

ARTICLE 19

# Kenya: The Data Protection Bill, 2019

July 2019

## Executive Summary

---

The Data Protection Bill currently being considered by the National Assembly of Kenya needs significant revisions to ensure that its protections are in harmony with those of fundamental rights of freedom of expression and the right to information as recognized by the Constitution of Kenya and in international law.

The current draft has only limited provisions on the processing of personal data by the media which are not adequate to protect freedom of expression and no provisions on ensuring that the law is consistent with the Access to Information Act and the Constitution.

### **Recommendations:**

1. Article 52 of the Data Protection Bill should be revised to broaden the journalistic exemption to processing that is intended to communicating information to the public, ideas, or opinions of general interest including for journalistic purposes and the purposes of academic, artistic or literary expression.
2. The exemptions for freedom of expression, literature, and artistic purposes should be separated from other exemptions in Article 8. The Draft Law should ensure that provisions protecting freedom of expression apply to all sections of the law, not just relating to principles of processing personal data.
3. The journalistic exemption should also apply to the section on transborder data flows to ensure that materials created for the purpose of journalism, including radio and television and other media published on the internet or otherwise transferred across borders are not restricted.
4. The definition of personal information in Article 2 should be synchronized with the Access to Information Act and should specifically exempt information about the public activities and functions of public officials and those exercising public functions;
5. Public registers and other information not of a personal nature about activities of government including procurement, services and subsidies, should remain public.
6. The Data Protection Bill should specifically recognise the public interest provisions in the Access to Information Act held by public bodies and ensure that the public interest is considered in any request which relates to personal information.



<b>Executive Summary</b>	<b>2</b>
<b>About the Article 19 Transparency Programme</b>	<b>4</b>
<b>I. Introduction</b>	<b>5</b>
<b>II. Analysis of the Draft Law</b>	<b>5</b>
A. Freedom of Expression Problems.....	5
1. Media and Journalism.....	5
2. Transborder Data Flow.....	8
B. Conflicts with the Right of Access to Information.....	9
International law obligations.....	9
Definition of personal data.....	10
Public Records and Databases.....	11
IV. Conclusion	12

## About the Article 19 Transparency Programme

---

The ARTICLE 19 Transparency Programme advocates for the development of progressive standards on access to information at the international and regional levels, and their implementation in domestic legal systems. The Transparency Programme has produced a number of standard-setting publications, which outline international and comparative law and best practice in areas such as national security and privacy.

On the basis of these publications and ARTICLE 19's overall legal expertise, the Transparency Programme publishes a number of legal analyses, guides, and other materials each year, commenting on legislative proposals, as well as existing laws that affect the right to information, whistleblowing and related rights. This analytical work frequently leads to substantial improvements in proposed or existing domestic legislation. All of our materials are available online at <http://www.article19.org/>

If you would like to discuss this analysis further, please contact contact the Kenya Office at [kenya@article19.org](mailto:kenya@article19.org) or +254727 862230.

# I. Introduction

---

The rights of privacy and data protection and freedom of expression and information are co-equal human rights. ARTICLE 19 believes that privacy and freedom of expression and information are complimentary rights designed to empower the citizen to protect their rights and to improve the transparency of public and private bodies that hold and wield power in society. ARTICLE 19 supports the adoption of well-designed data protection acts, which protect individuals' rights to personal privacy while ensuring government transparency and freedom of expression.

The right of data protection has been growing rapidly in Africa over the last few years. To date, twenty four countries in Africa have adopted comprehensive laws protecting personal data while 14 countries are currently undertaking initiatives to adopt data protection legislation. In 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection, which sets standards on protecting personal data.

African countries are also increasingly participating in initiatives from outside the continent, most notably the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention is the world's only legally binding treaty on privacy and data protection. Mauritius, Senegal and Tunisia are party to Convention while Burkina Faso, Cabo Verde and Morocco are in undertaking the process for accession. Accession has considerable advantages for acceding countries and also provides strong assistance to countries wishing to obtain an EU adequacy finding under the General Data Protection Regulation (GDPR). In 2017, the European Commission stated "the Commission encourages accession by third countries to Council of Europe Convention 108 and its additional Protocol", because this will "contribute to the convergence towards a set of high data protection standards".

The rules on international transfers under the GDPR set high requirements for third countries to be deemed as offering sufficient protection of personal data, so that companies and public bodies in those countries will be able to receive such data from EU entities. The free flow of data between European and African countries will therefore be conditional upon development of good practices in the latter, oriented towards the offering of an "adequate level" of data protection that is a level equivalent to the one set by GDPR.

In this analysis, ARTICLE 19 sets out its concerns about the Data Protection Bill and its compatibility with Kenya's international obligations under international human rights law to protect freedom of expression and information. It also analyses various other aspects of the Data Protection Bill and proposes changes to make it stronger and more consistent with international standards.

## II. Analysis of the Draft Law

---

### A. Freedom of Expression Problems

#### 1. Media and Journalism

International law requires that freedom of expression concerns need to be harmonized with privacy protections. The key international data protection instruments include specific exemptions for journalistic, academic, artistic, literary and other cultural purposes which allows for the rules limiting processing to be waived for those purposes. These exemptions have been widely adopted in national data protection laws.

At a minimum, there must be exemptions from the application of, and/or limitations embedded in, data protection laws for the protection of journalistic, literary, academic, and artistic purposes and for the discharge of any legal obligation to make information publicly available, such as the maintenance of archives for historical or other public interest purposes, or under right to information laws. Moreover, such exemptions or limitations must be interpreted broadly so as to give meaningful effect to the rights to freedom of expression and to information.

The Data Protection Bill fails to take these concerns into account fully and raises additional problems around the publication of information.

#### *International law*

Most of the key international instruments on data protection have specifically included provisions requiring that freedom of expression and data protection be reconciled through exemptions for journalism, literary purposes and other reasons. Nearly all countries around the world that have adopted data protection acts have specifically included a clear exemption for journalistic, artistic, literary, and other cultural purposes which allows for the rules limiting processing to be waived for those purposes.

The African Union Convention on Cyber Security and Personal Data Protection also provides that processing for journalism and other FOE purposes should be exempt from limits on processing. Article 14 states:

Personal data processing for journalistic purposes or for the purpose of research or artistic or literary expression shall be acceptable where the processing is solely for literary and artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions.

In the updated Council of Europe Convention 108, Article 11 requires that signatories ensure that the rights are balanced in practice for freedom of expression:

No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5, paragraph 4, Article 7, paragraph 2, Article 8, paragraph 1, and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for... (b) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

The Explanatory Memorandum to the Convention clearly sets out the needs to protect journalism:

96. Littera b. concerns the rights and fundamental freedoms of private parties, such as those of the data subject himself or herself (for example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of journalistic, academic, artistic or literary expression, and the right to receive and impart information, confidentiality of correspondence and communications, or business or commercial secrecy and other legally protected

secrets. This should apply in particular to processing of personal data in the audio-visual field and in news archives and press libraries. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

Under the previous European Union Directive on Data Protection 95/46, Article 9 on “Processing of personal data and freedom of expression”, required that all EU Member States adopt exemptions to data protection rules in cases of all persons who are engaged in journalistic, literary or creative pursuits. The European Court of Justice in evaluating this provision ruled that states must develop a “fair balance” between the two rights based on the principle of proportionality.<sup>1</sup>

The breadth of protected freedom of expression-related activities has been extended in the revised data protection framework of the European Union. Under the new EU GDPR, Recital 153 states:

Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

#### *Data Protection Bill provisions*

The Data Protection Bill does not adequately reconcile the two fundamental rights. In the Bill, there are two applicable provisions, neither of which fully address the issue, and in fact, further restrict freedom of expression in violation of the Kenyan Constitution and international law.

Article 30 states the processing of personal data without consent is allowed in several circumstances. Among them, the processing for the purpose of historical, statistical, journalistic, literature and art or scientific purpose is included. Article 52 further holds that an exemption for journalistic, literary and artistic purposes applies whenever “the data controller reasonably believes that publication would be in the public interest”.

The provisions in Article 52 are overly narrow to fully protect freedom of expression. ARTICLE 19 believes that this exemption should be expanded to reflect a broader recognition of freedom of expression interests. The provision should encompass the processing done for any “journalistic purposes”, not just an ill-defined “public interest”.

Article 52 also only exempts journalistic purposes from the principles of processing personal data in Section IV of the bill. Consequently, all other sections apply when personal data are processed for journalistic purposes, including the requirements of registration of data processing, the processing of

---

<sup>1</sup> Case C-101/01, Bodil Lindqvist, 6 November 2003, p. 87-90.

sensitive data, the limits on the transfer of personal data outside Kenya and the application of criminal offences.

The failure to include the other substantive and administrative provisions in the exemption has serious consequences. The journalistic exemption would not apply when the processing involves sensitive personal data such as for example financial information, which relates to corruption and abuse of power, or health information particularly when this data is related to the grave illness of a leader.

Further, by not being exempted from the registration requirements, journalists and media will have the obligation to inform the Data Commissioner about, among other things, the personal data being processed, for which purpose and the category of data subjects. Such obligation poses serious risks of informing targets when journalists are conducting investigations.

Lastly, the application of criminal offences when data are processed for journalistic purpose can have a serious chilling effect on freedom of expression, as the disclosure of personal data in an article published in good faith and later found not to be in the public interest might bring the journalist and the media under proceedings. Penalties under the Data Protection Bill include a fine not exceeding three million shillings and/or imprisonment for up to two years. The imposition of all of these other obligations would seriously undermine the right of freedom of expression as protected under the Constitution and international law.

Other regional data protection laws have much more clearly and effectively ensured that freedom of expression is protected. In comparison, the South African Protection of Personal Information Act, states:

This Act does not apply to the processing of personal information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.<sup>2</sup>

### **Recommendations**

- Article 52 of the Data Protection Bill should be revised to broaden the journalistic exemption to processing that is intended to communicating information to the public, ideas, or opinions of general interest including for journalistic purposes and the purposes of academic, artistic or literary expression.
- The exemptions for freedom of expression, literature, and art purposes should be separated from other exemptions in Article 8. The Draft Law should ensure that provisions protecting these activities apply to all sections of the law, not just relating to principles of processing personal data in Section IV

### *2. Transborder Data Flows*

The meaningful exercise of the right to freedom of expression requires that the right to privacy and personal data protection be strongly protected, including in legal agreements for data flows. In order to ensure a consistent level of protection of personal data, the Data Protection Bill also applies to personal data transferred outside Kenya.

In data transfer agreements, States should ensure that the applicable law is the one providing the highest protection for personal data. The level of data protection applicable to an individual's personal data must not be lowered because of the data being transferred.

---

<sup>2</sup> Act No. 4 of 2013, Protection of Personal Information Act, 2013, §7



Article 48 of the Data Protection Act provides that a data controller or processor may transfer personal data to another country only where the data controller or processor has given proof of respect to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data, the data subject has given consent or the transfer is necessary for any matter of public interest.

Again, because Article 52 only applies the exemption to a limited section of the Bill, journalists could be violating the provisions on transborder data flows when they publish any materials, including articles, audio, video, or images on the Internet or through other networks, and could be subject to civil and criminal penalties, even if the publication was legal in the country. The Data Protection Bill must apply the journalistic exemption to transborder data flows.

### **Recommendation**

- The journalistic exemption should also apply to the section on transborder data flows to ensure that materials created for the purpose of journalism, including radio and television and other media published on the internet or otherwise transferred across borders are not restricted.

### **B. Conflicts with the Right of Access to Information**

The right of access to information and data protection often play complementary roles. They both are focused on ensuing accountability of powerful institutions to individuals in information age. It is also a fundamental human right recognised under international law and under the African Charter on Human Rights.

In 2016, Kenya adopted the Access to Information Act. The law was intended to implement Article 35 of the Constitution guaranteeing the right to information.

Unfortunately, the Data Protection Bill threatens to seriously undermine this achievement and reduce the availability of information. In fact, it appears to be a step backwards and undermines the rights given to all persons under the Access to Information Act and protected by the Constitution.

#### *International law obligations*

International law clearly requires that the right of access to information is reconciled with the right of privacy. The Declaration of Principles on Freedom of Expression in Africa states that “Privacy laws shall not inhibit the dissemination of information of public interest.”

Public bodies, as well as private bodies carrying out public functions, delivering public services, managing public resources or utilising public funds are required to apply the principle of maximum disclosure when dealing with right to information requests or proactively publishing information about their activities. The scope of exceptions to the right to information, including the right to privacy and protection of personal data, must be limited and subject to strict “harm” and “public interest” tests.

Public bodies must also proactively disclose government data, including through the use of accessible formats and anonymised datasets (“open data”), subject to safeguards for the protection of the right to privacy, of the right to personal data protection, and of confidential sources.

The Council of Europe stated in a 1986 Resolution that the right to information and privacy are “not mutually distinct but form part of the overall information policy in society.”<sup>3</sup> The revised Council of Europe Convention 108, includes a specific reference to public access to information in its recitals:

Considering that this Convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to official documents;

<sup>3</sup> Council of Europe Recommendation 1037 On Data Protection and Freedom of Information (1986).

## The explanatory note to the revised convention states

Furthermore, the Convention confirms that the exercise of the right to data protection, which is not absolute, should notably not be used as a general means to prevent public access to official documents.

The EU GDPR further extends this recognition. Article 86 states:

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

### *Definition of personal data*

Article 2 of the Bill sets out a broad definition of personal data to apply to “any information relating to an identified or identifiable natural person”. However, the Access to Information Act provides in Article 3 a more detailed definition by including and therefore, mentioning

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical, psychological or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
- (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- (c) any identifying number, symbol or other particular assigned to the individual;
- (d) the fingerprints, blood type, address, telephone or other contact details of the individual;
- (e) a person's opinion or views over another person;
- (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) any information given in support or in relation to an award or grant proposed to be given to another person;
- (h) contact details of an individual.

Further, the Data Protection Bill includes some of the information mentioned in the Access to Information Act in the definition of “sensitive personal data”.

The two definitions should be synchronized to make sure that the same categories of data follow the same regime and guarantees as established under the Data Protection Bill in relation to sensitive personal data.

We further recommend that the Bill be amended to include an explicit exemption for personal information relating to public activities of public officials or others acting under public authority or spending public money. This exemption is currently found in the 2016 Access to information Act in Article 6 and should be expanded to reflect the constitution right of information and the public interest in obtaining information about the official activities of public officials.

This approach has been adopted in both data protection and right to information laws around the world. By way of example, in South Africa the Promotion of Access to Information Act requires that disclosure

of information must be declined if it “would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.” However, the information can be disclosed if it is:

about an individual who is or was an official of a public body and which relates to the position or functions of the individual, including, but not limited to—

- (i) the fact that the individual is or was an official of that public body;
- (ii) the title, work address, work phone number and other similar particulars of the individual;
- (iii) the classification, salary scale or remuneration and responsibilities of the position held or services performed by the individual; and
- (iv) the name of the individual on a record prepared by the individual in the course of employment.<sup>4</sup>

#### *Public Records and Databases*

Governments also hold a considerable information which contains personal data about private citizens. While it is an obvious point that some of this information is sensitive and should not be made public, such as that relating to health conditions, there is a considerable amount of information which should be public. These records can be quite crucial to ensuing accountability, including information about public procurement, public registers of company owners and boards, information on company officials meeting with public officials to influence their decisions, recipients of subsidies, and more.

It is important to ensure that public registers and other information relating to the operation of government or in the public interest also remain public, and are not unnecessarily restricted in the name of data protection.

These registers can be public under the Bill when they meet the principles under Article 4 but it should be revised to ensure that this point is clear.

For information that is not in public registers, is also necessary that the Data Protection Bill fully recognise the public interest test in Access to Information Act as a legal condition for release of personal information and ensure that there is a consideration of the public interest when there is a request to access records which contain personal information of any kind about private individuals.

The Access to Information Act allows for the withholding of information relating to privacy or personal data when it would harm the person’s interest. The exemptions are not considered absolute as “a public entity or private body may be required to disclose information where the public interest in disclosure outweighs the harm to protected interests as shall be determined by a Court.”

The exemption also includes a public interest test which allows for the release of personal information which would otherwise be exempt when relating:

- (a) promote accountability of public entities to the public;
- (b) ensure that the expenditure of public funds is subject to effective oversight;
- (c) promote informed debate on issues of public interest;
- (d) keep the public adequately informed about the existence of any danger to public health or safety or to the environment; and

---

<sup>4</sup> Promotion of Access to Information Act , §34.

(e) ensure that any statutory authority with regulatory responsibilities is adequately discharging its functions.

### ***Recommendations***

- The definition of personal information in Article 2 should be synchronized with the Access to Information Act and should specifically exempt information about the public activities and functions of public officials and those exercising public functions;
- Public registers and other information not of a personal nature about activities of government including procurement, services and subsidies, should be public.
- The Data Protection Bill should specifically recognise the public interest provisions in the Access to Information Act held by public bodies and ensure that the public interest is considered in any request.

## **IV. Conclusion**

---

The existing Data Protection Bill is in clear need of improvements to ensure that Kenya is compliant with its international obligations on data protection and privacy, as well as to ensure compliance with the GDPR and other laws to facilitate the transborder flow of personal information.

However, the Data Protection Bill is insufficient to provide those protections, and further endangering free expression and right of access to information under the Kenyan constitution.