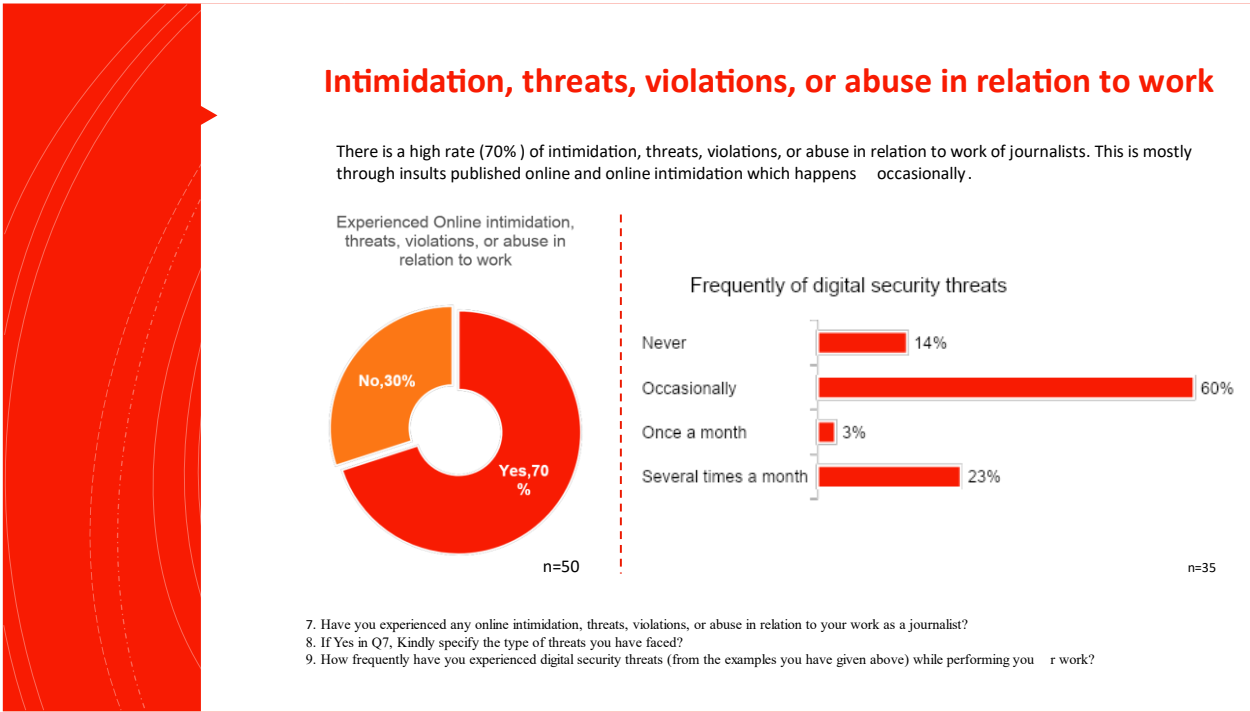


Figure 12. Respondents' experience of online intimidation, threats, violations, and abuse

In addition to digital security threats, we also sought to find out if any daily habits of respondents could put them or those covered by their work at risk. More than 70% of respondents believed privacy is more important than convenience and worried a lot about levels of privacy protection while online. More than 76% said they protect the contents of their emails and browsing habits from advertisers and third parties (Figure 13).

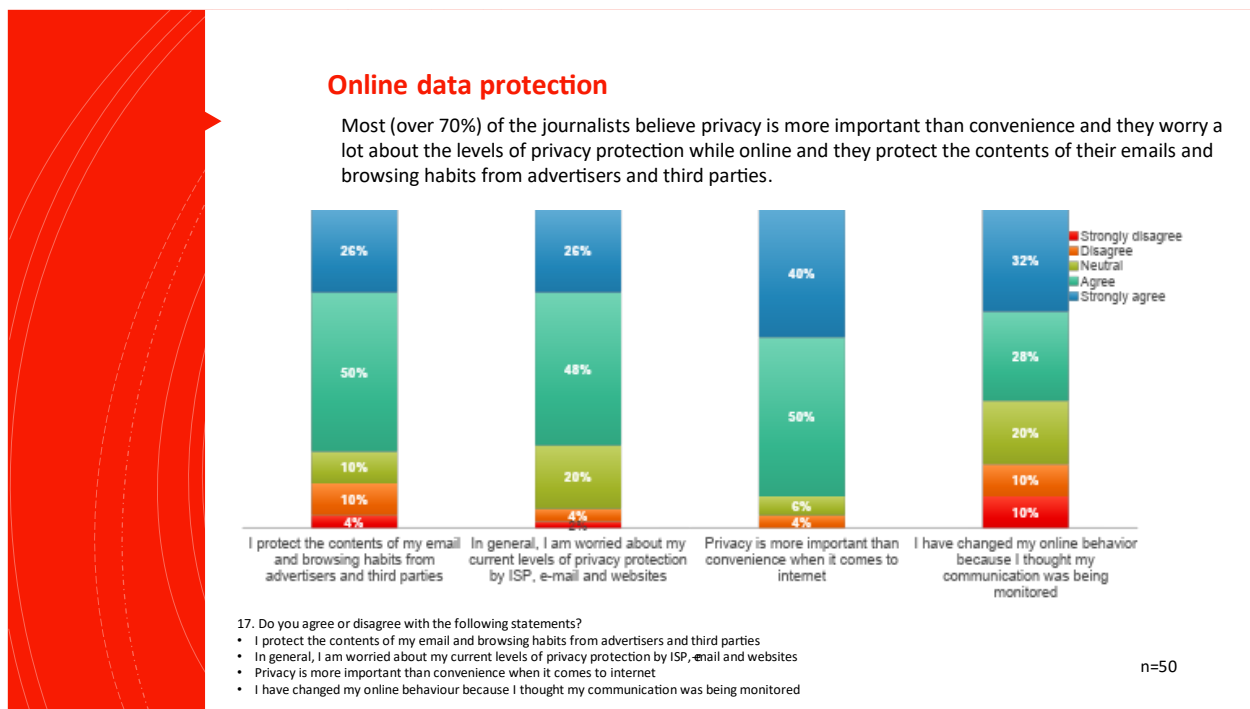


Figure 13. Respondents and online data protection: views and practices

Secure devices are important when processing data. However, the survey showed that some respondents worked online in various ways that may compromise data security. At least 12% of respondents said they used devices in cybercafés; 10% connected their devices to public wi-fi; and some used devices borrowed from friends (Figure 14).

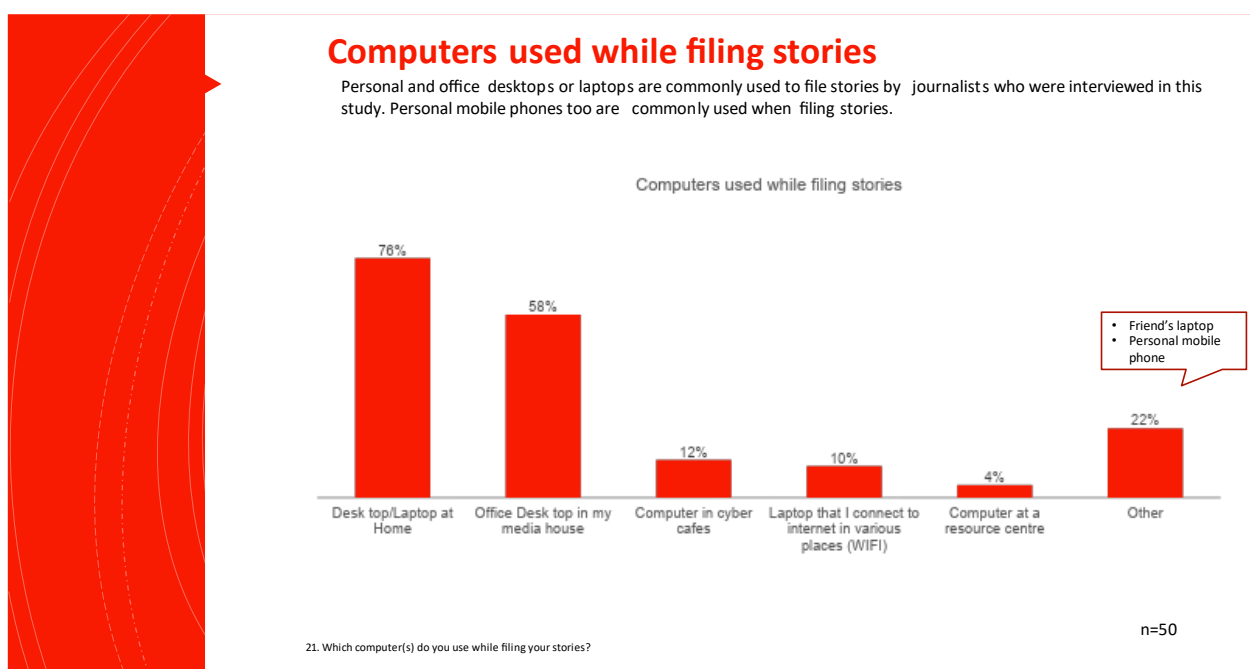
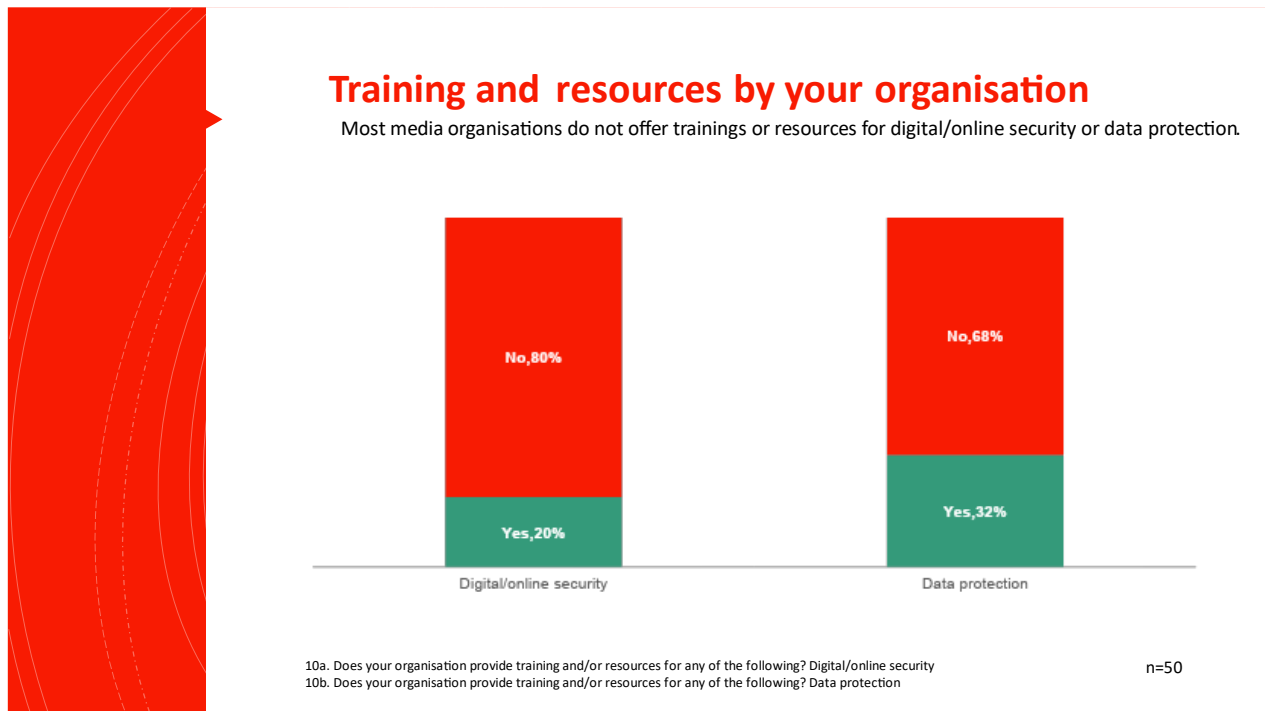


Figure 14. Online devices and locations used by respondents to file stories

## Training and resources

Survey questions also sought to learn about the resources available to help media practitioners understand their data protection responsibilities and what more would be required to improve current practices.

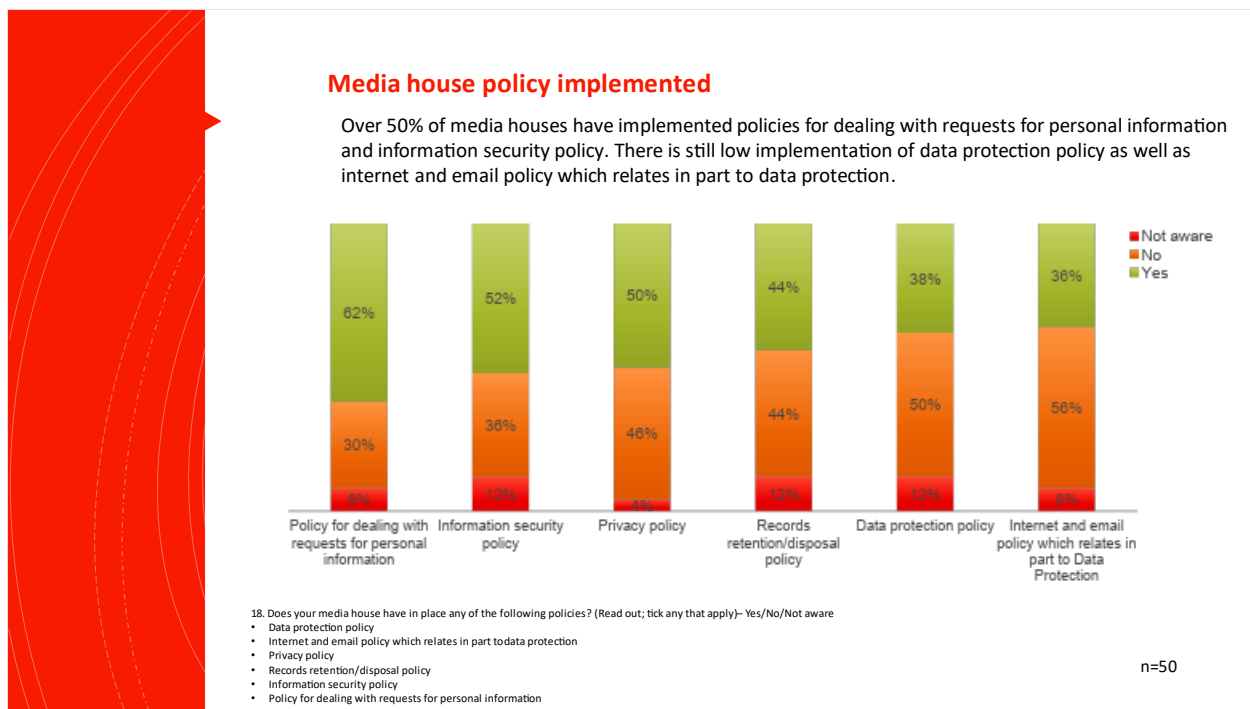
At least 68% of respondents said their media organisation did not provide training or resources on data protection or digital security (Figure 15). However, after a further probe, the results showed that organisations did at least provide and implement certain policies.



*Figure 15. Respondents' organisations' provision of relevant training and/or resources*

After a further probe, the findings included that:

- At least 62% of respondents stated that their media organisation had a policy for dealing with requests for personal information from data subjects.
- At least 12% stated that their media organisation did not have a data protection policy.
- 44% of respondents did not know if their media organisation had a record retention or disposal policy (Figure 16).



*Figure 16. Media organisations' implementation of policies relevant to data protection*

These findings indicate that some media organisations need to develop additional policies in relation to data protection and that media practitioners need to become more familiar with existing organisational policies that cover critical aspects of their data protection obligations.

Finally, 100% of respondents showed high interest in receiving more training on data protection and digital security. This is critical to ensure media practitioners understand their obligations (Figure 17).





*Figure 17. Respondents' interest in receiving training on data protection and digital security*

# Recommendations

Kenya's Office of the Data Protection Commissioner (ODPC) should:

1. adopt an approach that gives effect to both freedom of expression and the right to privacy and not unduly limit the right to free expression and access to information in the context of journalism.
2. Define the exact scope of the journalistic exemption, including the provisions of the Data Protection Act 2019 from which derogations are permissible under the exemption.
3. Clarify that Section 52 of the DPA 2019 includes journalism, with a wide definition and interpretation of what constitutes journalism.
4. Clarify that the journalistic exemption not only applies to journalists and media organisations but covers civil society organisations and campaigners as long as they publish, or intend to publish, journalistic material that is newsworthy and in the public interest.
5. Establish that organisations and campaigners can collect and process (analyse) data to produce a story even if in the end the data is not published, as the collection of personal data plays an important role in facilitating journalism
6. Require media organisations to publish and regularly review their policies relating to the protection of personal data and privacy, and to train new staff – and retrain existing staff – on their policies, particularly in areas of balancing between privacy and free expression.
7. Encourage digital media practitioners to comply with the self-regulatory Code of Conduct for Digital Media Practitioners.

Kenyan media organisations should:

1. Publish and regularly review of your policies relating to the protection of personal data and privacy.
2. Train new staff – and retrain existing staff – on the policies, particularly in areas of balancing between privacy and free expression.

And Kenyan digital media practitioners should:

3. Commit to comply with the self-regulatory Code of Conduct for Digital Media Practitioners.

# Notes

<sup>1</sup> Data Protection Act 2019, Section 2, <https://www.odpc.go.ke/dpa-act/>

<sup>2</sup> African Union, African Charter on Human and Peoples' Rights (1981), [https://au.int/sites/default/files/treaties/36390-treaty-0011\\_-\\_african\\_charter\\_on\\_human\\_and\\_peoples\\_rights\\_e.pdf](https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf)

<sup>3</sup> OSCE Representative on Freedom of the Media, 'Why Free Media Matters' (2012), <https://www.osce.org/files/f/documents/8/e/31230.pdf>

<sup>4</sup> African Commission on Human and Peoples' Rights (ACHPR), Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019), [https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression\\_ENG\\_2019.pdf](https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf)

<sup>5</sup> Charter of Fundamental Rights of the European Union (2012, C 326/02), Article 10(2), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>

<sup>6</sup> Human Rights Committee, General comment No. 34, CCPR/C/GC/34 (July 2011), Paragraph 13, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

<sup>7</sup> ACHPR, Declaration of Principles, Principle 19.

<sup>8</sup> ACHPR, Declaration of Principles, Principle 11.

<sup>9</sup> ARTICLE 19, *The Global Principles on Protection of Freedom of Expression and Privacy* (2017), <https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf>

<sup>10</sup> International Covenant on Civil and Political Rights, General Assembly Resolution 2200A (adopted 1966, entry into force 1976), Article 17, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

<sup>11</sup> Universal Declaration of Human Rights, General Assembly 217A (1948), Article 12, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

<sup>12</sup> Charter of Fundamental Rights of the European Union, Article 7.

<sup>13</sup> Charter of Fundamental Rights of the European Union, Article 8.

<sup>14</sup> African Union Convention on Cyber Security and Personal Data Protection (2014), [https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

<sup>15</sup> ACHPR, Declaration of Principles, Principle 42.

<sup>16</sup> ACHPR, Declaration of Principles, Principle 9.

<sup>17</sup> UN Special Rapporteur on the right to privacy, *Artificial intelligence and privacy, and children's privacy - Report of the Special Rapporteur on the right to privacy* (2021), <https://www.ohchr.org/en/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy>

<sup>18</sup> Constitution of Kenya (2010), Article 33, <https://www.klrc.go.ke/index.php/constitution-of-kenya>

<sup>19</sup> Constitution of Kenya, Article 34.

<sup>20</sup> Constitution of Kenya, Article 35.

<sup>21</sup> Constitution of Kenya, Article 31.

<sup>22</sup> Constitution of Kenya, Article 33(2).

- 
- <sup>23</sup> Constitution of Kenya, Article 33(3).
- <sup>24</sup> Constitution of Kenya, Article 24.
- <sup>25</sup> ARTICLE 19, *Global Principles on Protection of Freedom of Expression and Privacy*.
- <sup>26</sup> ARTICLE 19, *Global Principles on Protection of Freedom of Expression and Privacy*.
- <sup>27</sup> ARTICLE 19, 'ARTICLE 19's response to Google Advisory Council' (October 2014), <https://www.article19.org/data/files/medialibrary/37733/A19-comments-on-RTBF-FINAL.pdf>
- <sup>28</sup> EU, General Data Protection Regulation (2016), Article 85, <https://gdpr-info.eu/art-85-gdpr/>
- <sup>29</sup> EU, Directive 95/46/EC on the Protection of individuals with regard to the processing of personal data and the free movement of such data (1995), Article 9, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>
- <sup>30</sup> Data Protection Act 2019, Section 52, [http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019#part\\_VII](http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019#part_VII)
- <sup>31</sup> Article 85 of the GDPR states that, to apply the journalistic exemption, EU member states can provide for exemptions or derogations on chapters dealing with the principles of data protection, rights of the data subject, controllers and processors, transfer of personal data to third countries or international organisations, independent supervisory authorities, cooperation and consistency, and specific data processing situations where necessary to reconcile the right of protection of personal data with freedom of expression and access to information.
- <sup>32</sup> UK Government, Data Protection Act 2018, <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
- <sup>33</sup> For example, under [Article 85](#) the GDPR, journalism is listed in addition to academic, artistic, or literary purposes. In [Part V, Schedule 2, of the UK Data Protection Act](#), the purpose of journalism is listed in addition to academic, artistic, and literary purposes.
- <sup>34</sup> Media Council Act 2013, Section 2, <https://mediacouncil.or.ke/sites/default/files/downloads/media-act-2013.pdf>
- <sup>35</sup> Under the Media Council Act, Section 2, a journalist must be accredited by the Media Council.
- <sup>36</sup> Global Witness, 'Information Commissioner throws out Beny Steinmetz complaint against Global Witness' (21 December 2014), <https://www.globalwitness.org/en/archive/information-commissioner-throws-out-beny-steinmetz-complaint-against-global-witness/>
- <sup>37</sup> Information Commissioner's Office, 'Public Task', <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/public-task/>
- <sup>38</sup> Data Protection Act (General) Regulations (2021), Regulations 55, 56, <http://kenyalaw.org:8181/exist/kenyalex/sublegview.xql?subleg=No.%2024%20of%202019#doc-1>
- <sup>39</sup> European Court of Human Rights, Application No. 23373/03 (2008), <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-89827%22%5D%7D>
- <sup>40</sup> Code of Conduct for the Practice of Journalism, Section 9.
- <sup>41</sup> Media Council Act, Section 3.
- <sup>42</sup> Media Council Act, Second Schedule, Code of Conduct for the Practice of Journalism in Kenya, Section 2, 'Accuracy and Fairness', <https://mediacouncil.or.ke/sites/default/files/regulations/Code%20of%20Conduct%20%20for%20the%20Practice%20of%20Journalism%20-%20Media%20Council%20Act%202013.pdf>
- <sup>43</sup> Code of Conduct for the Practice of Journalism, Section 4(2)(a).

---

<sup>44</sup> Code of Conduct for the Practice of Journalism, Section 14.

<sup>45</sup> Media Council of Kenya, Code of Conduct for Digital Media Practitioners (n.d.), <https://mediacouncil.or.ke/sites/default/files/downloads/Code%20of%20Conduct%20for%20Media%20Practitioners.pdf>

<sup>46</sup> ARTICLE 19, Focus group discussion, 30 November 2022.

<sup>47</sup> The Nation Media Group, Editorial Policy and Guidelines & Objectives (no date), <https://www.nationmedia.com/wp-content/uploads/2018/02/Editorial-policy-online.pdf>