

Approved for tabling

12.1
SNA
17/10/19


REPUBLIC OF KENYA



THE NATIONAL ASSEMBLY
TWELFTH PARLIAMENT - THIRD SESSION

THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION
AND INNOVATION

REPORT ON THE CONSIDERATION OF THE DATA PROTECTION BILL, 2019

 THE NATIONAL ASSEMBLY PAPERS LAID	
DATE:	17 OCT 2019
	DAY: THURSDAY
TABLED BY:	Hon. William Kisang Chair, C.I.&I Committee
CLERK OF THE TABLE:	Lemuna Mosef

DIRECTORATE OF COMMITTEE SERVICES

CLERK'S CHAMBERS

PARLIAMENT BUILDINGS

NAIROBI-KENYA

OCTOBER, 2019

Table of Contents

LIST OF ABBREVIATIONS AND ACRONYMS	3
LIST OF ANNEXURES	4
THE CHAIRPERSON'S FOREWORD	5
CHAPTER ONE	7
PREFACE	7
1.1 Committee Mandate	7
1.2 Committee Membership	8
1.3 Committee Secretariat	9
CHAPTER TWO.....	10
INTRODUCTION.....	10
2.1 Background Information	10
2.2 Overview of the Bill	10
PUBLIC PARTICIPATION.....	16
3.1 Introduction	16
3.2 Committee Meetings	16
3.3 Consideration of the Data Protection Bill, 2019	16
3.4 ADDITIONAL PROPOSALS	35
MOMBASA COUNTY	35
CHAPTER THREE.....	40
COMMITTEE RECOMMENDATIONS.....	40

LIST OF ABBREVIATIONS AND ACRONYMS

CAK	Communications Authority of Kenya
Cap.	Chapter
CAK	Commission on Administrative justice
CODE-IP	Content Development and Intellectual Property Trust
CS	Cabinet Secretary
ICT	Information and Communications Technology
ISP	Internet Service Provider
IT	International technology
KNCHR	Kenya National Commission on Human Rights
KEPSA	Kenya Private Sector Alliance
KMA	Kenya Medical Association
TESPOK	Technology Service Providers of Kenya
TSC	Teachers Service Commission
CIPIT	Center for Intellectual Property and Information Technology Law

LIST OF ANNEXURES

Annexure 1	Adoption List
Annexure 2	Minutes of the Committee
Annexure 3	National Assembly Advertisements in the Daily Nation and Standard Newspapers dated 11 th July, and 8 th August, 2019
Annexure 4	Commission on Administration of Justice (CAJ)
Annexure 5	Amnesty International Kenya
Annexure 6	Lawyers Hub
Annexure 7	Google Kenya
Annexure 8	Mozilla
Annexure 9	TESPOK
Annexure 10	Article 19
Annexure 11	KEPSA
Annexure 12	CODE-IP
Annexure 13	Taskforce that formulated the Bill
Annexure 14	Bowman's/Coulson and Haney LLP
Annexure 15	Kenya Medical Association
Annexure 16	Branch International Limited
Annexure 17	Digital Lenders Association of Kenya
Annexure 18	Teachers Service Commission
Annexure 19	Karanja Matindi
Annexure 20	Center for Intellectual Property and Information Technology Law

THE CHAIRPERSON'S FOREWORD

The report contains the Committee's proceedings on the consideration of the Data Protection Bill, 2019 which was read a first time on Thursday 4th July, 2019.

The Data protection Bill, 2019 a Bill for an Act of Parliament sponsored by Hon. Aden Duale,MP was referred to the Departmental Committee on Communication, Information and Innovation for consideration and thereafter the Committee is to report to the House pursuant to National Assembly Standing Order No.127(1).

The Committee placed an advertisement in the local dailies on 11th July, 2019 and wrote to key stakeholders inviting them to submit their views on the Bill on or before 16th July, 2019.

Upon receipt of the memoranda, the Committee held a total of fifteen meetings with the stakeholders and considered submissions received which submissions are incorporated in this report. A total of sixteen memoranda were received from members of the public and institutional stakeholders in the ICT sector.

The Committee held public County forum meetings with stakeholders from Kakamega, Mombasa, Kilifi, Kisumu, Kericho and Nakuru Counties. It further held meetings with the Commission on Administration of Justice, Google Kenya, Amnesty International Kenya, Article 19, Bowmans La/Coulson Harney LLP, Lawyers Hub, Tespok, CODE-IP, Kenya Private Sector Alliance (KEPSA) and the Ministry of Information, Communication and Technology to deliberate on their memoranda.

Thereafter, the Committee proceeded for a report writing retreat which provided the opportunity to consider the submissions of the public and stakeholders and to further draft, consider and approve its Report.

On behalf of the Departmental Committee on Communication, Information and Innovation and pursuant to the provisions of the Standing Order 199 (6), it is my pleasant privilege and honour to present to this House the Report of the Committee on its consideration of the Data Protection Bill, 2019.

The Committee is grateful to the Offices of the Speaker and the Clerk of the National Assembly for the logistical and technical support accorded to it during its sittings. Finally I wish to express my appreciation to the Honorable Members of the Committee who made useful contributions towards the preparation and production of this report.

Hon William Kisang, MP

EXECUTIVE SUMMARY

The Data Protection Bill, 2019 a Bill for an Act of Parliament sponsored by Hon. Aden Duale, was read a first time on 4th July, 2019 and subsequently referred to the Departmental Committee on Communications, Information and Innovation for consideration and thereafter report to the House pursuant to Standing Order No.127(1).

From the memorandum of objects and reasons the principal object of the Bill is to give effect to the right to privacy as provided for in *Article 31 and (d)* of the Constitution by setting out the requirements for the protection of personal data processed by both public and private entities. Further, the Bill outlines the key principles that shall govern the processing of personal data by both public and private entities, while setting out the rights of data subjects and the duties of data controllers and processors as they handle data.

The Bill further seeks to establish the Office of the Data Protection Commissioner, and sets out the mandate of the office which shall include inter-alia to make provisions for the regulation of the processing of personal data, and obligations of data controllers and processors, and for connected purposes.

The rights of data subjects under this Bill include the right to be informed of the use to which personal data is to be put, right to access their personal data in custody of a data controller or data processor, right to object to the processing of all or part of their personal data, right to correction of false or misleading data and the right to deletion of false or misleading data about them.

CHAPTER ONE

PREFACE

1.1 Committee Mandate

1. The Departmental Committee on Communications, Information and Innovation is established under Standing Order 216 whose mandate pursuant to the Standing Order 216 (5) is as follows;
 - a. Investigate, inquire into, and report on all matters relating to the mandate, management, activities, administration, operations and estimates of the assigned Ministries and departments;
 - b. Study the programme and policy objectives of Ministries and departments and the effectiveness of the implementation;
 - c. Study and review all legislation referred to it;
 - d. Study, assess and analyze the relative success of the Ministries and departments as measured by the results obtained as compared with their stated objectives;
 - e. Investigate and inquire into all matters relating to the assigned Ministries and departments as they may deem necessary, and as may be referred to them by the House;
 - f. To vet and report on all appointments where the Constitution or any law requires the National Assembly to approve, except those under Standing Order 204 (Committee on Appointments);
 - (fa) examine treaties, agreements and conventions;
 - g. make reports and recommendations to the House as often as possible, including recommendation of proposed legislation;
 - h. make reports and recommendations to the House as often as possible, including recommendation of proposed legislation;
 - i. consider reports of Commissions and Independent Offices submitted to the House pursuant to the provisions of Article 254 of the Constitution; and
 - j. Examine any questions raised by Members on a matter within its mandate.
2. In accordance with Second Schedule of the Standing Orders, the Committee is mandated to oversee Communication, Information, media and broadcasting (except for broadcast of parliamentary proceedings), Information Communications Technology (ICT) development and advancement of technology and modernization of production strategies.

1.2 Committee Membership

- 1 The Departmental Committee on Communication, Information and Innovation was constituted by the House in December 2017 and comprises of the following Members-

Chairperson

Hon. Kisang William Kipkemoi, M.P
MP for Marakwet West Constituency

Jubilee Party

Vice-Chairperson

Hon. George Macharia Kariuki
MP for Ndia Constituency

Jubilee Party

Hon. Liza, Chelule Chepkorir, MP
M.P for Nakuru County

Jubilee Party

Hon. Alfah O. Miruka, MP
M.P for Bomachoge Chache Constituency

Kenya National Congress

Hon. Annie Wanjiku Kibeh, MP
MP for Gatundu North Constituency

Jubilee Party

Hon. Joshua Kimilu, Kivinda, MP
MP for Kaiti Constituency

Wiper Democratic Party

Hon. Marwa Kitayama Maisori, MP
MP for Kuria East Constituency

Jubilee Party

Hon. Mwambu Mabongah, MP
MP for Bumula Constituency

Independent

Hon. Maritim Sylvanus, MP
MP for Ainamoi Constituency

Jubilee Party

Hon. Mwangaza Kawira, MP
MP for Meru County

Independent

Hon. Jonah Mburu, MP
MP for Lari Constituency

Jubilee Party

Hon. Gertrude Mbeyu Mwanyanje, MP
MP for Kilifi County

Orange Democratic Party

Hon. Wamuchomba, Gathoni, MP
MP for Kiambu County

Jubilee Party

Hon. (Eng.) Mark Nyamita Ogola, MP
MP for Uriri Constituency

Orange Democratic Party

Hon. John Kiarie Waweru, MP
MP for Dagoretti South

Jubilee Party

Hon. Erastus Nzioka Kivasu, M.P.
MP for Mbooni

New Democrats Party

Hon. Innocent Momanyi Obiri, MP
Bobasi Constituency

People's Democratic Party

Hon. Godfrey Osotsi Atieno, MP
Nominated

African National Congress

Hon. Anthony, Tom Oluoch, MP
MP for Mathare Constituency

Orange Democratic Party

1.3 Committee Secretariat

2 The Committee is facilitated by the following secretariat:-

Ms. Hellen Kina
Clerk Assistant II
Lead Clerk

Ms. Marlene Ayiro
Senior Legal Counsel

Ms. Ella Kendi
Clerk Assistant II

Mr. Gorod Abdirahaman
Fiscal Analyst II

Ms. Lorna Okatch
Research Officer III

CHAPTER TWO

INTRODUCTION

2.1 Background Information

- 3 The Data Protection Bill, 2019 sponsored by the Leader of the Majority Party, the Hon. Aden Duale, MP, was read a first time on 4th July, 2019 and subsequently referred to the Departmental Committee on Communication, Information and Innovation for consideration and report to the House.
- 4 The Bill seeks to give effect to *Article 31(c) and (d)* of the Constitution on the right to privacy. The Bill further seeks to establish the office of the Data Protection Commissioner to oversee the implementation of and be responsible for the enforcement of this law. The Bill also seeks to provide obligations of data controllers and processors as well as provide for the regulation of the processing of data by data processors and data controllers. The Bill also sets out the rights of data subjects which rights include the right to be informed of the use to which personal data is to be put, to access their personal data in custody of a data controller or data processor, to object to the processing of all or part of their personal data, to correction of false or misleading data and to deletion of false or misleading data about them.

2.2 Overview of the Bill

- 5 Part I of the Bill provides for preliminary provisions and sets out the objects and purposes of the Bill.
- a) This Bill is an Act of Parliament that seeks to give effect to *Article 31(c) and (d)* of the Constitution; to establish the Office of the Data Protection Commissioners; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors.
 - b) This part provides for the interpretation section which contains definition of terms that are to be used in the Bill. It introduces new terms such as;
“Anonymisation” which means removing personal identifiers from personal data so that the data subject is no longer identifiable. This being read together with “consent” which means any voluntary, specific and informed expression of will of a data subject to process personal data. This implies some control that a data subject may exercise with regard to data that pertains to them.
Data has been categorized into three; biometric data, health data and personal data.
Personal data breach has been defined in an effort to curb cyber security.
 - c) The object and purpose of this Bill have been highlighted as follows—
 - i. regulation of the processing of personal data;
 - ii. ensuring the lawful handling of personal data in accordance with the principles of lawful processing;
 - iii. establishing legal and institutional mechanisms to protect personal data;
 - iv. providing data subjects with rights and remedies in respect to the protection of their personal data.
- 6 Part II establishes the office of the Data Commissioner and provides for the appointment, qualifications, functions, powers, removal of the Data Commissioner.
- a) This part provides for the Establishment of the Office of the Data Protection Commissioner which is a body corporate with perpetual succession and a common seal capable of suing and being sued;

- b) It is a designated state office under *Article 260(q)* of the Constitution. (an office established and designated as a State office by national legislation);
- c) The office shall comprise of the Data Protection Commissioner as its head and accounting officer and other staff appointed by the Data Commissioner.
- d) Clause 6 of the Bill provides for the appointment of the Data Commissioner. The appointment of the Data Protection Commissioner is to be initiated by the Public Service Commission who after receiving applications from the applicants shall shortlist the qualified candidate in a transparent process and forward the names to the Cabinet Secretary who shall within 14 days of receipt of names of the nominated candidates appoint the Data Commissioner.
- e) The data commissioner may establish such directorates as may be necessary for the better carrying out of the function of the office.
- f) Clause 7 of the Bill provides for the qualifications of the Data commissioner which include inter-alia-
 - (i) holds a degree from a university recognized in Kenya in data science, law, information technology or any other related field
 - (ii) has knowledge and relevant experience of not less than ten years; and
 - (iii) meets the requirements of Chapter Six of the Constitution.
- g) The Data Commissioner shall be appointed for a single term of six years and shall not be eligible for re-appointment.
- h) Some of the functions to be carried out by the office include—
 1. Overseeing the implementation and enforcement of the Act;
 2. Establish and maintain a register of data controllers and processors;
 3. Conduct assessment of a public and private bodies or at the request of a private body to ascertain whether information is processed according to the provisions of the Act;
 4. Educate the general public on the provisions of this Act;
 5. Receive and investigate any complaints regarding infringements of the Act;
 6. Undertaking research to the further developments in data processing and ensuring that there are no adverse effects of any developments on the privacy of individuals.
- i) In performing his duties, the Data Commissioner shall have the following powers—
 1. To conduct investigations on its own initiative or by virtue of a complaint made;
 2. To obtain relevant consultancy or advice from persons within the public service outside it where it is appropriate;
 3. To facilitate alternative dispute resolution on disputes arising from the Act;
 4. To summon witnesses for the purposes of investigation;
 5. To impose fines for failure to comply with the Act.
- j) Clause 11 of the Bill provides for instances when the office of the Data Commissioner may become vacant. These include instances where the Data Commissioner dies, resigns from office is convicted and sentenced to imprisonment for a term exceeding six months, or is removed from officer on various grounds.

- k) Clause 12 of the Bill provides for the procedure for removal of a Data Commissioner from office. A complaint shall be submitted to the Public Service Commission who shall inform the Data Protection Commissioner of the complaint and investigate the matter.
 - l) Clause 13 of the Bill provides that the Data commissioner shall appoint such staff as may be necessary for the proper discharge of the functions of the office.
- 7 Part III provides for the registration of data controllers and data processors.
- a) Clause 18 of the Bill provides that no person shall act as a data controller or data processor unless registered with the Data Protection Commissioner.
 - b) It outlines the application procedure including necessary thresholds that will be prescribed by the Data Protection Commissioner that must be met by a person seeking to be registered.
 - c) A persona seeking to be registered as a data controller or data processor must provide the following information to the Data. Protection Commissioner-
 - (i) a description of the personal data to be processed by the data controller or data processor;
 - (ii) a description of the purpose for which the persona data is processed;
 - (iii) the category of data subjects to which the persona data relates;
 - (iv) contact details of the data controller or data processor;
 - (v) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data; and
 - (vi) any other details as may be prescribed by the Data Commissioner.
 - d) It provides for the issuance of a registration certificate upon successful application which shall be valid for three years (Clause 20).
 - e) The Data Protection Commissioner is to keep a register of all the registered data controllers and data processors (Clause 21).
 - f) The Data Protection Commissioner can cancel or vary the terms of the certificate upon showing sufficient cause (Clause 22).
 - g) Clause 24 of the Bill provides for the appointment of Data Protection Officer by the data controller or processor to advice the data controller and ensure that they complied with the provisions of the Act.
- 8 Part IV of the Bill provides for principles and obligations of personal data protection-
- a) Clause 25 of the Bill provides for eight principles for the processing of personal data that every data controller is bound by to ensure that the data is handled in a way that is lawful. Which principles include that the data controller or processor shall ensure that personal data is-
 - (i) processed in accordance with the right to privacy of the data subject;
 - (ii) processed lawfully, fairly and in a transparent manner in relation to any data subject;
 - (iii) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
 - (iv) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
 - (v) accurate and where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
 - (vi) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected;

- (vii) released to a third party only with the consent of the data subject; and
- (viii) not transferred outside Kenya, unless there is proof of adequate
- b) There are several rights that are conferred on a data subject under Clause 26 of the Bill which rights include the right to be informed of the use of their personal data, right to access of personal data and to have false data corrected and right to have misleading data deleted.
- c) Clause 27 of the Bill provides for exercise of rights of data subject in cases of minors, or data subjects with physical or mental disability with the assistance of guardians.
- d) Clause 28 of the Bill provides that the data processor is to collect data from a subject-
 - (i) directly from the subject; or
 - (ii) in indirectly where data is contained in a public record, the data subject has deliberately made the data public, the data subject has consented to the collection from another source where there is a guardian the guardian has given consent among others.
 - (iii) The data processor is obliged to collect, store or use personal data for a purpose that was explicitly defined.
- e) Clause 29 of the Bill provides for the duty to notify where a data controller or data processor shall before collecting personal data in so far is practicable inform the data subject.
- f) Clause 30 of the Bill is on lawful processing of personal data which envisages that-
 - (i) the data subject consents to the processing; or
 - (ii) the processing is necessary for- processing of a contract which the data subject is party to, compliance with any legal obligation, in order to protect the vital interest of the data subject, for the performance of a task carried out in the public interest, performance of a task carried out by a public authority and for the purpose of historical, statistical, journalistic, literature and art or scientific research.
- g) Clause 31 of the Bill provides for a data protection impact assessment in instances where the operation is likely to result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.
- h) Clause 32 of the Bill provides for conditions of consent. A data subject must consent to having their personal data processed and the burden of proof lies on the data processor to determine express consent of the data subject.
- i) Clause 33 of the Bill provides for processing of personal data relating to a child. The consent of the parent and/or guardian is required before processing data relating to a child.
- j) Clause 34 of the Bill provides for restrictions on processing of data by the data subject where the accuracy of the personal data is contested by the data subject, personal data is no longer required, processing is unlawful and the data subject opposes the erasure of personal data, the data subject has objected to the processing pending verification as to whether the legitimate interest of the data controller or processor overrides that of the data subject.

- k) Clause 36 of the Bill provides that the data subject can object to their processing of their personal data, however if the data controller shows compelling legitimate interest that overrides the data subjects interest, the overriding interest will stand.
 - l) Clause 37 of the Bill provides for processing for direct marketing and data controller or a data processor shall not provide, use, obtain, procure personal data of a data subject for the purposes of direct marketing without prior consent.
 - m) Clause 39 of the Bill provides Limitation to retention of personal data. A data controller or processor shall retain persona information only as long as may be necessary to satisfy the purpose for which it is processed.
 - n) Clause 40 of the Bill provides for the right of rectification and erasure. The data subject has a right to request for rectification without undue delay of personal data that is inaccurate, outdated, incomplete or misleading.
 - o) Clause 43 of the Bill provides that the data subject has the right to be notified by the data controller where their personal data is subject to breach- unauthorized access to their personal data.
- 9 Part V of the Bill outlines the grounds for processing of sensitive personal data including further categorization of sensitive personal data.
- a) The principles of data processing must apply when handling sensitive personal data (Clause 44).
 - b) Clause 45 of the Bill provides for permitted grounds for processing sensitive personal data is only processed where-
 - (a) the processing is carried out in the course of legitimate activities with appropriate safeguards;
 - (b) the processing relates to personal data which is manifestly made public by the data subject; or
 - (c) processing is necessary for-
 - (i) the establishment, exercise or defence of a legal claim;
 - (ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or
 - (iii) protecting the vital interest of the data subject or another person where the data subject is physically or legally incapable of giving consent.
 - c) Clause 46 of the Bill provides for personal data relating to health. Personal data regarding health is to be processed by healthcare professionals.
 - d) Clause 47 of the Bill provides that the Data Commissioner may prescribe further categories of personal data which may be classified as sensitive personal data.
- 10 Part VI provides for the conditions for the transfer of personal data outside Kenya.
- a) Clause 48 of the Bill provides for Conditions for transfer out of Kenya. Some of the conditions for transfer out of Kenya include; consent by the data subject, necessity and that the Data Commissioner has been given proof on appropriate safeguards regarding protection of the data.
 - b) Clause 49 of the Bill provides for Safeguards prior to transfer of personal data out of Kenya. The Data commissioner is empowered to suspend, prohibit or subject a transfer to certain conditions in protection of the rights of the data subject.

- c) Clause 50 of the Bill provides for processing through a data server or data center in Kenya. This clause empowers the Cabinet Secretary to prescribe processing of certain data in Kenya.
- 11 Part VII provides for the exemptions to processing of personal data.
- a) Clause 51 of the Bill provides for general exemptions for data controllers or data processors from complying with the provisions of this Act. Exemptions maybe given when processing of data which is for journalism, literature and Art, data for research, history and statistics.
 - b) Clause 52 of the Bill provides that the Data Commissioner is to develop a data sharing code which aims to promote good practice in sharing data.
 - c) Clause 54 of the Bill provides that the data commissioner is empowered to prescribe instances where compliance with the Act may be exempted.
- 12 Part VIII sets out enforcement provisions of how the Data Commissioner may exercise the powers granted to them under the act.
- a) Clause 56 of the Bill makes provisions for complaints to the Data Commissioner. The Data Commissioner may receive complaints on matters regarding non-compliance of this Act.
 - b) Clause 57 of the Bill provides for investigation of complaints. The Data Commissioner may conduct investigation and summon witnesses and issue enforcement notices and penalty notices if necessary where there is failure to comply with the provisions of the Act.
 - c) Clause 58 of the Bill provides for enforcement notices that the Data Commissioner may serve on a person requiring that person to take such steps and within the period as may be specified in notice.
 - d) Clause 64 of the Bill provides for the Right of Appeal. The right to appeal to the High Court is bestowed upon a person aggrieved by the decision of the Data Commissioner.
 - e) Clause 65 of the Bill provides for the right to Compensation to a subject data. The data subject may be compensated where they suffer damage as a result of non-compliance with the Act.
- 13 Part IX provides for financial provisions, reporting mechanism, and management of funds by the office of the Data Commissioner.
- a) Clause 67 of the Bill provides for the source of funds for the office are provided to include allocations from the National Assembly, grants and donations and funds accruing to the office in the discharge of their functions.
 - b) Clause 68 of the Bill provides for annual estimates. The Office shall prepare estimates of their expenditure to submit to the National Assembly before the commencement of every financial year.
 - c) That the Office is subject to having its annual accounts audited.
- 14 Part X contains the provisions on delegated powers. This part empowers the Cabinet Secretary to make regulations that give effect to the implementation of this Act.
- 15 Part XI contains miscellaneous provisions and provides for offences including the unlawful disclosure of personal data, general penalties, the development of codes and guidelines and the consequential amendments.
- 16 The first schedule details the oath of office for the Data Commissioner upon appointment in office.
- 17 The second schedule provides for the consequential amendments of various laws that would need to be aligned to the data protection regime.

CHAPTER THREE

PUBLIC PARTICIPATION

3.1 Introduction

- 18 Pursuant to *Article 118(1) (b)* of the Constitution and Standing Order No. 127(3) which provides that the Parliament shall facilitate public participation, the Committee placed an advert in the local dailies on 11th July, 2019 and wrote to the key stakeholders inviting them to submit their views to the Clerk of the National Assembly on or before 16th July, 2019.
- 19 By the deadline for submission, the Committee had received seventeen (17) memoranda from; Commission on administration of Justice (CAJ), Amnesty International Kenya, Lawyers Hub, Google Kenya, Mozilla, TESPOK, Article 19, KEPSA, CODE-IP, Taskforce that formulated the Bill, Bowman's/Coulson and Haney LLP, Kenya Medical Association, Branch International Limited, Digital Lenders Association of Kenya, Teachers Service Commission Mr. Karanja Matindi and CIPIT. The memoranda are numbered as Annexures four (4) to nineteen (20).

3.2 Committee Meetings

- 20 Upon receipt of the memoranda, the Committee held a total of fifteen sittings, three of which were held to hear oral submissions from Google Kenya, Amnesty International Kenya, Tespok, Code -IP-, CAJ, Lawyers Hub, Article 19, Bowmans law/ Coulson Harney LLP Kenya Private Sector Alliance etc. The Committee also had meeting with the Senate committee on ICT over the Senate Bill on Personal Data Protection Bill, 2018 as well as a meeting with Hon Omar Mohamed Maalim, MP who had formulated a legislative proposal on Data Protection and Privacy Bill, 2019.

3.3 Consideration of the Data Protection Bill, 2019

- 21 In considering the Data Protection Bill, 2019, the Committee took into account the memoranda and oral submissions received from the public and its deliberations. The following constitutes the views of the Committee on the issues arising with regard to each Clause of the Bill—

Clause 2 Interpretation

- 22 Six memoranda received by the Committee contained submissions relating to this Clause. KEPSA proposed an amendment to the definition of the term "sensitive personal data" as the definition provided for in the Bill was ambiguous. The Committee disagreed with this view, noting that the provisions under the Act and as proposed by the Bill was similar to what KEPSA was proposing its memorandum.
- 23 Digital Lenders Association proposed that the term "Sensitive Personal Data" be defined to include religious or political belief or affiliation to belief. The Committee disagreed with this view as religious and political beliefs should not be categorized as sensitive data.
- 24 Mozilla proposed to expand the definition of sensitive personal data to include official or national IDs, passwords, financial data, location information.
- 25 Article 19 recommended that the definition of "personal data" to be synchronized with the one provided for in the Access to Information Act thus exempting information about public activities and functions of public officials and those exercising public functions.
- 26 Content Development and Intellectual Property (CODE-IP) Trust proposed that the definition of several other terms be include as follows-

“data collector” means a natural or legal person, public authority agency or other body which alone or jointly with others, collects public data.

“data owner” means the same as “data subject”

“metadata” means data about data, and for the purposes of this Act, qualifies as data wherever consolidated metadata reveals private data or personally identifiable information.

- 27 CIPIT proposed revision of the definition of the term ‘ sensitive personal data’ to include membership of trade union, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.
The Committee proposed the definition of the terms “data” and “persons” and elaborately define the term “consent”

Clause 3- object and purpose of the Act

Two memoranda were received on this Clause.

- 28 CODE-IP Trust also recommended the inclusion of the purpose to establish a framework to protect against the unnecessary collection of information to relating to one’s family or private affairs.
- 29 CIPIT proposes incorporation of the internationally recognized data protection principles including; Fairness and Transparency, Storage limitation and Accountability.
The Committee did not agree with the proposals to amend the provisions of Clause 3 as the same were deemed to be in order.

Clause 4- Application

Four memoranda received by the Committee contained submissions relating to the clause.

- 30 Lawyers Hub recommended the expansion of application to include data controllers and processors who though not resident in Kenya, process data of data subjects resident in Kenya.
- 31 Bowmans law/ Coulson Harney LLP proposed that for purposes of clarity, the underlined words to be included; not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.
- 32 TESPOK proposed the exclusion of the processing of personal data outside Kenya from the scope of the Bill. Alternatively, they stated that there is need to limit application to the data of Kenyan residents in other jurisdictions, and that there was a need to limit the scope of data (eg. Data collected for the purpose of engaging in commercial activity).
- 33 CIPIT observed that clause 4(b) provided limited protection for the personal data of people in Kenya as the controller or processor established in Kenya can easily remove its processing from the scope of the Act by conducting the processing outside Kenya.
- 34 CODE-IP Trust proposed the expansion of the scope of privacy protection to include foreign entities collecting private data of Kenyans for inclusion in alien data systems. They suggested the revision of clause 4(b) to read as follows-
- “(b) by a data collector, data controller or data processor who-
- (i) is established or ordinarily resident in Kenya; or
 - (ii) not established or ordinarily resident Kenya but processing personal data of data subjects in Kenya

The Committee was of the opinion that inserting the term “located” was good for clarity purposes.

Clause 5 establishment of the office of the data commissioner

Four memoranda received by the Committee contained submissions relating to the clause.

- 35 Lawyers Hub in recognizing that the Commissioner shall exercise some quasi-judicial functions, opined that there is need to ensure independence and proper function of the Commission. They recommended the expansion of the composition to a board chaired by the Data Protection Commissioner.
- 36 The CAJ recommended that the clause should be amended so as to provide for the establishment of an independent oversight institution with full powers to oversight and implement the law, as well to receive and resolve complaints on implementation of data protection by both public and private bodies. Determinations made in exercise of the foregoing powers should also be subject to a right of appeal to the High court and not any other institution. The CAJ further opined that the data protection function should be undertaken by the proposed Office of the Data Commissioner so long as the independence of the office could be guaranteed given that it was intended to be an oversight institution which must ensure preservation of the rule of law and must not appear to be subservient to the executive. They stated that if that caveat could not be sufficiently guaranteed, however, Parliament should consider placing the function of the office within one of the existing Article 59 Commissions since their independence is heavily safeguarded under Chapter 15 of the Constitution.
- 37 KMA proposed inclusion of a data privacy Commission/Committee who will provide diversity and technical expertise on health data protection due to the nature and sensitivity of personal health data.
- 38 CIPIT recommended establishment of the Data Commissioner Office as a Constitutional Commission under Chapter 15 of the Constitution.
39. Mr. Karanja Matindi was of the view that the Data Protection Commissioner recruitment and removal process should be the same as for the constitutional commissions and independent office holders such as Director of Public Prosecution given the importance and mandate of the office.
40. As at the time of concluding its report, the Committee opined that the clauses as provided by the Bill were sufficient and that the provisions on the office of the data commissioner were adequate enough to accord the office the independence sought by the stakeholders in their proposals. The Committee however proposed that the clause be amended to provide for directorates of the office of the data Commissioner for ease of work.

Clause 6- Appointment of Data Commissioner

Four memoranda were received by the Committee which contained submissions relating to this clause.

41. The process of appointment connotes that the Data Protection Commissioner reports to the CS, which provision was said to be one that did not promote the independence of the Data Protection Commissioner. The stakeholders therefore recommended as follows-
42. Amnesty International Kenya proposed that the President gazettes the vacancy in the office of Commissioner and constitutes a selection panel for the purpose of appointment, that would be comprised of a chair person selected by the President and one representative from each of the following entities: Ministry for ICT, KNCHR, one data science professional of at least 15 years' experience, one IT professional of at least 15 years' experience, the Association of Professional Societies of East Africa and the Law Society of Kenya. The selection panel to hold proceedings in public and submit a report of the interview proceedings to the National Assembly, which should include the scores of each candidate interviewed together with

- criteria for selection. The selection panel should then forward 3 names to the President for nomination, the President then nominates one person for approval by the National Assembly.
43. Lawyers Hub proposed that appointment of the Data Commissioner to be done by the President and approved by the National Assembly and that a reconciliation of this clause and Clause 11 of the Bill should be done as clause 11 addressed the resignation process to the President and not the CS.
 44. Mozilla proposed that Parliament should set qualifications of the Data Commissioner and nominate the Data Protection Commissioner, and that the appointment should be made by the President.
 45. TESPOK proposed that the appointing body should be the same as the one of resignation as is addressed to clause 11 of the Bill.
 46. Further Committee agreed with the stakeholders that the Data Protection Commissioner should be appointed by the President and not the CS as has been proposed in the Bill.

Clause 7- Qualifications of the Data Commissioner

The Committee received two memoranda on this clause.

47. Digital Lenders Association proposed that the Data Commissioner should be appointed for a term of three years which shall be subjected to renewal for a further final. The Committee disagreed with the stakeholder as the provisions of Clause 7 that provided for a non-renewable six years' term were in order.
48. TESPOK submitted that it would be important for the Data Commissioner to demonstrate an understanding of Information Technology systems and data handling processes both manual and automated and have knowledge of sector specific data handling practices. This will ensure the streamlining of data handling legislation for various sectors.
The Teachers Service Commission (TSC) proposed inclusion of Information Science/ Record Management as one of the significant key requirements.
49. The Committee noted that the Data Protection Commissioner was going to be required to handle very novel and technical docket and it therefore proposed that the holder of that office should have at least a minimum of a master's degree so that he can be fully equipped to execute his mandate.

Clause 8- Function of the Office

Three memoranda received by the Committee contained submissions relating to the clause.

50. Lawyers Hub opined that the obligation of the Data Protection Commissioner to promote self-regulation was unnecessary, as a statutory body established to regulate cannot then be charged with the duty to promote self-regulation.
51. They also held the opinion that data processors should not be allowed to form self-regulating organizations whose mandate and jurisdiction would be, for instance, to conduct investigations and administer fines for breach. This would lead to double jeopardy.
52. Mozilla recommended that additional powers and functions be assigned to the Data Protection Commissioner including issuing of regulatory guidance, codes or practice to data controllers and processors, investigatory, adjudicatory, levying penalties and punitive measures as well as providing redress and compensation to users when their rights have been violated. The Data Protection Commissioner to be empowered to promote public awareness and engage in capacity development activities. The Committee did not agree with the proposal as the same was already provided for under clause 74 of the Bill.

53. TSC recommended that there was need to clarify linkages and relationship between the Office of the proposed Data Commissioner and public entities with constitutional or statutory mandate to generate public data e.g. teacher registration and Registrar of Persons.

Clause 9- Powers of the Office

54. CIPIT recommended that the process of sanction should apply to complaints investigated by the independent data protection authority on its own initiative as it empowered to do so under sub- clause 1 (a) The Committee agreed with the provisions of Clause 9.

Clause 10- Delegation by the Data Commissioner

55. The Committee agreed with the provisions of Clause 10. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 11- Vacancy in the Office of the Data Commissioner

52. The Committee agreed with the provisions of Clause 11. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 12- Removal of the Data Commissioner

53. Amnesty International Kenya was of the view that security of the office was key to the independence of the office of the Commissioner. The office of the Commissioner is established as a state office under *Article 260* and therefore requires that the removal process reflects the removal process of a state officer. They thus proposed the removal from office to be done in accordance with *Article 251* of the Constitution. Process of removal should commence with a petition to the National Assembly, which if satisfied will send the petition to the President for the formation of a tribunal to investigate the conduct of the Commissioner and recommend action to the President.

54. The Committee did not agree with the proposal from the stakeholder as the office of the Data Commissioner would enjoy independence pursuant to the provisions of the Bill.

Clause 13- Staff of the Office

55. The Committee noted that the Data Protection Commissioner had no singular capacity to appoint the staff of the data protection office and therefore the Committee proposed that such appointment should be done in consultation with the Public Service Commission a constitutionally mandated office to handle matters of human resources in the public service.

Clause 14- Remuneration of the Data Commissioner and Staff

56. The Committee agreed with the provisions of Clause 14. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 15- Oath of office

57. The Committee agreed with the provisions of Clause 15. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause. However, the Committee noted that there was a typographical error that needed to be corrected in the Bill

Clause 16 - Confidentiality agreement.

58. The Committee agreed with the provisions of Clause 16. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 17- Protection from personal liability

59. The Committee agreed with the provisions of Clause 17. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 18-Registration of data controllers and data processors

Ten memoranda were received with the provisions of Clause 18. The stakeholders were opposed to and recommended the removal of the requirement for mandatory registration for all data controllers and processors, or alternatively, a threshold for registration be established.

60. Google Kenya and CODE-IP Trust proposed that Clauses 18-24 be struck out entirely on the grounds that data controlling and data processing are not business models in the strict sense, they are incidental to the normal course of business. Therefore, requiring registration will create an immense implementation burden.
61. Google and Mozilla opined that the requirement for registration places an undue burden on SMEs and startups. They also stated that the requirement for fees would disproportionately affect SMEs.
62. Bowmans law/ Coulson Harney LLP proposed that registration should not be mandatory on all data controllers and processors and that a threshold to the registration requirement should be introduced to the Bill. This can be linked to turnover, employees' numbers or according to the number of data subjects processed.
63. Lawyers Hub recommended the removal of mandatory registration and only require registration from those who meet the threshold to be espoused by the commissioner.
64. Digital Lenders Association of Kenya suggested the removal of the registration requirement since it will cause an implementation challenge.
65. KEPSA provided that the Bill required mandatory registration of data controllers and processors and registration of Data Commissioners and requires the Data Commissioner to set a threshold to exempt small companies. KEPSA proposed that the Clause should be changes to be as follows: " No person shall act as a Data officer or Data controller except those expressly exempted from the Act unless one is registered and accredited by the data Commissioner"
66. It further recommended that in prescribing the threshold for mandatory registration the Data Commissioner should exempt the data controllers in the following circumstances from registration. Data controllers who process personal data by non-automatic means as a part of a filing system, lawyers, independent accountants and financial advisors. Natural or legal persons having less than fifty employees per annum, the processing of personal data is required for criminal investigations or for prevention of a criminal offense, if persona data being processed is already publicized by the data subject, if processing of personal data is required to protect the economic and financial interest of the state in relation to budget, tax and financial matters.
67. TESPOK recommended that the requirement for registration be set within a set threshold for controllers/processors dealing with sensitive/personal data an further proposes additional clause that will list sensitive/personal data as information relating to sex, gender, pregnancy, race, marital status, ethnic or social origin, colour, age physical/psychological/ mental health, disability, religion, belief, culture, language, birth and death, identification and biometric details, personal contact details and child criminal records.

68. T.S.C were of the view that criteria for primary registration should be provided while the secondary criteria should be left for the Regulations

69. The Committee maintained that the requirement of registration should be compulsory for purposes of accountability and therefore the clause to stay as is.

Clause 19-Application for registration

70. CIPIT proposed the following amendments for clarification and to strengthen the right to information and the right to access as provided for in Clause 26

- a) sub-clause 2(a) to clearly state what personal data will be processed
- b) sub-clause 2(b) to specify the purpose for which the personal data is collected
- c) sub-clause 5 the period to be prescribed

71. The Committee agreed with the provisions of Clause 19 and proposed an amendment to sub-clause 4 of the Bill to give clarity to the provision that was ambiguous.

Clause 20- Duration of the registration certificate

72. The Committee agreed with the provisions of Clause 20. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 21- Register of data controllers and data processors

73. The Committee agreed with the provisions of Clause 21. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 22- Cancellation or variation of the certificate

74. The Committee agreed with the provisions of Clause 22 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause. However, the committee proposed an amendment to recast its wording.

Clause 23- compliance and audit

Three memoranda were received on the clause.

75. CIPIT proposed that the clause should provide clarity on the criteria the Data Commissioner to use to decide on carrying out of the audit and who would be undertaking the audit The Committee agreed with the provisions of Clause 23. Clause 24

76. Digital Lenders Association of Kenya proposed the amendment of clause 24 to provide for registration and accreditation of data officers.

77. T.S.C recommended inclusion of qualifications to be considered for appointment as a data protection officer

Clause 24-Designation of the Data Protection Officer.

78. CIPIT observed that the term 'may' in sub-clause 24(1) makes it unclear when the obligation to designate a data protection officer applies and they proposed a tiered system through subsequent regulations to delineate firms that will be required to employ/contract a data protection officer.

The Committee held that the law as provided in the clause of the Bill was adequate.

Clause 25-Principles of data protection

The Committee received four memoranda on this Clause.

79. Digital lenders Association of Kenya proposed that clause 25 (c) be reviewed to provide as follows-

“every data controller and processors shall ensure that personal data is collected and processed for explicit, specific or for any incidental purpose that may be reasonably inferred having regard to the specific purposes and the context and circumstances in which the personal data is collected including transfer to third parties with prior notification and consent.

80. CODE-IP Trust proposed the addition of a new subsection after (d) to read as follows-

“(e) A valid explanation must be provided whenever information relating to family or private affairs is necessary to be collected”.

81. Lawyers Hub recommended the use of the word “and” instead of “or”, for better protection of data subjects. This essentially would require that all conditions are met prior to the processing of the data. The committee held that the reasonability test and incidental test does not allow for the consent of the data subject prior to the collection of data. Consent should be sought prior to transfer of the data to the third parties and mere notification will not suffice.

82. CIPIT proposed inclusion of the following principles

a) Integrity and confidentiality – it listed in Clause 41 and 42 but must appear in this clause for consistency

b) Accountability

CIPIT further recommended that sub-clause 25(g) be amended to ensure consent is not the sole legal basis of sharing personal data with a third party and sub-clause 25 (h) be amended to ensure that the transfer of data outside of Kenya is not processed unless there is adequate data protection safeguards and consent.

The committee agreed with the submissions by CODE-IP noting that there was need to ensure that the data subjects are duly informed of reasons for collection of data relating to private and family affairs for them to make informed decisions before granting the consent.

Clause 26- Rights of data subject

The Committee received two memoranda on this clause.

83. On subsection 26 (d) and (e) T.S.C submitted that there was need for clarification on the power granted by virtue of the provision. They argued that the right to alter or vary personal data ought to be stringently regulated. They further submitted that there exists Government directions that speak to the integrity and preservation of primary official data declared by a public employee/ citizen eg place of birth

84. CIPIT proposed inclusion of the following rights; the right to an effective remedy, right to compensation and liability, right to suppress or block which is provided for in clause 36, right to data portability provided for in clause 38 and the rights in relation to profiling and automated decision-making which is provided for in clause 35

The Committee agreed with the provisions of Clause 26.

Clause 27-Exercise of rights by data subject

85. The Committee agreed with the provisions of Clause 27. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 28-Collection of personal data

The Committee received four memoranda on this clause.

86. Lawyers Hub stated that the clause creates a wide discretion on data controllers and processors to interpret what amounts to prejudice. This creates opportunity for abuse and therefore should be deleted.
87. On subsection 2(c), Bowmans submitted that the narrow exceptions where personal data can be collected indirectly should be finite and limited. By allowing for the indirect collection of personal data where the data subject has consented to the collection from another source limits and conflicts with the data subject rights under the Bill and conflicts with the definition of 'consent'
88. CIPIT submitted that the sub-clauses 28 (a, b,c,e,and f(ii) require amendments in order to ensure that the right to information provided for under clause 26 (a) is upheld effectively. Further the clause should be strengthened to require the firms to conduct a Data Protection Impact Assessment to show that they understand the risks and effects of collecting maintaining and dissemination of personal data
89. Digital Lenders Association of Kenya proposed the inclusion of; "A data subject has a right to be notified of the use of their personal data. The Committee held that the clause should stay as is because is the element of consent was already set out in the Bill. The amendment implies that consent can be done away with as long as they are notified of their use of their data after the fact.

The Committee was of the view that the Clause as provided for in the Bill was adequate enough.

Clause 29- Duty to notify

90. CIPIT submitted the clause is open to abuse and that a specific period of time should be provided. Further, they proposed inclusion of the following information to be provided
 - a) a description of the personal data;
 - b) the legal basis for the processing;
 - c) the third parties whom the personal data has been or will be transferred, including details of safeguards adopted;
 - d) the envisaged time limits for deletion of the different categories of data;
 - e) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data.

The committee agreed with the stakeholder on the need to provide for a description of the technical and organizational security measure taken to ensure the integrity and confidentiality of the data.

Clause 30- Lawful processing of personal data

Two memoranda were received on the clause.

91. Bowmans law/Coulson Harney LLP were of the view that there should be strict limits on the avoidance of the application of the Bill for national security reasons by any person in public interest, national security or public order. The parties seeking protection under the exemptions should be subject to a higher standard of proof and should indicate beyond reasonable doubt why a data subjects rights should be protected.

92. CIPIT was the view that there was need for clarity as what are the legal grounds for processing personal data by defining the terms such as public interest and legitimate interests to strengthen the protection of such data.

Clause 31-Data protection impact assessment

The Committee received two memoranda on this clause.

93. Digital Lenders Association which proposed that clause 31(3) be amended to provide for Data Commissioners powers to provide for processes that are considered to be high risk thus requiring this assessment. They further proposed that Clause 31(2) on consultation to be deleted and finally that Clause 31(4) to be introduced to provide that Data Impact Assessment Reports shall be submitted within 60 days from the date of publication as per clause 31(3).
94. CIPIT recommended that assessment should be an obligation prior to any processing activities. In addition, the duty should be strengthened by specifying the means/forms in which this right should be implemented.

The Committee did agree with the proposals and the importance of ensuring that timelines were provided on when data impact assessment reports would be made available.

Clause 32-Conditions of consent

The Committee received two memoranda on this clause.

95. Mozilla stated that explicit consent should be required for processing sensitive data and that the Data Protection Commissioner to issue guidelines on how requirements for consent should be interpreted.
96. Digital Lender Association proposed that the clause be amended to provide that as follows-
“Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time and the data controller or processor shall notify the data subject of the procedure of withdrawal of the consent prior to obtaining the consent to receiving personal data. Provided further that withdrawal shall not be arbitrary and shall be subject to the overriding legitimate grounds of the data controller or data processor as provided in clause 34(d).

The Committee held that a data subject should have the right to withdraw consent at any time and any processing of the data subjects data after withdrawal of the consent is not lawful. However, caution should be taken to ensure that the procedure given by the data controller for withdrawal was not so stringent that it prevents the data subject from easily withdrawing consent. The requirement for consent has been adequately provided for in the Bill in clauses 25, 26, 30, 32. Further that the definition of the word “consent” in the Bill captures the explicitness of consent.

Clause 33-Processing of personal data

The Committee received four memoranda on this clause.

97. Code-IP proposed the addition of a new sub-section after sub-section (c) to provide-
“all personal data relating to a child collected, processed and or achieved subject to subsection (b) must be deleted upon the child becoming an adult”.
- This in their view would prevent the overzealous law enforcement officers from labeling children as criminals for life as a result of a child’s youthful indiscretions.

98. Mozilla proposed the need for reconciliation of the provisions of this Bill with those of the Children Act. The Bill should specify that data controllers and processors should not knowingly market, track or profile children without the consent of their parent or guardian. Mozilla also opined that the Parental consent raises practical questions regarding its implementation, thus Data Commissioner be mandated to provide guidelines. They also proposed deletion of the provision mandating the Data Protection Commissioner to appoint data controllers and processors as guardians. The Committee in disagreeing with the stakeholder stated that the provision in the Bill was adequate.

99. CIPIT recommended the clause be reconciled with the protection provided for in the Children Act which upholds the right to privacy under Article 19

100. KEPSA recommended that clearer guidance that protect children's data should apply to children under the age of 13 avoiding any suggestion that additional privacy-invasive measures are needed for the purposes of age verification should be considered. In essence the requirement for age of consent for children should be reduced to 13 years. The committee did not agree with the proposals of the stakeholders and emphasized on the need to ensure that the data of children beyond age of majority are protected.

101. Mr. Karanja Matindi, submitted that the provision could breach the rights of the children since under the law of Kenya a child is anyone under 18 years. He emphasized that requirement for the Parental/guardian consent would be inappropriate for a child of between 13-17 years as they may want to access services that require them to give personal details.

The Committee resolved that the clause should be left as it was provided for in the Bill.

Clause 34-Restriction on processing

102. The Committee agreed with the provisions of Clause 34 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 35- Automated individual decision making

The Committee received three memoranda on this Clause.

103. Digital Lenders Association of Kenya proposed that the clauses be deleted accordingly and replaced with the following new clause- "the data controller should implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

104. Branch International Limited proposed that clause 35(3) and (4) of the Bill be amended to provide that the rights of a data subject do not apply to circumstances where the data subject had given prior consent to decisions being made solely based on automated data processing.

105. CIPIT were of the view that the section should be strengthened by including the following obligations and key considerations;

- a) data controllers and processors who profile must be transparent about it and individuals must be informed about its existence for the onset and not as soon as practicable as per sub subsection 3(a);
- b) for profiling, the data controllers and processors should also notify the data subjects about the risks and their rights;

- c) impose restrictions and safeguards on the ways in which data can be used to profile and make decisions.

The committee was of the opinion that the provision should remain as was crafted in the Bill. The initial consent should not be binding onto the data subject and there should be various opportunities given to the data subject to review the consent given. The Committee however, proposed an amendment to correct typographical error.

Clause 36-Objecting to processing

Two memoranda were received on the clause.

106. Digital Lenders Association of Kenya proposed the inclusion of a provision that a data subject has a right to object to the processing of their personal data under clause 30(iv) and 37, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim.

107. CIPIT were of the view that the clarity must be provided on what the 'compelling grounds' are.

The Committee opined that a data subject must always have the right to object to the processing of their personal data. Subjecting it to the included in the clauses may eliminate any entitlement to consent that the data subject has.

Clause 37-Processing for direct marketing

108. The Committee agreed with the provisions of Clause 37 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause, however it proposed that the clause be amended to provide for the processing of broad commercial data as opposed to narrowing down to just direct marketing.

Clause 38-Right to data portability

109. The Committee agreed with the provisions of Clause 38 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 39-Limitation to retention of personal data

The Committee received two memoranda on this Clause.

110. TSC recommended that management/ retention/ destruction of personal data ought to be harmonized with existing regulatory frameworks.

111. CIPIT proposed that clarity must be provided for in terms on the applicability of this law to other laws which imposed the data retention policies such as the KICA which regulates the retention of electronic records and the Registration of subscribers Telecommunication Services Regulations, 2015. Further they submitted that pseudonymised data is still personal data and therefore subject to the protections of the law.

The Committee opined that the provision as provided for in the Bill was sufficient to cater for the concerns raised by the stakeholder.

Clause 40-Right of rectification

The Committee received three memoranda on this clause.

112. Google Kenya proposed that a clarification be made to the effect that erasure rights are to be associated with where processing is occurring, an on the basis of consent with no other legal

ground. They noted that Article 17(b) of the GDPR uses equivalent language to the recommendation,

113. TESPOK recommended that a provision providing to the effect that ‘where erasure is not technically possible, controller/processor to restrict use’

114. CIPIT were of the view that the clause lacks clarity on the factors to be considered when deciding on a data subject’s request to delete information

The Committee was of the view that the provision in the Bill was very clear.

Clause 41-Data protection by design or default

115. Mozilla cautioned against the over-reliance on pseudonymization as a security tool under clause 41(4), as it may not be feasible in many cases. The Committee averred that the provision in the law was adequate. The Committee proposed amendment of sub-clause 3 as the cost of producing the data may be exponential and therefore should be accounted for.

Clause 42-Particulars of determining organizational measures

116. The Committee agreed with the provisions of Clause 42 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 43-Notification and communication of breach

The Committee received six memoranda from stakeholders on this clause.

117. Digital Lenders Association of Kenya proposed that the Data Commissioner should issue guidelines on the threshold for reporting because parties may report non material breaches.

118. Mozilla recommended clarifying clause 43(5) to require that attribution information to be included “where available”, as it is always very difficult and time consuming to obtain such information. This will ensure timely notification of breach.

119. CIPIT submitted that the terms ‘real risks of harm to the data subject’ is vague and can constitute a loophole for data controllers. Further, subsection 3 to be clarified on what justification for delaying notification meant in subsection 6 there is no guarantee that the encrypted data won’t be accessible to the person who unlawfully obtained the data at that point in time and that they should acquire means to decrypt the data.

120. Google Kenya and CODE-IP Trust proposed that the clause be revised to require notifications only when breach is likely to result in a risk to the rights of the natural persons. They noted that the GDPR contains an equivalent provision.

121. Lawyers Hub proposed that the duty to notify a data subject and should ensure security measures especially for sensitive personal data. Alternatively, such breaches should be logged and presented to the Commission in the annual audit.

122. The Committee held that establishment of a reporting threshold is agreeable to prevent reporting of immaterial breaches. However, a very high threshold must be put in place to protect data subject’s data from being compromised.

Clause 44-Processing of sensitive personal data

The Committee received two memoranda on this Clause.

123. Google Kenya opined that the exemptions provided for under clause 44-47 are very narrow (e.g. religious and political institutions for their membership) and excludes processing even when persons/institutions may have legitimate interests. The recommend that the Bill allows

processing of sensitive data in the language and on similar grounds as GDPR provisions. The committee held that the exemptions were properly provided for in the Bill.

124. TESPOK recommended that entities handling data for deceased will apply the principles of data protection that deal with sensitive personal data as this will provide for sanity in addressing succession issues to enable only registered kin to handle the information with relevant entities.

125. The committee in disagreeing with the stakeholder was of the view that the exemptions are properly provided for under the law.

Clause 45-Permitted grounds for processing sensitive data

The Committee received three memoranda on this clause.

126. Lawyers Hub and Digital Lenders Association of Kenya proposed that the clause should expressly include the government and other public authorities who will collect sensitive personal data and biometric data pursuant to the Registration of Persons Act. The Committee did not agree with the stakeholder.

127. CIPIT disagreed with subsection (b) noting that the complexity of the data generation and processing a data subject 'manifestly' making data public is not sufficient justification of indirectly processing the data without involving the data subject.

Clause 46- Personal data relating to health

128. The Committee agreed with the provisions of Clause 46 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 47-Further categories of sensitive personal data

The Committee received two memoranda on the clause.

129. CIPIT submitted that the threshold provided for in subsection 2(a) and (c) was too high and should be revised to ensure the best interests and protection of the data subjects

130. The Committee agreed with the provisions of Clause 47 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 48-Conditions for transfer out of Kenya

The Committee received four memoranda on this clause.

131. Bowmans law/Coulson Harney LLP proposed that the Data Commissioner should establish at the outset what exactly appropriate safeguards entail. They also proposed that the following underlined words to be included and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

132. Digital Lenders Association of Kenya proposed the revision of clause 48(1)(a) to read; " the Data Controller or Data Processors has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards include jurisdictions with commensurate Data protection Laws and approved by the Data Commissioner.

133. Lawyers Hub proposed clauses 48 and 49 be amended to allow a data subject to waive the requirement of having adequate safeguards as long as the data subject has been adequately informed.

134. CIPIT submitted that the terms 'proof' and 'appropriate safeguards' in subsection 1(a) be clarified and how this oversight and authorization will work in practice. They further noted that subsection c(iii) may be open for abuse due to the term 'public interest'

The Committee agreed with some of the proposal of ensuring that processing of data in jurisdictions with commensurate data protection laws was brought to the attention of the Data commissioner by the data processors and controllers.

Clause 49-Safeguards prior to transfer of personal data out of Kenya

Two memoranda were received on this clause.

135. Digital Lenders Association of Kenya Clause proposed revision of clause 49(1) and (2) to state that appropriate safeguards include jurisdictions with commensurate Data Protection Laws and approved by the Data Commissioner. The committee in not agreeing with the stakeholder stated that amending clause 49 would create a high likelihood of abuse thereby jeopardizing the protection of data subjects.

136. TESPOK was in support of allowing cross border data transfer as long as there was proof of adequate safeguards in place.

Clause 50-Processing through a data server or centre in Kenya

The Committee received five memoranda on this clause. Most stakeholders who made comments on this clause were weary of the power given to the CS regarding processing through a data server or data centre in Kenya.

137. Mozilla opined that the requirement for servers and data centers to be located in Kenya creates a security risk, with a central point of attack or single point failure. It also undermines efficiency and integrity and integrity of internet traffic.

138. CIPIT submitted that strategic interests of the state or on protection of revenue is too vague and must be defined clearly and define 'critical personal data'. They further noted that other jurisdictions have imposed data localization as a way to facilitate unlawful surveillance and limiting the capacity of individuals to protect the confidentiality of their communications.

139. Branch International Limited opined that there should be an amendment to introduce a requirement that where data processing is restricted, the cost of processing data in Kenya as well as the applicable capacity should be comparable to what is available cross border. They also suggested that the affected data controller or data processor should be informed by way of notice of the restriction. And that the affected data controllers/ processors should be heard and be given an opportunity to take any measures to comply or mitigate any adverse effects on its operations. Checks and balance should be introduced to ensure that the powers under the clause are exercised reasonably.

140. Digital Lenders Association of Kenya proposed that the clause should be deleted. There should not be a restriction to force data processors to hold data in their local servers. They also proposed that the decision of the Cabinet Secretary should be subject to appeal at the high court.

141. Bowmans law/ Coulson Harney LLP were of the opinion that Kenya cannot place territorial limits on the processing of certain types of data at the discretion of the Cabinet Secretary since international data controllers need to be assured of the level of technical and network security integrity which Kenya may not be able to guarantee.

142. The committee resolved that there was no need to effect an amendment on this clause as it provided that the Cabinet Secretary “may” prescribe that certain data of strategic interest be processed through Server or data center located in Kenya. This Clause did not mean that all data must be processed in Kenya, besides the process of making regulations will require the requisite public participation from all stakeholders who will be given an opportunity to raise their concerns.

Clause 51- General exemptions

The Committee received five memoranda on this clause. Stakeholders who made submissions under this clause were concerned that the wording of this clause regarding the exemptions for purposes of national security or public order will be prone to abuse if left in the ambiguous wording it currently is in.

143. CIPIT submitted that the exemptions provided in the clause were too broad and should be revised to ensure that they are prescribed by law, respect individuals rights and freedoms. Amnesty International Kenya was concerned that the extent of national security or public order has not been defined in the clause. It must be clear the nature and extent of data that may be collected for purposes of national security or public order. They propose that the state agencies responsible for national security and public order be bound by the general rules of data protection e.g. security of data, collection limitation, purpose limitation, etc.
144. Digital Lenders Association of Kenya proposed that the exemption should apply to both personal data and sensitive data, not just personal data.
145. Article 19 proposed that the clause should require public bodies to apply for exparte orders before processing data unless there is imminent danger to life/property
146. Regarding clause 51(2)(b), Bowmans law/ Coulson Harney LLP were of the view that there should be strict limits on the avoidance of the application of the Bill for national security reasons, by any person in the public interest, national security or public order. The parties seeking protection under the exemptions should be subject to a higher standard of proof and should indicate beyond reasonable doubt why a data subjects rights should not be protected.
147. The taskforce appointed to formulate the Bill and KEPSA also recommended an amendment of clause 51 (2) (c) to delete the word “order” and substitute therefor the word “ interest” as public interest as opposed to public order was more encompassing.
148. The Committee held that this submission should be considered and the rights of a data subject should be given high priority and must be protected from breach that may be excused by flimsy reasons by any public body. It therefore resolved that an amendment requiring public bodies to apply for ex parte orders when collecting data should be added to the clause.

Clause 52- Journalism, literature and art

149. TESPOK proposed the broadening of the journalistic exemption to “processing that is intended for communicating information to the public, ideas or opinions of great interest, including for journalistic purposes and the purposes of academic, artistic or literary expression” The committee did not agree with the stakeholder and directed that the provision in the Bill be retained as it was.

Clause 53- Research, history and statistics

150. The Committee agreed with the provisions of Clause 53 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 54-Exemptions by the Data Commissioner

151. Amnesty International Kenya recommended that the provisions of the Bill regarding limitations to article 31 of the Constitution should meet the criteria set out in article 24 of the Constitution. They thus proposed that clause 54 should instead set out the exemptions clearly in the law and the Commissioner bound by the rules in Article 24 in the exercise of this function. The committee was of the opinion that the clause as provided for in the Bill was adequate.

Clause 55- Data-sharing code

152. The Committee agreed with the provisions of Clause 55 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 56-Complaints to the Data Commissioner

153. CIPIT submitted that subsection 56(b) fails to provide further details on what avenues would be open to a data subject should the Data Commissioner be 'unable to arrange within a reasonable time for the amicable resolution by the parties concerned' The Committee was of the view that the clause should be amended to provide clarity in how the office of the Data Commissioner was going to handle complaints from Data Subjects.

Clause 57- Investigations of complaints

154. The Committee agreed with the provisions of Clause 57 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 58-Enforcement notices.

155. Three memoranda were received on this Clause. Stakeholders who made submissions under this clause had divergent views on the measure of fines and penalties under the Act. Some held the opinion that the fines were too punitive, especially for the SMEs and start-ups while others considered them too lenient.
156. Digital Lenders Association of Kenya opined that the fines are too punitive especially for small players and should be reduced to five hundred thousand and removal of the jail term.
157. Amnesty International Kenya thought the penalties are lenient and may not serve the deterrence purpose especially for big corporations.
158. Google Kenya opined that the fines were not clearly mapped to the likelihood or severity of breach. They proposed that the penalties accorded for violations should be commensurate to the nature, gravity and extent of infringement, in line with GDPR Article 84.
- The Committee was of the view that the penalty was in order so as to deter malpractices in the area of data protection.

Clause 59-Power to seek assistance

159. The Committee agreed with the provisions of Clause 59 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 60-Power of entry and search

160. The Committee agreed with the provisions of Clause 60 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 61-Obstruction of the Data Commissioner

Three memoranda were received on this Clause. Stakeholders who made submissions under this clause had divergent views on the measure of fines and penalties under the Act. Some held the opinion that the fines were too punitive, especially for the SMEs and start-ups while others considered them too lenient.

161. Digital Lenders Association of Kenya opined that the fines are too punitive especially for small players and should be reduced to five hundred thousand and removal of the jail term.
162. Amnesty International Kenya thought the penalties are lenient and may not serve the deterrence purpose especially for big corporations.
163. Google Kenya opined that the fines are not clearly mapped to the likelihood or severity of breach. They proposed that the penalties accorded for violations should be commensurate to the nature, gravity and extent of infringement, in line with GDPR Article 84.
164. The committee was of the view that clause as provided for in the law was adequate.

Clause 62-Penalty notices

165. The Committee agreed with the provisions of Clause 62 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 63- Administrative fines

166. Four memoranda were received on this Clause. Stakeholders who made submissions under this clause had divergent views on the measure of fines and penalties under the Act. Some held the opinion that the fines were too punitive, especially for the SMEs and start-ups while others considered them too lenient.
167. Digital Lenders Association of Kenya opined that the fines are too punitive especially for small players and should be reduced to five hundred thousand and removal of the jail term.
168. CIPIT recommended for a wider variety of sanctions beyond administrative sanctions in case of no compliance or breach of the Bill eg criminal offences and direct liability for directors of companies
169. Amnesty International Kenya thought the penalties are lenient and may not serve the deterrence purpose especially for big corporations.
170. Google Kenya opined that the fines were not clearly mapped to the likelihood or severity of breach. They proposed that the penalties accorded for violations should be commensurate to the nature, gravity and extent of infringement, in line with GDPR Article 84.
171. The committee was of the view that clause as provided for in the law was adequate.

Clause 64-Right of appeal

172. Digital Lenders Association of Kenya proposed the creation of the Data Protection Tribunal to handle all appeals from the administrative action of the Data Commissioner.

This was not agreeable to the committee as the country was moving from the creation of many bodies and tribunals and was of the opinion that the High Court would be better placed to deal with appellate matters arising from the subject matter under this law.

Clause 65-Compensation of data subject

173. The Committee agreed with the provisions of Clause 65 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 66-Preservation Order

174. The Committee agreed with the provisions of Clause 66 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 67- Funds of the Office

175. The Committee agreed with the provisions of Clause 67 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 68-Annual estimates

176. Amnesty International Kenya and Lawyers Hub proposed that the Commissioner to report to the National Assembly instead of the Cabinet Secretary. They suggested that clause 68 be amended to provide that he Commissioner prepares and tables annual financial estimates to the National Assembly.

177. The Committee opined that the provision in the Bill was in order and there was no need for amending the clause of the Bill.

Clause 69-Accounts and Audit

178. The Committee agreed with the provisions of Clause 69 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 70-Annual report

179. Amnesty International Kenya proposed the amendment of clause 70 to provide that the Commissioner gazettes and forwards the annual reports to the Clerk of the National Assembly for debate and adoption.

180. The Committee in disagreeing with the stakeholder opined that the office of the data commissioner was to be held under the aegis of the Cabinet Secretary and therefore the provisions were sufficient.

Clause 71-Regulations

181. CIPIT submitted that the delegated powers were too wide and in particular subsection 2(i) that requires them to make any other regulations they see fit

Clause 72- Offences of unlawful disclosure of Personal Data

182. The Committee agreed with the provisions of Clause 72 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 73- General penalty

183. Amnesty International Kenya were concerned that the penalties provided for under this clause are lenient and may not serve the deterrence purpose especially for big corporations. The Committee agreed with the stakeholder and enhanced the penalty from two years to ten years.

Clause 74-Codes, guidelines and certification

184. The Committee agreed with the provisions of Clause 74 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

Clause 75-Consequential amendments

185. The Committee agreed with the provisions of Clause 75 As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the clause.

3.4 ADDITIONAL PROPOSALS

186. As had been indicated the Committee held public engagements in various counties, the Committee received both oral and written submissions, and the following were the key observation and recommendations from the various counties.

MOMBASA COUNTY

187. The term limit of a data commissioner to be clear such as 3 years and renewable once or a one term of 6 years.

188. Emphasis on the rights of data subject(s) to issue consent before any data is collected or used with clear provisions on the kind of penalties and fines provided in the bill in case of misuse of personal information.

189. The right to consent be clear on the purpose of the data to be collected and consent obtained in a manner that is consultative and not to be obtained forcefully. Information or data collected should not be used to intimidate or deployed for malice by the person or entity tasked with the same

190. The proposed law to include requirements such as values such as trustworthy, professionalism, honesty and respect that will apply to data collectors or processors as well as those in the office of the Data Commissioners.

191. Data collected should be used for only the purpose and objective for which it was collected or sought and not any other.

192. Include a clause to cater for information already in the wrong hands/entities/bodies/agencies.

193. Consent by children through guardian to be clear.

194. Government trusted offices such as the office of the chief to provide data on street families or children without parents and guardian.

195. Data managers to ensure safe keeping and security of data including protecting such data by means of data password with aim of protecting and safeguarding private information.

196. The proposed data commissioner's office should be well resourced with highly qualified and competent staff.

197. Research institutions should be exempted from this law.

198. Enhance provisions on penalties by including a penalty of Kshs 1 million or an imprisonment for 1 year for practices such as unethical hacking.

199. The bill to provide for three (3) months timeframe within which disputes and cases before a court relating to violations of this law be heard and concluded.

200. There should be a specified timeline for data deletion and erasure as well as continuous updating of information/data that may have changed due various circumstances.
201. The rights of the disabled should be considered and be clear in the proposed bill
202. The data commissioner to be independent
203. The office of the data commissioner should be fair and transparent in its dealings, and thus to further inform principles provided in the bill.
204. There should be continuous civic education through the office of the data commissioner
205. The rights of a registered guardian should be protected.
206. Provisions and clauses on deter data leakage should be clear
207. Enhance definition of data to include all forms of data: numbers, text, video, messages, images etc
208. The bill to provide for safety of people giving out data or information on account of their position/mandate or given task or whistle-blowing. Safety of such people is currently compromised.

KILIFI COUNTY

During the public forum sessions in Kilifi, members of the public submitted the following views on the Bill;-

209. The Bill to provide for powers of the Data Commissioner to sue
210. Data misuse to attract a fine not exceeding 2 million and a jail term of 2 – 5 years.
211. The Bill to address concerns on data privacy stored or preserved in various storage locations, forms/ or platforms such as iClouds ,etc
212. Disclosure of sensitive private data including data on personal health should attract a penalty of life imprisonment
213. There should be a clear protocol and engagement mechanism before disclosure by the data subject. Need for systematic approach and policy coherence.
214. The Data Commissioner to ensure integrity of the data, maintenance of data while safeguarding sensitive data particularly on data on health
215. The Data Commissioner's office should be decentralised to enhance outreach and service delivery
216. The creation of the Office of the data Commissioner to be considered further with a view to reduce duplication among existing government offices and if possible the proposed office to be domiciled in the State Department of Interior.
217. Transmission of data to be done within the shortest time possible for effective service delivery and only for the purpose for which it has been obtained.
218. The office of the Data Commissioners should have and utilize adequate legal services i.e. a pool of lawyers to assist in legal issues.
219. Proposed penalties by the public such as life imprisonment to be looked at from the rights of accused person and ensure proposed penalties are deterrent and not punitive.

220. The proposed law to ensure protection of children including dissemination of their data to foreigners.
221. The office of the data commissioner to ensure use of uniform questionnaires when collecting data on a particular theme or same subject to avoid misuse or discrimination.
222. The Bill to be clear on cost of accessing data and to ensure that the cost is affordable.
223. The Data Commissioners office to be domiciled in the office of the Directorate of Criminal Investigations.

KERICHO COUNTY

During the public forum sessions in Kericho, members of the public submitted the following views on the Bill;-

224. The proposed Office of the Data Commissioner would create more institutions, and this will lead to more government expenditure Therefore, use the existing institutions to address the public expenditure pressure that would result from passing of the proposed law.
225. Provide for a penalty of Kshs. 1M and a jail term of 10 to 15 years on account of misuse of data belonging to data subjects or use of such data that are under institutions like Kenya Power and Safaricom for fraud and other criminal activities.
226. Fine to be introduced on third parties in case there is breach or mishandling of the data without consent of the data subjects or where necessary , concurrence of by office of the data commissioner
227. Section 25 of the Bill to be amended to include the following additional principles;
- (a) Fairly and lawfully processed and online with existing rights
 - (b) Processed for limited purpose
 - (c) Adequate relevant and not excessive
 - (d) Not kept for longer than its necessary
 - (e) Secure and where necessary not transferred to other Countries without adequate protection/ safeguards
 - (f) Not giving out information without consent
228. Data Commissioner office should be independent
229. Bill to ensure that the services of the office of Data Commissioner are decentralized with offices across the Country such as Kericho town
230. Sections on regulations to contain provisions to mandating the data protection law to consistently be updated with modern technologies, innovations and other developments in the ICT sector to keep up with the evolving trends in the ICT sector and modern technologies.
231. The bill to provide timelines for data breach notification and to be set at 72 hours, and where possible with penalties to punish for such breaches.
232. The Data Protection Bill to encourage innovation and use of big data including levying businesses using such data for commercialization/business or other purposes.
233. The Bill to provide clause on applications that mine data either by registration or through other means embedded in applications or accessing data through simple source code.

234. Introduce penalties or offences to deter breach of consent

NAKURU COUNTY

During the public forum sessions in Nakuru, members of the public submitted the following views on the Bill:-

235. Sharing of data and related information only be permitted in unavoidable circumstances such as on national security, money laundering investigations by Government agencies, normal criminal/electoral malpractices/ terror activities and drug trafficking investigations.
236. Issues on National security to be well spelt out and declared with clear criteria or circumstances for purpose of ensuring clarity.
237. Criminalize release / sharing of individual information without consent with the following penalties while taking into account deterrence aimed at decongesting prison facilities;
Fine of Ksh 1 Million and imprisonment of 1 year or both fine and jail in extreme cases.
238. Include provisions to grant compensation to Kenyans who suffered in any manner on account of unlawful dissemination of their data in the last five years.
239. Conditions on consent to be clear in every instance or stage.
240. The bill to provide clarity including interpretation on personal data relating to State Officers vis-a-vis provisions of Chapter 6 of the Constitution without curtailing public scrutiny on state officers.
241. The bill to be clear on the number of commissioners, powers of the Commissioners as well as functions of the commissioners as its not clear and comprehensive as currently proposed.
242. Under Clause 8 of the Bill on the functions of the office to include a provision to recognize, reward and sustain intellectuals in the field of data processing and management.
243. The bill to provide for protection of whistle-blowers and witness that give information relating to the provisions of the bill. Past experiences indicate unfair and dangerous treatment of whistle blowers.
244. Data Commissioners to be given prosecutorial and High Court powers to further buttress his functions and enforce consent and other provisions of the bill.
245. Under the Second schedule of the Bill the following proposals were cited by stakeholders for inclusion in the schedule-
- (a) Intellectual Property Act
 - (b) Trade Mark and Copyright Act
 - (c) Industrialization and Trade Act
 - (d) Prevention of organized Crimes Act
 - (e) Ethics and Anti corruption Act
 - (f) Central and Banking Act
 - (g) Land Act
246. The Data Commissioner Office to constantly enhance capacity to handle and manage data.

247. Data commissioner should possess experience on data and ICT rather than having qualification on data science.
248. In clause 30, exemptions in respect to journalistic use may be used for malice and misinformation.
249. When appointing a Data Commissioner, the Public Service Commission to conduct the recruitment process and nominate three persons for appointment by the Cabinet Secretary.

KAKAMEGA AND KISUMU COUNTIES

During the public forum sessions in Kakamega and Kisumu, members of the public submitted the following views on the Bill;-

250. The bill to provide that any data collected should be accompanied by a signed declaration form.
251. The following regime of penalties or fines to apply:
- (a) A fine of kshs 10 million Penalty on data misuse
 - (b) an imprisonment of 7 years with respect to data leakage
 - (c) A fine of kshs 10 million for unauthorised access of personal data i.e snooping and other forms/ways
252. Death sentence/penalty with respect to disclosure of sensitive data which can cause mass harm
253. Criminalize indirect collection of data
254. Proposed law to compel entities or persons who have misuse data to disclose or reveal their sources
255. The bill to provide that the vetting of the Data Commissioner to be done by the National Assembly
256. The bill to provide that cyber owners to be vetted as data processors
257. The data subject to be informed of the lifetime or duration of use of his or her personal data before issuing consent.
258. Ethical hacking should be protected by proposed law bill
259. Clear guidelines to be formulated to ensure full compliance of this bill once enacted into law

NAIROBI COUNTY

260. The Committee had a stakeholder forum in Nairobi and the stakeholders who had submitted their memorandum appeared before the committee to reiterate the contents of their memoranda.
261. The submissions and memoranda from various parties appearing before the Committee are as attached.

CHAPTER THREE

COMMITTEE RECOMMENDATIONS

262. In light of the submissions in the Memoranda, the oral representations made before the Committee and the Committee deliberations on the Bill, the Committee recommends—

CLAUSE 2

THAT, clause 2 of the Bill be amended by—

- (a) inserting the following new definitions in their proper alphabetical sequence—
- “data” means information which—
- (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
 - (b) is recorded with intention that it should be processed by means of such equipment;
 - (c) is recorded as part of a relevant filing system;
 - (d) where it does not fall under paragraph (a) (b) or (c), forms part of an accessible record; or
 - (e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d);
- “person” has the meaning assigned to it in to under Article 260 of the Constitution.

- (b) deleting definition of the term “consent” and substituting therefor the following new definition—
- “consent” means any manifestation of express, unequivocal, free, specific and informed indication of the data subject’s wishes by the data subject by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject”.

Justification:

1. To include the definitions of the terms data and person that have been repeatedly used in the Bill;
2. To delete the definition of “consent” provided for in the bill and substitute with a more elaborate definition that will properly define consent which is a pertinent element of data protection and management

CLAUSE 4

THAT, clause 4 of the Bill be amended by inserting the word “located” immediately after the words “data subjects” appearing in subparagraph (ii) of paragraph (b).

Justification:

The amendment seeks to provide for clarity of the kind of data that can be processed by a data controller or processor who is not resident in the country.

CLAUSE 5

THAT, clause 5 of the Bill be amended by deleting subclause (5) and substituting therefor the following new subclause—

(5) The Data Commissioner shall in consultation with the Cabinet Secretary, establish such directorates as may be necessary for the better carrying out of the functions of the office.

Justification:

The amendment seeks to provide clarity of the provision by inserting a word that was omitted in the sub-clause of the Act as well as to make provisions for directorates that will support the office of the Data Commissioner in the execution of its mandate under this Act.

CLAUSE 6

THAT, clause 6 of the Bill be amended—

- (a) in sub-clause (3) by deleting the words “Cabinet Secretary” and substituting therefor the word “President”;
- (b) by deleting subclause (4) and substituting therefor the following new subclause—

“(4) The Data Commissioner shall be nominated by the President and, with the approval of the National Assembly, appointed by the President”.

Justification:

To ensure that the Data Commissioner is recruited through a competitive process and appointed by the President and not the Cabinet Secretary given the onerous mandate that he or she will be required to execute.

CLAUSE 7

THAT, clause 7 of the Bill be amended by inserting the following new paragraph immediately after paragraph c—

“(ca) holds a master’s degree.

Justification:

To introduce reasonable qualifications for appointment as Data Commissioner i.e. one has to hold at least a masters’ degree to serve in this is a technical position that may require some additional knowledge and expertise.

CLAUSE 13

THAT, the Bill be amended by deleting clause 13 and substituting therefor the following

— Staff of the Office.

13. The Data Commissioner shall in consultation with the Public Service Commission, appoint such number of staff as may be necessary for the proper and efficient discharge of the functions under this Act or any other relevant law.

Justification:

To allow the Data Protection Commissioner to consult with the Public Service Commission when appointing his staff. Public Service Commission is a constitutionally mandated Commission that handles matters of human resource in the public service.

CLAUSE 15

THAT, clause 15 of the Bill be amended by deleting the word “the” appearing immediately after the words “First Schedule on” in sub-clause (5).

Justification:

The amendment seeks to correct a typographical error in the Bill.

CLAUSE 19

THAT, clause 19 of the Bill be amended by—

- (a) deleting subclause (4) and substituting therefor the following new subclause —
“(4) The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration;
- (b) inserting the word “this” immediately after the words “the provisions of” appearing in sub-clause (7).

Justification:

The amendment seeks to clarify the provision on registration and clearly set out that a certificate shall only be issued when the requirements of registration are met as well as to correct a typographical error.

CLAUSE 25

THAT, clause 25 of the Bill be amended by inserting the following new paragraph immediately after paragraph (d)—

“(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;”

Justification

The additional principle was aimed at ensuring that data subjects are duly informed of reasons for collection of data relating to private and family affairs so that they can make informed decisions before granting the consent.

CLAUSE 29

THAT, clause 29 of the Bill be amended by—

- (a) deleting paragraph (d) and substituting therefor the following new paragraph —
“(d) the third parties whom personal data has been or will be transferred to, including details of safeguards adopted;

- (b) inserting the following new paragraph immediately after paragraph (e)—
“(f) a description of the technical and organization security measures taken to ensure the integrity and confidentiality of the data”.

Justification

The proposed amendment seeks to ensure that the rights of data subjects are protected and that security measures are taken into account by data controllers and processors to ensure the integrity of data collected.

CLAUSE 31

THAT, clause 31 of the Bill be amended by inserting the following new subclauses immediately after sub-clause (4) —

“(5) The data impact assessment reports shall be submitted sixty days prior to the processing of data;

“(6) The Data Commissioner shall set out guidelines for carrying out an impact assessment under this section.

Justification:

1. There is need for the Data Protection Commissioner to set out the types of processing operations that will require a data impact assessment.
2. Setting of timelines on when data impact assessment reports should be submitted will ensure protection of the rights of data subjects when processing operations likely to result in high risk to the rights of data subjects.

CLAUSE 35

THAT, clause 35 of the Bill be amended in subclause (3) (b) by deleting the word “before” and substituting therefor the word “after”.

Justification:

The amendment seeks to correct a typographical error in the Bill.

CLAUSE 37

THAT, Bill be amended by deleting clause 37 and substituting therefor the following —

Commercial use of data.

37. (1) A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person-

- (a) has sought and obtained express consent from a data subject; or
- (b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

(3) The Cabinet Secretary in consultation with

the Data Commissioner may prescribe practice guidelines for commercial use of personal data in accordance with this Act.

Justification:

The current proposal was making reference to direct marketing while the new provision is seeking to ensure that data used for commercial purposes which is much broader than direct marketing is properly secured.

CLAUSE 41

THAT, clause 41 of the Bill be amended in subclause (3) by inserting the following new paragraph immediately after paragraph (d)—

(e) the cost of processing data and the technologies and tools used.

Justification

It is imperative to have in mind the cost and technology that will be required in processing data as sometimes the cost of producing the data may be exponential and therefore should be accounted for.

CLAUSE 48

THAT, clause 48 of the Bill be amended by—

- (a) deleting the item “(1)” appearing immediately before the words “a data controller”;
- (b) deleting paragraph (b) and substituting therefor the following new paragraph—
“(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;”

Justification

The amendment is necessary to provide clarity in the bill as well as to set out jurisdiction with commensurate data protection laws during transborder transfer of data

CLAUSE 51

THAT, clause 51 of the Bill be amended in sub-clause (2) by deleting the word “order” appearing in paragraph (b) and substituting therefor the word “interest”.

Justification:

1. To substitute the words public order with public interest. Public interest is a broader concept which encompasses an interest that is a common concern among citizens in the management, local and national affairs.
2. To mandate public bodies seeking to retrieve data necessary for national security and public interest to secure ex parte orders from the law courts before retrieving such information to safeguard the rights of data subjects against fragrant abuse.

CLAUSE 56

THAT, Bill be amended by deleting clause 56 and substituting therefor the following —

Complaints to the
Data Commissioner

56. (1) A data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner in accordance with this Act-

(2) A person who intends to lodge a complaint under this Act shall do so orally or in writing.

(3) Where a complaint made under subclause (1) is made orally, the Data Commissioner shall cause the complaint to be recorded in writing and shall be dealt with in accordance with such procedures as the Data Commissioner may prescribe.

(4) A complaint lodged under subclause (1) shall contain such particulars as the Data Commissioner may prescribe.

(5) a complaint made to the data commissioner shall be investigated and concluded within ninety days.

Justification:

This clause seeks to provide clarity with regards to complaints mechanism by data subjects aggrieved by a decision of any person under this Act.

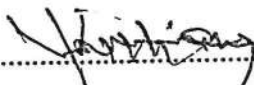
CLAUSE 73

THAT, clause 73 of the Bill be amended in subclause (1) by deleting the word “two” appearing immediately after the word “year” and substituting therefor the word “ten”.

Justification:

To enhance the sentence of the general penalty in a bid to deter persons from committing offences under this Act. The proposed two years’ imprisonment is too lenient and may not serve the purpose of ensuring the protection of personal data.

SIGNED.....



DATE.....

17/10/2019

HON. WILLIAM KISANG, MP - CHAIRPERSON

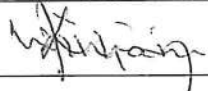

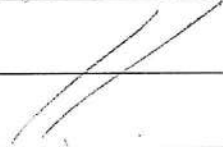
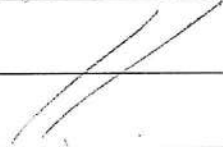





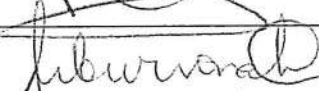
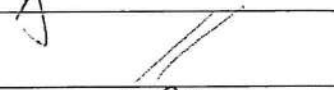


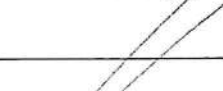
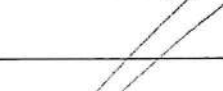
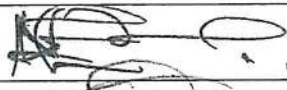



DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION
AND INNOVATION

**THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION
AND INNOVATION**

ADOPTION LIST

DATE: 17/10/2019 **TIME:** 9:30 AM **VENUE:** 11th Floor Protection House

AGENDA: ADOPTION OF THE REPORT ON THE CONSIDERATION OF THE DATA PROTECTION BILL, 2019

NO.	NAME	SIGNATURE
1.	Hon. Kisang, William Kipkemoi, M.P - Chairperson	
2.	Hon. George, Macharia Kariuki, M.P - Vice – Chairperson	
3.	Hon. Liza, Chelule Chepkorir, M.P.	
4.	Hon. Alfah, O. Miruka, M.P.	
5.	Hon. Annie Wanjiku Kibeh, M.P.	
6.	Hon. Joshua Kimilu, Kivinda, M.P.	
7.	Hon. Marwa Kitayama Maisori, M.P.	
8.	Hon. Mwambu Mabongah, M.P.	
9.	Hon. Maritim Sylvanus, M.P.	
10.	Hon. Mwangaza Kawira, M.P.	
11.	Hon. Jonah Mburu, M.P.	
12.	Hon. Gertrude Mbeyu Mwanyanje, M.P.	
13.	Hon. Wamuchomba, Gathoni, M.P.	
14.	Hon. (Eng). Mark Nyamita Ogola, M.P.	
15.	Hon. John Kiarie Waweru, M.P.	
16.	Hon. Erastus Nzioka Kivasu, M.P.	
17.	Hon. Godfrey Osotsi, Atieno, M.P.	
18.	Hon. Innocent Momanyi, Obiri, M.P.	
19.	Hon. Anthony, Tom Oluoch, M.P.	

MINUTES OF THE 43RD SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION & INNOVATION HELD IN BOARDROOM ON 11TH FLOOR PROTECTION HOUSE, PARLIAMENT BUILDINGS ON THURSDAY 17TH OCTOBER, 2019 AT 9.30AM

PRESENT

- | | |
|---------------------------------------|--------------------|
| 1. Hon. William Kipkemoi, M.P. | -Chairperson |
| 2. Hon. George Macharia Kariuki, M.P. | -Vice- Chairperson |
| 3. Hon. Annie Wanjiku Kibeh, M.P. | |
| 4. Hon. Maritim Sylvanus, MP | |
| 5. Hon. Mwangaza Kawira, M.P | |
| 6. Hon. Anthony Oluoch, M.P. | |
| 7. Hon. Erastus Nzioka Kivasu, M.P | |
| 8. Hon. Godfrey Osotsi Atieno, M.P | |
| 9. Hon. Mwambu Mabongah, M.P | |
| 10. Hon. Marwa Kitayama Maisori, M.P | |
| 11. Hon. Joshua Kimilu Kivinda, M.P. | |
| 12. Hon. Wamuchomba Gathoni, M.P | |
| 13. Hon. Jonah Mburu, M.P | |

APOLOGIES

1. Hon. John Kiarie Waweru, M.P
2. Hon. Liza Chelule Chepkorir ,M.P
3. Hon. Innocent Momanyi Obiri, M.P
4. Hon. (Eng.). Mark Nyamita, M.P
5. Hon. Gertrude Mbeyu Mwanyanje, M.P
6. Hon. Alfah O. Miruka, M.P

THE SECRETARIAT

- | | |
|-----------------------|----------------------|
| 1. Ms. Hellen Kina | - Clerk Assistant II |
| 2. Ms. Ella Kendi | - Clerk Assistant II |
| 3. Mr. Nimrod Ochieng | - Audio Officer |

MIN.NO/NA/CII/2019/188: PRELIMINARIES

The Chairperson called the meeting to order at thirty two minutes past nine o'clock followed by a word of prayer.

MIN.NO/NA/CII/2019/189: CONFIRMATION OF THE MINUTES

The agenda was deferred to the next meeting.

MIN.NO/NA/CII/2019/190: ADOPTION OF THE REPORT ON THE CONSIDERATION OF THE DATA PROTECTION BILL, 2019

The Committee considered and adopted the report with the following recommendations having been proposed by Hon. Anthony Oluoch, MP and seconded by Hon. Marwa Maisori, MP

In light of the submissions in the Memoranda, the oral representations made before the Committee and the Committee deliberations on the Bill, the Committee recommends—

CLAUSE 2

THAT, clause 2 of the Bill be amended by—

- (a) inserting the following new definitions in their proper alphabetical sequence—
“data” means information which—
 - (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
 - (b) is recorded with intention that it should be processed by means of such equipment;
 - (c) is recorded as part of a relevant filing system;
 - (d) where it does not fall under paragraph (a) (b) or (c), forms part of an accessible record; or
 - (e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d);“person” has the meaning assigned to it in to under Article 260 of the Constitution.

- (b) deleting definition of the term “consent” and substituting therefor the following new definition—
“consent” means any manifestation of express, unequivocal, free, specific and informed indication of the data subject’s wishes by the data subject by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject”.

Justification:

1. To include the definitions of the terms data and person that have been repeatedly used in the Bill;
2. To delete the definition of “consent” provided for in the bill and substitute with a more elaborate definition that will properly define consent which is a pertinent element of data protection and management

CLAUSE 4

THAT, clause 4 of the Bill be amended by inserting the word “located” immediately after the words “data subjects” appearing in subparagraph (ii) of paragraph (b).

Justification:

- a. The amendment seeks to provide for clarity of the kind of data that can be processed by a data controller or processor who is not resident in the country.

CLAUSE 5

THAT, clause 5 of the Bill be amended by deleting subclause (5) and substituting therefor the following new subclause—

- (5) The Data Commissioner shall in consultation with the Cabinet Secretary, establish such directorates as may be necessary for the better carrying out of the functions of the office.

Justification:

The amendment seeks to provide clarity of the provision by inserting a word that was omitted in the sub-clause of the Act as well as to make provisions for directorates that will support the office of the Data Commissioner in the execution of its mandate under this Act.

CLAUSE 6

THAT, clause 6 of the Bill be amended—

- (a) in sub-clause (3) by deleting the words “Cabinet Secretary” and substituting therefor the word “President”;
- (b) by deleting subclause (4) and substituting therefor the following new subclause—

“(4) The Data Commissioner shall be nominated by the President and, with the approval of the National Assembly, appointed by the President”.

Justification:

To ensure that the Data Commissioner is recruited through a competitive process and appointed by the President and not the Cabinet Secretary given the onerous mandate that he or she will be required to execute.

CLAUSE 7

THAT, clause 7 of the Bill be amended by inserting the following new paragraph immediately after paragraph c—

“(ca) holds a master’s degree.

Justification:

To introduce reasonable qualifications for appointment as Data Commissioner i.e. one has to hold at least a masters’ degree to serve in this is a technical position that may require some additional knowledge and expertise.

CLAUSE 13

THAT, the Bill be amended by deleting clause 13 and substituting therefor the following —

Staff of the Office.

13. The Data Commissioner shall in consultation with the Public Service Commission, appoint such number of staff as may be necessary for the proper and efficient discharge of the functions under this Act or any other relevant law.

Justification:

To allow the Data Protection Commissioner to consult with the Public Service Commission when appointing his staff. Public Service Commission is a constitutionally mandated Commission that handles matters of human resource in the public service.

CLAUSE 15

THAT, clause 15 of the Bill be amended by deleting the word “the” appearing immediately after the words “First Schedule on” in sub-clause (5).

Justification:

The amendment seeks to correct a typographical error in the Bill.

CLAUSE 19

THAT, clause 19 of the Bill be amended by—

- (a) deleting subclause (4) and substituting therefor the following new subclause —
“(4) The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration;
- (b) inserting the word “this” immediately after the words “the provisions of” appearing in sub-clause (7).

Justification:

The amendment seeks to clarify the provision on registration and clearly set out that a certificate shall only be issued when the requirements of registration are met as well as to correct a typographical error.

CLAUSE 25

THAT, clause 25 of the Bill be amended by inserting the following new paragraph immediately after paragraph (d)—

“(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;”

Justification

The additional principle was aimed at ensuring that data subjects are duly informed of reasons for collection of data relating to private and family affairs so that they can make informed decisions before granting the consent.

CLAUSE 29

THAT, clause 29 of the Bill be amended by—

- (a) deleting paragraph (d) and substituting therefor the following new paragraph —
“(d) the third parties whom personal data has been or will be transferred to, including details of safeguards adopted;
- (b) inserting the following new paragraph immediately after paragraph (e)—
“(f) a description of the technical and organization security measures taken to ensure the integrity and confidentiality of the data”.

Justification

The proposed amendment seeks to ensure that the rights of data subjects are protected and that security measures are taken into account by data controllers and processors to ensure the integrity of data collected.

CLAUSE 31

THAT, clause 31 of the Bill be amended by inserting the following new subclauses immediately after sub-clause (4) —

- “(5) The data impact assessment reports shall be submitted sixty days prior to the processing of data;
- “(6) The Data Commissioner shall set out guidelines for carrying out an impact assessment under this section.

Justification:

1. There is need for the Data Protection Commissioner to set out the types of processing operations that will require a data impact assessment.
2. Setting of timelines on when data impact assessment reports should be submitted will ensure protection of the rights of data subjects when processing operations likely to result in high risk to the rights of data subjects.

CLAUSE 35

THAT, clause 35 of the Bill be amended in subclause (3) (b) by deleting the word “before” and substituting therefor the word “after”.

Justification:

The amendment seeks to correct a typographical error in the Bill.

CLAUSE 37

THAT, Bill be amended by deleting clause 37 and substituting therefor the following —

Commercial use of
data.

37. (1) A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person-

- (a) has sought and obtained express consent from a data subject; or
- (b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

(3) The Cabinet Secretary in consultation with the Data Commissioner may prescribe practice guidelines for commercial use of personal data in accordance with this Act.

Justification:

The current proposal was making reference to direct marketing while the new provision is seeking to ensure that data used for commercial purposes which is much broader than direct marketing if properly secured.

CLAUSE 41

THAT, clause 41 of the Bill be amended in subclause (3) by inserting the following new paragraph immediately after paragraph (d)—

- (e) the cost of processing data and the technologies and tools used.

Justification

It is imperative to have in mind the cost and technology that will be required in processing data as sometimes the cost of producing the data may be exponential and therefore should be accounted for.

CLAUSE 48

THAT, clause 48 of the Bill be amended by—

- (a) deleting the item “(1)” appearing immediately before the words “a data controller”;
- (b) deleting paragraph (b) and substituting therefor the following new paragraph—
“(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;”

Justification

The amendment is necessary to provide clarity in the bill as well as to set out jurisdiction with commensurate data protection laws during transborder transfer of data

CLAUSE 51

THAT, clause 51 of the Bill be amended in sub-clause (2) by deleting the word “order” appearing in paragraph (b) and substituting therefor the word “interest”.

Justification:

1. To substitute the words public order with public interest. Public interest is a broader concept which encompasses an interest that is a common concern among citizens in the management, local and national affairs.
2. To mandate public bodies seeking to retrieve data necessary for national security and public interest to secure ex parte orders from the law courts before retrieving such information to safeguard the rights of data subjects against fragrant abuse.

CLAUSE 56

THAT, Bill be amended by deleting clause 56 and substituting therefor the following —

Complaints to the
Data Commissioner

56. (1) A data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner in accordance with this Act-

(2) A person who intends to lodge a complaint under this Act shall do so orally or in writing.

(3) Where a complaint made under subclause (1) is made orally, the Data Commissioner shall cause the complaint to be recorded in writing and shall be dealt with in accordance with such procedures as the Data Commissioner may prescribe.

(4) A complaint lodged under subclause (1) shall contain such particulars as the Data Commissioner may prescribe.

(5) a complaint made to the data commissioner shall be investigated and concluded within ninety days.

Justification:

This clause seeks to provide clarity with regards to complaints mechanism by data subjects aggrieved by a decision of any person under this Act.

CLAUSE 73

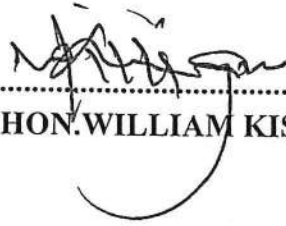
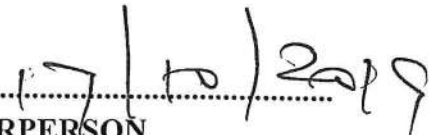
THAT, clause 73 of the Bill be amended in subclause (1) by deleting the word “two” appearing immediately after the word “year” and substituting therefor the word “ten”.

Justification:

To enhance the sentence of the general penalty in a bid to deter persons from committing offences under this Act. The proposed two years’ imprisonment is too lenient and may not serve the purpose of ensuring the protection of personal data.

MIN.NO/NA/CII/2019/191:ADJOURNEMENT

There being no other business, the meeting was adjourned at forty nine minutes past ten o’clock

SIGNED..........DATE..........
HON.WILLIAM KISANG, MP - CHAIRPERSON

which involved meticulous details his directive to have uniforms based in Syongila, loaded and and the country," said Mr Kakawa.

REPUBLIC OF KENYA



THE NATIONAL ASSEMBLY TWELFTH PARLIAMENT - THIRD SESSION

In the matter of consideration by the National Assembly:-
The Data Protection Bill (National Assembly Bill No.44 of 2019)

NOTIFICATION FOR PUBLIC HEARINGS

Article 118(1)(b) of the Constitution provides that, "Parliament shall facilitate public participation and involvement in the legislative and other business of Parliament and its Committees". Further, the National Assembly Standing Order 127(3) requires the Departmental Committee to which a Bill is committed to facilitate public participation and take into account the views and recommendations of the public when the Committee makes its report to the House.

The Data Protection Bill, 2019 main objective is to give effect to the right to privacy as provided for in Article 31(c) and (d) of the Constitution by setting out the requirement for the protection of personal data processed by both public and private entities.

The Data Protection Bill, 2019 has undergone First Reading pursuant to Standing Order 127(3) and is now committed to the Departmental Committee on Communication, Information and Innovation for consideration and thereafter report to the House.

Pursuant to Article 118(1)(b) of the Constitution and the Standing Order 127(3) members of the public are hereby notified that the Committee will be conducting public hearings on the Data Protection Bill, 2019 in the following Counties:-

COUNTY	VENUE/TOWNS	DATE
1. - Mombasa	Kenya School of Government Hall	Thursday, 15 th August, 2019
2. Kilifi	Makio Kinamai Social Hall	Friday, 16 th August, 2019
4. Kisumu	New Nyanza Regional Headquarters	Thursday, 22 nd August, 2019
5. Kakamega	Salvation Army Social Hall	Friday, 23 rd August, 2019
6. Kericho	Holy Trinity Academy Hall	Thursday, 29 th August, 2019
7. Nakuru	Nakuru Old Town Hall	Friday, 30 th August, 2019
7. Laikipia	Nanyuki Social Hall	Friday, 13 th September, 2019
8. Isiolo	Silver Bells Hotel	Saturday, 14 th September, 2019
9. Nairobi	County Hall, Parliament Buildings	Tuesday, 17 th September, 2019

The soft copy of the Bill is available on the website of the Parliament of Kenya www.parliament.go.ke.

MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY



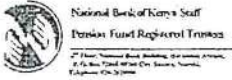
MINISTER
State Department of
KASARANI TECHNICAL
P.O. BOX 51898-00200 NA
Email: kasaranitechnical@gmail.com

Kasarani Technical and Vocational College is a Public Nairobi County, Kasarani Constituency, Kamulu Shop from City Centre: at Bus Station, use bus No. 39, routes courses listed below which are starting in September 2019

COURSES COMMENCING		
DIPLOMA COURSES	Minimum Grade	Duration
Welding & Fabrication Module 1-3	KCSE C- or above	3 years
Information Comm. & Telecommunication Module 1-3	KCSE C- or above	3 years
Automotive Engineering Module 1-3	KCSE C- or above	3 years
Electrical Engineering (Power) Option Module 1-3	KCSE C- or above	3 years
Building & Construction Module 1-3	KCSE C- or above	3 years
Mechanical Engineering (Production) Module 1-3	KCSE C- or above	3 years
Social Work & Community Development Module 1-3	KCSE C- or above	3 years
Information Science Modul 1-3	KCSE C- or above	3 years
Business Management Module 1-3	KCSE C- or above	3 years
Supply Chain Management Module 1-3	KCSE C- or above	3 years
Human Resource Management Module 1-3	KCSE C- or above	3 years
Project Management Module 1-3	KCSE C- or above	3 years

Download an application form from www.kasaranitechnical.com application fee of 500 Kenya Shillings. Any student who is to register. The application for HELB loan is ongoing until 30th August.

All applications to be addressed to: The Principal, Kasarani TVC,



National Bank

Notice is hereby given that the Annual General Meeting of the National Bank of Kenya Limited Staff Pension Fund Registered Trustees will be held at TinTin Restaurant, KICC, Harambee Avenue on Tuesday, 27th July 2019 at 11:30 A.M. to transact the following business:-

- Ordinary Business**
1. Introduction by the Chairperson of the Board of Trustees.
 2. The Chairperson's Report.
 3. Presentation on the Fund Investments by GenAfrica Asset Managers & Sanlam Investments.
 4. Presentation on the Role of the Custodian by National Bank of Kenya Limited.
 5. Presentation on the role of the administrator and financial planning tips by Zamara Actuaries, Administrators & Consultants Ltd.
 6. Presentation on the Fund Audited Accounts for the year ended 31st December 2018 by Deloitte & Touche.
 7. Presentation by the Retirement Benefits Authority.
 8. Trustees Remuneration.
 9. Question and Answer Session.
 10. Vote of Thanks.

To transact any other business of the Annual General Meeting for which notice has been given in advance.

Copies of the annual reports and financial statements of the Scheme are available from the Human Resources Department.

By order of the Board of Trustees
 Linnet Mirehane
 Chairperson, NBK Staff Pension Fund Registered Trustees

REPUBLIC OF KENYA



**THE NATIONAL ASSEMBLY
 TWELFTH PARLIAMENT - THIRD SESSION**

- Matters of consideration by the National Assembly:-
1. The Crops (Amendment) Bill (National Assembly Bill No. 25 of 2019)
 2. The Data Protection Bill (National Assembly Bill No. 44 of 2019)

SUBMISSION OF MEMORANDA

Article 118(1)(b) of the Constitution provides that, "Parliament shall facilitate public participation and involvement in legislative and other business of Parliament and its Committees". The National Assembly Standing Order 127(3) provides that, "the Departmental Committee to which a Bill is committed shall facilitate public participation and take account the views and recommendations of the public when the Committee makes its report to the House".


Crops (Amendment) Bill, 2019 seeks to amend the First Schedule to the Crops Act, 2013 to include Achioté as one of the scheduled crops. Achioté crop is locally known as 'Mrangi' because of its bright red fruits and is grown largely in the coastal region but its potential has not been fully utilized. According to the Agricultural experts, the crop matures fully in four to five years and has an economic life span of 20 years but can be harvested even after one year in the farm. It is the world's second most important natural colourant and makes about 70 percent of the world's natural dyes.

Data Protection Bill, 2019 seeks to give effect to the right to privacy as provided for in Article 31(c) and (d) of the Constitution by setting out the requirement for the protection of personal data processed by both public and private entities.

The above mentioned Bills have undergone First Reading pursuant to Standing Order 127(3) and stand committed to the Departmental Committee on Agriculture & Livestock and Departmental Committee on Communication, Information & Innovation respectively, for consideration and thereafter report to the House.

Pursuant to the provisions of Article 118(1)(b) of the Constitution and Standing Order 127(3), the respective Committee members of the Public to submit representations they may have on the said Bills. The representations may be made to the Clerk of the National Assembly, P.O. Box 41842-00100, Nairobi; hand-delivered to the Office of the Clerk, Main Parliament Buildings, Nairobi; or emailed to clerk@parliament.go.ke; to be received on or before Tuesday, 16th July, 2019 at 5.00 pm.

MICHAEL R. SIALAB, EBS
 CLERK OF THE NATIONAL ASSEMBLY



KENYA INSTITUTE OF SUPPLIES MANAGEMENT
 Promoting Professionalism in Supply Chain Management

JULY-DECEMBER 2019 TRAINING PROGRAM

Theme	Dates Venue / No. of Days	About the Course	CPD Hours	Fees in Ksh (Exclusive of VAT)			
				Member		Non-member	
				Early Bird	Normal	Early Bird	Normal
Procurement Contract Implementation and Monitoring	3-5, July 3 Days Kisumu	The workshop outlines the role of procurement practitioners and users in contract implementation, monitoring and reporting.	20	61,500	63,000	65,500	67,000
Surveying and Developing Your Supply Market	23-26, July 4 Days Nakuru	Obtaining the right suppliers contributes to success in the purchasing process. The workshop presents a guide for supplier management, and equips the practitioners with salient skills to ensure good supplier management practices.	24	70,000	73,500	76,000	79,500
WORLD BANK PROGRAM							
Procurement for World Bank Financed Projects	5-16, August 2 Weeks Mombasa	This workshop has been structured to equip participants with knowledge and techniques for managing procurement under the new (2015) World Bank Procurement Policy, and for similar donor financed projects. The program has been developed by the World Bank and is delivered in partnership with Kenya Institute of Supplies Management (KISM).	24	KES 185,600.00 (Inclusive VAT)			
				USD 1,700.00 (Inclusive VAT)			
Logistics, Inventory & Warehousing Management	27-30, August 4 Days Kisumu	The necessity of inventory holding remains a heated debate the world over. Concepts such as JIT, Lean and Agile supply chains have emerged in the last few decades as strategies towards zero stockholding. This workshop equips the practitioner with best practice in inventory and stores management that lead to cost savings and efficiency in the stores function.	24	67,500	71,000	73,500	77,000
INTERNATIONAL FEDERATION OF PURCHASING AND SUPPLY MANAGEMENT PROGRAM							
IFPSM World Summit 2019: Sustainable Procurement and Supply Chain Practices for the 21 st Century	10-13, September 4 Days Mombasa	The World Summit 2019 will review pertinent procurement and supply chain management issues and developments from around the world. Participants will be updated on trends and future direction of procurement and supply management knowledge, professional practice, technology, legal, regulatory and policy frameworks. Research findings in procurement and supply will also be discussed at the summit.	24	KES 72,000.00			
				USD 720.00			
Preparing Bidding Documents	23-27, September 5 Days Mombasa	Bidding documents form an integral part of the procurement cycle. The documents embody a framework and prescribe the quality of all inputs and outputs of a procurement process, from conceptualization to contract implementation and closure. Attendees in this workshop will be taken through the rigours of developing reliable and effective bidding documents for their procurement processes.	24	83,000	86,500	90,000	93,500
Procurement Training for Committee Members and Users Departments	1-4, October 4 Days Nakuru	Procurement is a collaborative activity that requires all officials within an organisation to obtain working knowledge of procurement laws and regulations. The role of users and various committee members in the success of a procurement cannot, therefore, be over-emphasized. This workshop is designed to equip various players in the procurement process with transferable skills for optimal performance.	24	70,000	73,500	76,000	79,500
Realizing LEAN in Procurement and Supply Chain Management	21-25, October 3 Days Kisumu	LEAN is a philosophy of delivering value from your customer's perspective, eliminating waste and continuously improving your processes. The workshop focuses on strategies for reducing inventory, shortening lead time and reducing cost.	20	61,500	63,000	65,500	67,000
Procurement of Consultancy and Non-Consultancy Services	12-15, November 4 Days Kisumu	This course is designed to bring out best practices in procurement of consultancy and non-consultancy services.	24	67,500	71,000	73,500	77,000
Avoiding the Pitfalls of Public Procurement: Lessons from Review Board Cases	27-29, November 3 Days Mombasa	This workshop analyses and draws lessons from public procurement appeals and cases handled by the Administrative Reviews Board. The workshop's primary objective is to upscale participants capacity to recognize risks in procurement proceedings, and with a frame of mind to formulate, guide or implement decisions that eliminate or mitigate the risks. The delivery of this workshop will be through a partnership between KISM and the Administrative Reviews Board.	20	70,000	73,500	77,000	80,500
Project Procurement Management	3-6, December 4 Days Mombasa	This workshop presents fundamental concepts and techniques for project acquisition and procurement within the project. Participants will be guided through project evaluation, planning, financing, contracting, negotiation, and procurement execution. Methods, principles, and practices in infrastructure project procurement, including Public-Private Partnerships will be highlighted.	24	67,500	71,000	74,500	78,500
Implementing the Public Procurement and Asset Disposal Act 2015	17-20, December 4 Days Mombasa	This workshop focuses on procurement reforms and enlightens practitioners on how best to take advantage of the reforms to improve procurement performance at the organisational level.	24	70,500	74,000	76,500	80,000

12th Floor, Nation Centre, Nairobi
 ☎ 254-721 2448280 / 713 244828 / 705 244828
 ✉ programs@kism.or.ke @ www.kism.or.ke

③ CHEMWEU
Please note
FA
24/9/19

① D/Com's
Please deal
23/09/19

Mr Michael L Sialai EBS
Clerk of the National Assembly of Kenya <clerk@parliament.go.ke>
Nairobi
Kenya

② KINA
Please deal
FA
24/9/19

Dear Mr Sialai,

Ref: Your call for Submission of Memoranda regarding the Data Protection Bill, 2019 (National Assembly Bills No. 44.)

I refer to your recent public notice inviting members of the public to submit representations they may have on the above bill. Please find below my representations.

Before I give my representations, I should like to strongly object to the very short time provided for members of the public to give their views to their matter.

It is scandalous and, almost certainly unconstitutional, as well as against the National Assembly's own guidance, to only give 3 working days (11th - 16th July 2019) for contributions on what is, without any doubt, a very important piece of legislation that seeks to give further effect to the constitutional right to privacy. It is further regrettable that, despite request for additional time for public representatives, you have chosen to stick to the original deadline.

It is sincerely hoped that you will consider the issue for the future and allow enough time for members of the public a chance to exercise their constitutional right of public participation.

It is welcome that Parliament has finally decided to enact data protection legislation for Kenya. There has been a lacuna in our laws, especially since the adoption of the new Constitution almost 10 years ago.

Having had a chance to read through the bill, I have the following observations, points to be clarified and suggestions to make. Kindly bring them to the attention of the relevant departmental committee on my behalf.

1. The bill creates a new state office: the Data Protection Commission (DPC). Unlike similar constitutional commissions, for example, the Commission on Administrative Justice (CAJ) and the Kenya National Human Rights Commission (KNHRC) there is no public vetting or any form of public participation in the appointment of the DPC. Instead, this role is left to the Public Service Commission (PSC). Given the importance that is being given to this new office (state office, security of tenure, under the jurisdiction of the Salary and Remuneration Commission (SRC), Parliament should consider adopting the same recruitment process for the DPC as currently applies to constitutional commissions and independent office holders such as the Director of Public Prosecution, the Auditor General and the members of the Commission on Revenue Allocation. The same principle applies to the process of removal from office of the DPC. Parliament should consider prescribing the removal process set out in Article 251, Constitution of Kenya (CoK) 2010 to be applicable to the removal of the DPC. This would be in keeping with the letter and the spirit of the CoK;
2. The bill allows nomination of three people, listed in the order of merit, to be forwarded to the responsible Cabinet Secretary (CS) from which the CS to choose one person.



This provision allows for considerations other than merit to be used by the CS to make the appointment. This cannot be right as it allows the CS to consider extraneous factors, not provided for in the law or clearly known to either the candidates or the general public, in making the appointment. Parliament should provide that only the candidate who meets the recruitment criteria set by the PSC is recommended for and appointed by the CS;

3. While the bill provides a time-frame for the filing of any vacancy in the office of the DPC, it does not provide how soon after such a vacancy arises that the recruitment process should commence. This contrasts to how vacancies in most of the independent commissions or offices are filled: within 14 days of a vacancy arising. To safeguard the effectiveness of the office of the DPC, Parliament should explicitly require the CS to notify the PSC of a vacancy in the office of the DPC within 14 days of such a vacancy arising;
4. Parliament has a duty to be prudent about the use of public resources. In the respect, it is not clear why role of the DPC cannot be fulfilled by CAJ. The CAJ is already up and running, there are current moves to require it to have offices in each county. In addition, the CAJ already has mandate to enforce the Access to Information Act, 2016, including the rights under Art. 35(2), CoK, 2010. The money for setting up new DPC would be better spent increasing capacity of an existing state agency that seems to be making a difference in people's lives. This would also address some of the governance and structural weaknesses of the new DPC as set out above;
5. Is the definition of "personal data" in the bill the same as the one Parliament has given to "personal information" in the Access to Information, Act, 2016, which implements Art. 35, CoK, 2010?
6. How will the bill, if enacted without changes, affect the ability of a deceased person's relatives/executors/administrators deal with the deceased person's personal data in the absence of an explicit and verifiable authorisation from the deceased before their death?
7. The bill's provision regarding processing of personal data for children seems very draconian and could well be in breach of the rights of children. Since, under the laws of Kenya, a child is anyone under the age of 18 years, the requirement for parental/guardian consent, which may be appropriate for, say a child of 5 years, would be totally inappropriate for a child of say, 13 – 17 years. This needs to be reconsidered to ensure that, while the right of children is protected, it is also recognised that they may want to access services that require them to give their personal details in instances they may not want to involve their parents and guardians. Related to this, the duty of data processors and controllers to be able to verify the age of their users needs to be thought through. As it currently stands, the bill may end up making it a requirement of data processors to verify the age of all their users as the default position. This would then defeat the whole object of the bill which is to control how personal data is used, based on the principle of only requiring disclosure of the least amount of information needed for a particular purpose;
8. The removal of a duty of a data processor or controller to inform data subjects of theft or unauthorised access of personal data where such data had been encrypted should be revised and removed. People should be told when their data has been hacked, even if the same is said to have been encrypted. They can then be on the look-out in

case such data is decrypted by the hackers or, if they so wish, make informed decisions whether they still wish to deal with organisations who have suffered data breaches. In addition, a duty to report data breaches, even when this was encrypted, will provide additional reason for data processors and controllers to take their legal duty to protect personal data seriously;

9. It is inconceivable how Section 51(2)(b) of the bill can be constitutional as it effectively repeals Art. 31(c)(d), CoK, 2010. Matters of national security and public order are adequately covered by 51(2)(c). It is instructive that there was an attempt to insert a similar provision in the draft CoK. The same constitutional bar may apply to the power given to the DPC under Sec. 54. Same had been sneaked into draft CoK, 2010;
10. It seems to me the penalties provided for in the bill for breaches are totally inadequate. Many of data processors and controllers who will be bound by the Act are international corporations whose business model is based on their exploitation of personal information – Facebook, UBER, Google, Amazon, Netflix, etc. For these organisations, a maximum fine of Ksh 5M will not have any effect whatsoever to act either as a deterrent or a punishment for failure to comply. The DPC should have the power to levy unlimited fines for administrative breach, or at the very least, up to a maximum of Ksh 20M. It is also not explicit the basis of the 2% fine on turn-over for breaching an undertaking applies to a company's global annual turnover or just for their operations in Kenya. It is imperative for Parliament to clarify this and close what seems to be a loophole and, just like the European Union's General Data Protection Regulations (GDPR), the 2% is based on the organisation's global turnover.

I would be most grateful if you could kindly confirm receipt of my submissions. Please further advise me regarding the progress of the bill through the legislative process.

Yours sincerely,

Karanja Matindi

16/07/2019

TEACHERS SERVICE COMMISSION

Telephone: Nairobi 2892000
Email: info@tsc.go.ke
Web: www.tsc.go.ke

When replying please quote
Ref. N^o:
CS/TSC/76/VOL.IV



TSC HOUSE
KILIMANJARO ROAD
UPPER HILL
PRIVATE BAG- 00100
NAIROBI, KENYA

23rd September, 2019.

Clerk of the National Assembly
Clerk's Chambers,
Parliament Buildings
P.O Box 41842-00100
NAIROBI

① Dloms
Please deal
24/09/19

THE NATIONAL ASSEMBLY
RECEIVED
24 SEP 2019
DIRECTOR COMMITTEE SERVICES

Att: Jeremiah W. Ndombi

CONSIDERATION OF THE MEMORANDA ON DATA PROTECTION BILL, 2019

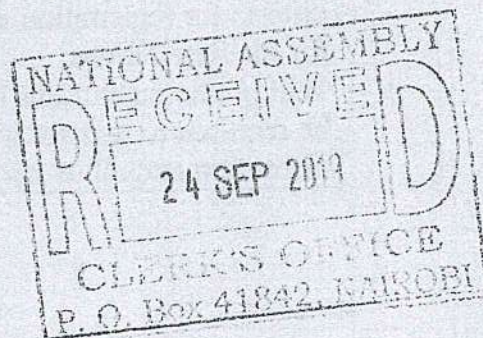
Reference is made to your letter dated 13th September, 2019 on the above matter.

Attached, herewith, please find a matrix of the Commission's views on the said Bill for your consideration.


DR NANCY NJERI MACHARIA, CBS
SECRETARY/CHIEF EXECUTIVE

② KINA
Please deal
FA
24/9/19

③ Chemwano
Please note
FA
24/9/19



GENERAL COMMENTS ON THE BILL

It is important for the Bill to address the following emerging gaps:

1. Forms of Data

There is need for a clear distinction to be drawn between the different forms and formats of personal data. For instance, the mechanism for protection of data may vary depending on the form and format thereof.

2. Data for Public use

The Bill is silent on the personal data generated for public use by virtue of the constitutional/statutory mandate donated to various public agencies. The questions that arise in this regard are two fold;

- a) Whether the data generated in this manner ought to be shared upon the request of another public body or ought to be obtained at a fee;
- b) The authorisations that may be necessary for accessibility to the data for public use.

3. The Bill is silent on the strategies to secure and safeguard both the data and its integrity.

4. Accessibility by external parties

The Bill appears to be silent on the personal data that may be generated or passed to external parties on account of contractual relation/assignment. For example, medical information of employees in an organization, information on learners in an educational institution, voters, etc.

COMMENTS TO SPECIFIC PROVISIONS OF THE BILL

S/No.	Section	Comment/proposal
1.	7	Include Information Science/Record Management as one of the significant key requirements
2.	8	There is need to clarify linkages and relationship between the office of the proposed Data Commissioner and public entities with constitutional or statutory mandate to generate public data e.g teacher registration and Registrar of Persons
3.	18 (2)	<ol style="list-style-type: none">i. It is good practice for the Act to provide for the primary criteria for registration while the secondary criteria may be left for the Regulations.ii. Will public institutions involved in personal data management be required to register with the Data Commissioner the institution and all its personnel involved in Data management.

		iii. If so will these supersede, in case of public institutions, their constitutional and statutory mandate to collect and manage personal data?
4.	24	Outline <u>specific</u> competencies/qualification to be considered for appointment as a Data Protection Officer
5.	26 (d), (e)	<p>i. The power granted by virtue of this provision needs to be regulated /clarified. the right to alter or vary personal data ought to be stringently regulated. Perhaps the need for such variation may be subjected to the jurisdiction of a court or quasi-judicial entity.</p> <p>ii. There exists Government directions that speak to the integrity and preservation of primary official data declared by a public employee/citizen, for instance date or place of birth</p>
6.	39 (1)	Management/retention/destruction of personal data records ought to be harmonized with existing regulatory frameworks.

		iii. If so will these supersede, in case of public institutions, their constitutional and statutory mandate to collect and manage personal data?
4.	24	Outline <u>specific</u> competencies/qualification to be considered for appointment as a Data Protection Officer
5.	26 (d), (e)	<p>i. The power granted by virtue of this provision needs to be regulated /clarified. the right to alter or vary personal data ought to be stringently regulated. Perhaps the need for such variation may be subjected to the jurisdiction of a court or quasi-judicial entity.</p> <p>ii. There exists Government directions that speak to the integrity and preservation of primary official data declared by a public employee/citizen, for instance date or place of birth</p>
6.	39 (1)	Management/retention/destruction of personal data records ought to be harmonized with existing regulatory frameworks.

① D/Coms
Please deal.
01/10/19



② KINHA
Please deal
FA
01/10/19



Comments on the Data Protection Bill, 2019

Presented to National Assembly, July 2019

September 2019



which involved meticulous details his directive to have uniforms based in Syongila, loaded and and the country," said Mr Kakawa.

REPUBLIC OF KENYA



THE NATIONAL ASSEMBLY TWELFTH PARLIAMENT - THIRD SESSION

in the matter of consideration by the National Assembly:-
The Data Protection Bill (National Assembly Bill No.44 of 2019)

NOTIFICATION FOR PUBLIC HEARINGS

Article 118(1)(b) of the Constitution provides that, "Parliament shall facilitate public participation and involvement in the legislative and other business of Parliament and its Committees". Further, the National Assembly Standing Order 127(3) requires the Departmental Committee to which a Bill is committed to facilitate public participation and take into account the views and recommendations of the public when the Committee makes its report to the House.

The Data Protection Bill, 2019 main objective is to give effect to the right to privacy as provided for in Article 31(c) and (d) of the Constitution by setting out the requirement for the protection of personal data processed by both public and private entities.

The Data Protection Bill, 2019 has undergone First Reading pursuant to Standing Order 127(3) and is now committed to the Departmental Committee on Communication, Information and Innovation for consideration and thereafter report to the House.

Pursuant to Article 118(1)(b) of the Constitution and the Standing Order 127(3) members of the public are hereby notified that the Committee will be conducting public hearings on the Data Protection Bill, 2019 in the following Counties:-

	COUNTY	VENUE/TOWNS	DATE
1.	Mombasa	Kenya School of Government Hall	Thursday, 15 th August, 2019
2.	Kilifi	Makio Kinamai Social Hall	Friday, 16 th August, 2019
4.	Kisumu	New Nyanza Regional Headquarters	Thursday, 22 nd August, 2019
5.	Kakamega	Salvation Army Social Hall	Friday, 23 rd August, 2019
6.	Kericho	Holy Trinity Academy Hall	Thursday, 29 th August, 2019
7.	Nakuru	Nakuru Old Town Hall	Friday, 30 th August, 2019
7.	Laikipia	Nanyuki Social Hall	Friday, 13 th September, 2019
8.	Isiolo	Silver Bells Hotel	Saturday, 14 th September, 2019
9.	Nairobi	County Hall, Parliament Buildings	Tuesday, 17 th September, 2019

The soft copy of the Bill is available on the website of the Parliament of Kenya www.parliament.go.ke.

MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY



MINISTER State Department of KASARANI TECHNICAL

P.O. BOX 51898-00200 NA
Email: kasaranitechnical@gmail.com

Kasarani Technical and Vocational College is a Public Institution located in Nairobi County, Kasarani Constituency, Kamulu Shopping Centre, from City Centre: at Bus Station, use bus No. 39, routes and courses listed below which are starting in September 2019.

COURSES COMMENCING		
DIPLOMA COURSES	Minimum Grade	Duration
Welding & Fabrication Module 1-3	KCSE C- or above	3 years
Information Comm. & Telecommunication Module 1-3	KCSE C- or above	3 years
Automotive Engineering Module 1-3	KCSE C- or above	3 years
Electrical Engineering (Power) Option Module 1-3	KCSE C- or above	3 years
Building & Construction Module 1-3	KCSE C- or above	3 years
Mechanical Engineering (Production) Module 1-3	KCSE C- or above	3 years
Social Work & Community Development Module 1-3	KCSE C- or above	3 years
Information Science Module 1-3	KCSE C- or above	3 years
Business Management Module 1-3	KCSE C- or above	3 years
Supply Chain Management Module 1-3	KCSE C- or above	3 years
Human Resource Management Module 1-3	KCSE C- or above	3 years
Project Management Module 1-3	KCSE C- or above	3 years

Download an application form from www.kasaranitechnical.com application fee of 500 Kenya Shillings. Any student who is to register. The application for HELB loan is ongoing until 30th September.

All applications to be addressed to: The Principal, Kasarani TVC.

About us

This submission is made by the National Coalition of Human Rights Defenders – Kenya (NCHRD-K), the Centre for Intellectual Property and Information Technology (CIPIT), KELIN and Privacy International (PI).

The Centre for Intellectual Property and Information Technology (CIPIT) an evidence-based research and training think tank based at Strathmore University Law School, Nairobi, Kenya. Our Mission is to study, create, and share knowledge on the development of intellectual property and information technology, especially as they contribute to African Law and Human Rights. We take pride in furthering non-partisan research that is independent and objective. CIPIT has in the past been instrumental in helping to highlight some of the limitations facing data protection in Kenya most recent of which includes a study on the privacy implications of adopting biometrics in the 2017 Kenyan elections. The report was discussed in one of the events of the 62nd session of the African Charter for Human and Peoples Rights to inform the inclusion of the right to privacy to that Banjul Charter. In partnership with other stakeholders, CIPIT has also organized local forums and workshops to identify and debate the pertinent issues on the current legislative proposals.

The National Coalition of Human Rights Defenders-Kenya (NCHRD-K) is a national organization established in 2007 and incorporated in the Republic of Kenya as a Trust in 2012 whose mission is to strengthen the capacity of Human Rights Defenders (HRDs) to work effectively in the country and to reduce their vulnerability to the risk of persecution. The NCHRD-K has a track record in advocating for a favourable legal and policy environment in Kenya, conducting preventive security management trainings and offering support to HRDs at risk through legal, medical and psychosocial support.

KELIN is an independent Kenyan civil society organization working to protect and promote health related human rights in Kenya. We do this by; Advocating for integration of human rights principles in laws, policies and administrative frameworks; facilitating access to justice in respect to violations of health-related rights; training professionals and communities on rights based approaches and initiating and participating in strategic partnerships to realize the right to health nationally, regionally and globally.

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Working internationally through an International Network of partners, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

To find out more about privacy and data protection in Kenya, please refer to '[The State of Privacy in Kenya](#)' (last updated in February 2019).

Contacts

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.org

Dr. Isaac Rutenberg

Dr. Robert Muthuri

Director, CIPIT
irutenberg@strathmore.edu

Senior Research Fellow – IT, CIPIT
rmuthuri@strathmore.edu

Kamau Ngugi
Executive Director, NCHRD-K
dkngugi@hrdcoalition.org

Allan Maleche
Executive Director, KELIN
Amaleche@kelinkenya.org

Overview

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 120 countries worldwide including 25 African countries,¹ and instruments have been introduced by international and regional institutions such as the African Union,² the OECD,³ Council of Europe,⁴ and ECOWAS.⁵

We welcome the effort by the Government of Kenya to give life to and specify the right to privacy, already enshrined in Article 31(c) and (d) of the Constitution of Kenya by proposing a draft Data Protection Act. We particularly appreciate the direct reference to this Constitutional right in the purpose of the Act and the way it is referred to on several occasions in this proposed Bill.

Development of an effective and comprehensive Data Protection law in Kenya is a priority. In particular, given that a number of strategies are currently being deployed in Kenya to promote digital inclusion including: digital identities, micro-lending and Alternative Credit Scoring. While these efforts have positive intentions, a number of concerns ought to be addressed and a strong data protection framework would be a step in the right direction, for example:

- a) Firms should deploy secure infrastructures to avoid data breaches, like those currently being seen with the Aadhaar system in India.
- b) Biometrics are used excessively in certain circumstances where less intrusive options such as unique identifiers would be sufficient without the concomitant risk. This is particularly true in the health sector where biometrics could expose certain at-risk populations.
- c) Alternative Credit Scoring by Micro-Lending institutions use a vast range of data points such as call detail records (CDR) and customer relationship management (CRM) details. These firms are often acting without clear opt-in mechanisms or sufficient information being provided to individuals.

However, the Data Protection Bill proposed by the Taskforce has a number of significant shortcomings. We recommend that to effectively protect privacy and to meet international standards in protecting personal data, that full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill, and include:

- Reviewing the definition of 'sensitive personal data' to ensure a comprehensive definition.

¹ See Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 Privacy Laws & Business International Report*, 10-13, UNSW Law Research Paper No. 45 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

² See the African Union Convention on Cyber security and Data Protection, 2014, available at <http://pages.au.int/infosoc/cybersecurity>

³ See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>

⁴ See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at <http://conventions.coe.int/Treaty/en/Treaties/html/108.htm>

⁵ See the Supplementary Act on personal data protection within ECOWAS, February 2010, at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf

- Replacing the current proposal to establish the office of the data commissioner as a body corporate with its establishment as a Constitutional Commission under Chapter 15 of the Constitution.
- Guaranteeing that all data protection principles are included and revised clearly to provide for principles of integrity and confidentiality and accountability.
- Guaranteeing that data subjects are consolidated in the law in a clear manner under the same section, and the right to effective remedy, and the right to compensation and liability which are currently missing must be added to the list of rights of data subjects.
- Reviewing the current scope of the obligation to inform a data subject about the processing of their personal data.
- Providing clarity as to what the legal grounds for processing may be including by defining concepts such as 'public interest' and 'legitimate interest', and in particular review the legal grounds for processing 'sensitive personal data' to strengthen the protection of such data.
- Ensuring that any exemptions relating to the different data protection principles and the rights of data subjects must be provided for in the law in a form which is clear, precise and limited to specific necessary and proportionate exceptions rather than broad blanket exemptions, particularly for government authorities.
- Reviewing the grounds for processing including ensuring that data processing of data which is available to the public or deemed publicly available is not free for all to use without requiring further involvement of the data subject.
- Reviewing the clause on the storage of data in Kenya and recommending that focus should be on ensuring the data is protected with the highest safeguards rather than demanding data localisation which may not achieve the purpose of providing a higher level of protection as intended.
- Guaranteeing that a strong process is in place to regulate the transfer of personal data including developing a process for assessing adequacy of protection in the receiving country, and not only in terms of data protection but protection of human rights and rule of law.
- Ensuring that the protection of the data subject and their data as well as their right of privacy is balanced with freedom of expression under Article 33 of the Constitution for the media, artistic or literary work.

Part I – Preliminary

Definitions (section 2)

The most fundamental and recurrent terms in the law must be clearly defined at the outset. In particular we would like to outline the following comments with regards to the definitions provided for in the Bill.

‘Sensitive personal data’

There are a couple of omissions from this definition including membership of a trade union, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings. These should be included. Furthermore, clarity should be provided that by ‘belief’; the law includes religious or philosophical beliefs or other beliefs of a similar nature.

Object and purpose (section 3)

Echoing concerns, we further flag down in this submission Section 3 (b) which fails to incorporate all of the internationally recognised data protection principles within this section of the Bill, including:

- Fairness and transparency
- Storage limitation
- Accountability

Application (section 4)

The scope of the Act as set out in section 4(b) provides limited protection for the personal data of people in Kenya as a controller or processor established in Kenya can easily remove its processing from the scope of the Act by conducting the processing outside Kenya.

PART II – ESTABLISHMENT OF THE OFFICE OF DATA PROTECTION COMMISSIONER

Establishment of the Office and Appointment (section 5 & 6)

The establishment of the office of the data commissioner as a body corporate does not grant this office with the necessary institutional and financial independence to execute its mandate effectively under the new law. We continue to call for the establishment of a Constitutional Commission under Chapter 15 of the Constitution.

Powers of the Data Commissioner (section 9)

Whilst we welcome the range of powers given to the Office of the Data Protection Commissioner we would suggest clarifying that the process of sanction should also apply to complaints investigated by the independent data protection authority on its own initiative as it empowered to do so under Section 9(1)(a).

PART III – REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Application of Registration (section 19)

We welcome the additional details provided around the process for registration of data controllers and processors but the following provisions require clarification to strengthen the right to information and the right to access provided for under section 26:

- Section 19 (2) (a): It is not sufficient to merely provide a "description" of the personal data to be processed. It should be clearly state what personal data will be processed.
- Section 19 (2) (b): It is not sufficient to merely provide a "description" of the purpose of processing. In accordance with the principle of purpose limitation, the purposes for which personal data are collected should be specified,
- Section 19(5): It is not clear what the "prescribed period" is. This must be clarified.

Compliance and audit (section 23)

It is unclear what the criteria would be for the Data Commissioner to decide to carry out an audit of the systems of a data controller or data processor. We would like to request further clarity on the decision-making process behind this section including who would be undertaking the audit. It is important that the audit be independent and effective.

Designation of the Data Protection Officer (section 24)

The use of the term 'may' in Section 24 (1) makes it unclear when the obligation to designate a data protection officer applies – it means that it appears optional as opposed to mandatory. We propose a tiered system through subsequent regulations to delineate firms that will be required to employ/contract a data protection officer.

What constitutes "*regular and systematic monitoring of data subjects on a large scale*" as noted in Section 24(1)(b). Further clarity should be provided on this term, so data controller and data processors know when they are obliged to designate a DPO.

This provision should be strengthened by including further details on the mandate and functions for the DPO including that they be involved in a timely manner in issues related to data protection, that they have the necessary resources to carry out their tasks, that they are sufficiently independent and will not be dismissed or penalised for carrying out their tasks, and that they report to management (i.e. Board).

PART IV–PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

Principles of data protection (section 25)

Section 25 should be strengthened by providing clear and coherent principles. In particular, this section would be strengthened if it included the following principles:

- **Integrity and Confidentiality:** This principle is provided for in Section 41 and 42 but it must also be listed here in section 22 for consistency.
- **Accountability:** The Bill should also include a principle of accountability. An entity which processes personal data, in their capacity as data controllers or processors, should be accountable for complying with standards, and taking measure which give effect to the provisions provided for in a data protection law. Those with responsibility for data processing must be able to demonstrate *how* they comply with data protection legislation, including the principles, their obligations, and the rights of individuals.

Section 25(g) must reviewed to ensure that consent is not the sole legal basis for sharing personal data with a third party. And Section 25 (h) needs to be reviewed to ensure that the transfer of data outside of Kenya is not processed unless there are adequate data protection safeguards and there is consent from the data subject. Consent should not be the sole condition for transferring data outside of Kenya.

Rights of a data subject (section 26)

A central component of any data protection law is the provision of the rights of *data subjects*. These rights should appear early in the law, as they should be seen as applying throughout, underpinning all provisions in the law. These rights impose positive obligations on data controllers and should be enforceable before an independent data protection authority and courts.

We welcome the inclusion of the current rights under section 26. However, there are several rights missing for the current Bill including, which we would urge be included:

The right to an effective remedy: The law must include the right of an individual to an effective remedy against a data controller and/or data processor, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law. A data subject must have the right to submit a complaint to the independent supervisory authority. This reaffirms the need for the independent supervisory authority to have the power to receive complaints from data subjects, investigate them, and sanction the violator within their own scope of powers - or refer the case to a court. The law should also provide for the data subject to take action against a supervisory authority where they have failed to deal with their complaint. As well as the right to complain to a supervisory authority, individuals should also have access to an effective judicial remedy via the courts. Individuals should be empowered to take action themselves, as well as instructing others (including NGOs) to take action on their behalf.

Right to compensation and liability: A person whose rights are found to have been violated should have a right to compensation for the damage suffered – material or non-material (e.g. distress). This underlines the need for robust enforcement models to be in place to ensure that any violation can be investigated and acted upon by a relevant authority, in this case the Office of the Data Protection Commissioner.

Furthermore, whilst there are provided elsewhere in the law, the following rights must also be listed under section 26:

- **The right to suppress or block:** Whilst this right is provided for in Section 36, it must also be listed in Section 26.
- **The right to data portability:** Whilst the right to data portability is provided for in Section 38, it must also be listed in Section 26.
- **The rights in relation to profiling and automated decision-making:** Whilst the right to not be subject to automated decision making is provided for in Section 35 and includes right not to be subject to profiling, these should also be listed in Section 26, ideally as separate rights.

Collection of personal data (section 28)

The principle behind Section 28(1) is in the right place (despite the fact that this often doesn't happen in practice), however, it is undermined by the number of situations where it can be disapplied which are outlined in Section 28(2). In particular we are concerned with the following parts of this section:

- Section 28 (a): Just because data is a matter of public record does not mean that it is available for further processing, and its 'public' availability should not be construed as consent nor as another legal basis for further processing.
- Section 28 (b): Acknowledging the complexity of the data generation and processing ecosystem, a data subject "deliberately" making data public is not a sufficient justification for indirectly processing the data without involving the data subject.
- Section 28 (c): If consenting to collection from another source, they must have been informed that there will be further processing and by who.
- Section 28 (e): The requirement that the collection "would not prejudice the interests of the data subject" is overly broad and could give rise to abuse.
- Section 28 (f) (iii): This provision is overly broad, in terms of what the protection of interests of another person are. It raises questions as to the intended purpose is: is it to be the vital interests of a natural person, or the commercial interests of a company or the political interests of a political party. The current wording is open to abuse.

These amendments are necessary in order to ensure that the right to information provided for under section 26 (a) is upheld effectively.

Furthermore, this section should be bolstered by a section that requires firms to conduct a Data Protection Impact Assessment to show that they understand the risks and effects of collecting, maintaining and disseminating personal data. It will also help to outline the appropriate policies to mitigate such risks. Such an assessment will also gauge whether the controller/processor complies with the legal and regulatory framework established under the bill.

Duty to notify (section 26)

The right of individuals to know what personal data that controllers hold on them is a fundamental component to data protection law.

The UN Human Rights Committee, in interpreting the scope of obligations of states parties to the International Covenant on Civil and Political Rights, noted, back in 1989, that:

"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination." (Human Rights Committee, General Comment No 16 on Article 17 of ICCPR.)

More recently in its 2018 annual report on "The right to privacy in the digital age", the Office High Commissioner for Human Rights noted that "The individuals whose personal data are being

processed should be informed about the data processing, its circumstances, character and scope, including through transparent data privacy policies.” (A/HRC/39/29, para 29)

The qualification of “reasonably practicable” in section 29 (1) is open to abuse. A specific time period should be provided.

The information to be provided in section 29(1) should additionally include:

- a description of the personal data;
- the legal basis for the processing
- the third-parties to whom the personal data has been or will be transferred, including details of safeguards adopted;
- the envisaged time limits for deletion of the different categories of data;
- a description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data.

Lawful processing of personal data (Section 30)

We would like to seek clarity as to what constitutes “public interest” in Section 30 (1) (iv) and (vi). The lack of definition, and clarity around what constitutes ‘public interest’ and its often-broad interpretation, raises concern that it can act as a loophole. A public interest ground should be clearly defined to avoid abuse. For example, it should be possible to list the specific public interest grounds and ensure that such a list is clear and exhaustive.

Section 30 (1)(vii) is overly broad, in terms of what “the legitimate interests pursued by the data controller or data processor by a third party”. It raises questions as to the intended purpose of this provision. The current wording is open to abuse. If this provision is included and there is any doubt in the balancing exercise that there is prejudice to the individual, then the presumption should be that the processing should not go ahead. This provision should not apply public authorities.

In order to avoid any abuse and wide interpretation of Section 30 (1)(viii), the following must be considered:

- There is a need for clarity on what the statistical and scientific purposes are. Further detail should be included within the law and/or guidance be developed to define this further.
- Such a ground must not exempt a data controller or processor from all of their obligations, and they should provide for appropriate safeguards for the processing of personal data for these purposes.
- Safeguards could include ensuring that the data will not be used to take decisions about the individuals and that the processing is prohibited if it would cause harm.
- A data subject should still have rights over their data including the right to be informed and the right to object that their data be processed for these purposes.

Data Protection Impact Assessment (Section 31)

We welcome the inclusion of this obligation for data controller and processor to undertake a data protection impact assessment. However, we believe the conditionality of the obligation as per Section 31 (1) to only comply when processing is likely to result “in a high risk” to the rights and freedoms of data subject is too high. Whilst it particularly important to do them in such instance, we recommend that conducting an assessment should be an obligation prior to any processing activities.

Furthermore, this duty should be strengthened by specifying the means/form in which this right should be implemented. Consideration should be given to including requirements as to the form in which this information/ notice is provided i.e. it should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Consideration must be given to ensure that those who are illiterate are not excluded from being informed, and alternative measures should be taken to communicate with them in a way that ensures they are adequately informed.

Conditions for consent (Section 32)

We welcome the addition of conditions for Consent. These are an important start in making consent meaningful in practice. However, it is still an issue which will require further consideration in terms of implementation and in particular guidance on the situations where consent is appropriate.

Processing of personal data relating to a child (Section 33)

This section must clarify what constitutes a child for the purposes of this law, i.e. how old is a child? This section should be reconciled with the protection provided for in the Children Act which upholds the right to privacy under Article 19.

*We question the use of the term "guardian" in Section 33 (1)(a) and the role of the Commissioner is appointing them. This leads to unnecessary conclusion.

Clarity is sought as to what constitutes "appropriate mechanisms for age verification" referred to in Section 33 (2) as well as "appropriate mechanisms for parental consent".

Safeguards should be provided against children's data being used for research or statistical purposes, and as noted elsewhere, the mere public availability of a child's data does not mean that it should be available for processing.

Automated individual decision making (section 35)

We welcome the inclusion of the right of a data subject not to be subject to automated decision making. However, it is important to distinguish between automated decision-making and profiling. The Bill should provide for effective protections and rights in relation to both. They do not need to be dealt with together (indeed this can lead to unnecessary confusion) but it is important that in relation to both there are requirements as to transparency, so that individuals are aware of the existence of these forms of processing.

For profiling, it is important that individuals are aware when profiling will reveal sensitive personal data and that there are safeguards in place. Individuals' rights should also apply to the data that is inferred, predicted and derived as a result of profiling.

In addition to treating profiling separately from automated decision making, Section 35 should be strengthened by including the following obligations and key considerations:

- A data controllers and processors who profile to be transparent about it and individuals must be informed about its existence from the onset and not "as soon as reasonably practicable" as per Section 35 (3)(a).
- Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their rights, including to access, rectification and deletion.

- This right need to be applied to derived, inferred and predicted data, to the extent that they qualify as personal data.
- This bill should impose restrictions and safeguards on the ways in which data can be used to profile and make decisions.

The exemptions provided for in Section 35(2) must be limited, as well as and clearly and narrowly defined. Even where exemptions allow for automated-decision making, an individual should have the right to obtain human intervention, express their point of view and challenge the decision.

Objecting to processing (Section 36)

This section alludes to the obligation of the data controller or data processor to demonstrate compelling legitimate grounds to overrule right to object of a data subject. However, we would like to stress once again that that the onus must be on the data controller or data processor to provide evidence for the need to continue processing the data of that individual, with reasons which override the interests, rights, and freedoms of that individual. Clarity must be provided on what "compelling legitimate grounds" are.

Limitation to retention of personal data (Section 39)

Exemptions for these purposes outlined in section 39 (1) should only be applied when strictly necessary and proportionate, and not been seen as a blanket exemption. The activities subject an exemption need to be clearly defined, for example, is research limited to academic research or does it include commercial research? There should be sufficient safeguards in place to protect the rights of data subjects.

Clarity must be provided for in terms of the applicability of the Data Protection Act in relations to other laws which imposed data retention policies such as the Kenya Information and Communications Act (2009) which regulates the retention of electronic records and of "information in original form", and the Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations (2015).

Data protection standards should be applied as far as possible and detailed consideration should be given to any limitation on the rights of data subjects and the relevant data controllers should consider and mitigate any prejudice to the rights and freedoms of the data subjects. This is particular crucial when retaining data about key populations who may be exposed to risks should their data be unlawful processed and so measures should be taken to minimise the retention of their data, along with other security measures, to mitigate the possible risk of a breach. A data subject should be given the right to object that their data be processed for these purposes.

Furthermore, whilst rarely noted within this provision as an exemption, we would suggest that this exemption apply under certain conditions to research carried out by independent non-governmental, non-for-profit organisations.

In relation to section 39(2) it is important to note that pseudonymised data is still personal data and therefore still subject to the protections of the law and not processed in this form longer than necessary.

Right to rectification and erasure (Section 40)

This section lacks clarity as to the factors to be considered when deciding on a data subject's request to delete information.

It is important that provision is made to ensure among other safeguards, that when processing the request for deletion, the data controller considers the public interest of the data remaining available. It is essential that any such right clearly provides safeguards and in particular exemptions for freedom of expression and freedom of information. The construction of this right and how it will play out in the national context must be considered very carefully to ensure that it is not open to abuse.

Notification of breach of security on personal data (Section 43)

Breach notifications are essential to a data protection law and to ensure transparency on part of the data controller. However, the threshold to only notify when there is "real risk of harm to the data subject" is vague and no criteria of risk and likelihood is laid down in the section. The vagueness can constitute a loopholes for data controllers who hide behind subjective determinations of risk.

Clarity is needed on section 43(3) and what this justification for delaying notification means.

It is imperative that for a breach notification to be meaningful for data subjects, the notification should be in clear and plain language and includes advice and the tools to take measures to protect from harm and to seek redress from harm suffered. Consideration must be given to ensure that those who are illiterate are not excluded and that the data controller takes necessary measures to ensure they are informed.

We are concerned by the exemption provided for in Section 43(6) which provides that the obligation to notify does not apply if the data affected was encrypted. There is no guarantee that even if it was encrypted that the data won't be accessible to the person who unlawful obtained the data at that point in time or at a later stage should they acquire the means to decrypt the data.

PART V – GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

Processing of personal sensitive data (Section 44)

In relations to section 44(1) consideration must be given the concerns presented in this submission with regards to the shortcomings of section 30 'Lawful processing of personal data'.

Permitted grounds for processing of personal sensitive data (Section 45)

It should be clear that one of these grounds must be satisfied in addition to a ground under section 30.

We reject the ground for processing sensitive personal data provided for in section 45(1)(b). Noting the complexity of the data generation and processing ecosystem, a data subject "manifestly" making data public is not a sufficient justification for indirectly processing the data without involving the data subject, particularly when it comes to sensitive personal data.

We challenge the ground for processing sensitive personal data provided for in section 45(1)(c)(ii) which refers to "rights of the controller". A data controller does not have rights, in the same way a data subject has rights and if it is legal obligations that are being referred to this should be clear.

In processing sensitive personal data, at minimum the following protections should be included:

- a prohibition on processing sensitive (or special category) personal data unless a specific narrow exemption applies;
- limits on the use of sensitive personal data for automated-decision-making;
- safeguards for international transfers; and record-keeping and data protection impact assessment obligations.

The sensitivity of the data should also be considered in enforcement and redress mechanisms. If these protections can be strengthened through sectoral regulation (for example in the financial or health sector) then this is to be encouraged.

Further categories of sensitive personal data (section 47)

The threshold of risk provided for in Section 47(2)(a) and (c) is too high and must be revised to ensure the best interests and protection of the data subjects.

PART VI – TRANSFER OF PERSONAL DATA OUTSIDE KENYA

Conditions for transfer out of Kenya (section 48)

Clarity should be provided as to what is meant by 'proof' and 'appropriate safeguards' in section 48(1)(a) and how this oversight and authorisation will work in practice.

As noted above, clarity should be provided on what is considered a matter of 'public interest' in section 48(1)(c)(iii), otherwise this provision is left open for abuse.

The provision under Section 48 (c)(v) is overly broad, in terms of what the protection of "vital interests" of another person are. It raises questions as to the intended purpose is: is it to be the vital interests of a natural person, or the commercial interests of a company or the political interests of a political party. The current wording is open to abuse.

Consideration should be given to the removal of section 48(c)(vi), 'compelling legitimate interest' is not a defined term and is open to abuse. The provision does not provide enough safeguards for individuals.

Processing through a data server or data centre in Kenya (Section 50)

We are concerned by the obligation under section 50 regarding the storage of data on a server or in a data centre located in Kenya. This sort of measures, often referred to as data localisation, does not per se protect the safety of personal data. If other jurisdictions offer an adequate level of protection, there is no justification based on safety of personal data for preventing their transfer or imposing the storage of the personal data in a particular country. Further, we note that in other jurisdictions the imposition of data localisation has been introduced as a way to facilitate unlawful surveillance and limiting the capacity of individuals to protect the confidentiality of their communications.

Firstly, we are concerned by the discretion awarded to the Cabinet Secretary under section 50). Secondly, "strategic interests of the state or on protection of revenue" is too vague and must be clearly defined and limited. Thirdly, it is unclear what "critical personal data" means/ This term is not defined elsewhere in the bill. Clarity needs to be provided on what this term means.

The prohibition of cross border processing of sensitive personal data will also be extremely complex in practice and limit access to services and systems for people in Kenya. The Bill should instead focus on building in safeguards.

VII – EXEMPTIONS

General exemptions (section 51)

The exemptions provided for in section 51 (2) are too broad and must be revised – in particular terms such as “national security” and “public order” which are not defined. Blanket exemptions are never justifiable. In the limited cases where an exemption is justifiable, it should only apply in limited circumstance. It is essential to ensure that any exemptions are:

- 1) clearly defined and prescribed by law;
- 2) respect individual’s fundamental rights and freedoms,
- 3) are necessary and proportionate measures in a democratic society, and
- 4) are only applicable, where failure to do so prejudice the legitimate aim pursued.

Research, history and statistics (section 53)

In order to avoid abuse and wide interpretation of this exemption:

- There is a need for clarity on what the research, history and statistical purposes are. Further detail should be included within the law and/or guidance be developed to define this further.
- Such a ground must not exempt a data controller or processor from all of their obligations, and they should provide for appropriate safeguards for the processing of personal data for these purposes.
- Safeguards could include ensuring that the data will not be used to take decisions about the individuals and that the processing is prohibited if it would cause harm.
- A data subject should still have rights over their data including the right to be informed and the right to object that their data be processed for these purposes.

PART VIII – ENFORCEMENT PROVISIONS

Complaints to the Data Commissioner (section 56)

We are concerned that section (56)(b) fails to provide further details on what avenues would be open to a data subject should the Data Commissioner be “unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned”.

As noted above, whilst we welcome the range of powers given to the Office of the Data Protection Commissioner we note that the failure of the Act to provide the Office with the power to impose appropriate civil penalties, including fines, enforcement notices and undertakings. This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority.

Furthermore, the law should also include provisions for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective

complaints would ensure corrective action by organisations processing personal information, which would benefit all those affected. Provision should therefore be made in the process to allow individuals to be represented by qualified representatives and for certain qualified bodies, such as non-profit groups working in the field of data protection, to make complaints and seek remedies.

Administrative Fines (section 63)

We welcome that inclusion of fines if there is an infringement of a provision of this Act. However, we would advocate for the Bill to provide for a wider variety of sanctions beyond administrative sanctions in case of non-compliance or breach of the Bill. The types of sanctions/ penalties to consider including are:

- Criminal offences (individual responsibility) for certain actions, for example knowingly or recklessly, without the consent of the data controller, obtaining or disclosing personal data.
- Direct liability for directors of companies.

Part X – PROVISIONS ON DELEGATED POWERS

Regulations (section 71)

The delegated powers afforded to the Cabinet Secretary under this section are too wide. In particular section 71(2)(l) which allows them to make regulations in any other matter as they see fit. As much as possible the provision should be made on the face of the Bill and subject to effective Parliamentary scrutiny.

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

Prepared by;

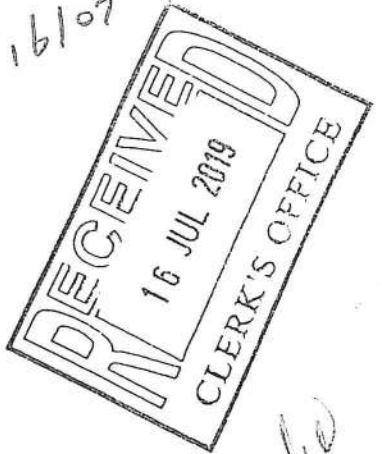
Content Development & Intellectual Property (CODE-IP) Trust
Box 75474-00200 City Square,
Nairobi

Submitted to:

The Departmental Committee on Communication Information and Innovation,
The National Assembly, Twelve Parliament of Kenya,
Nairobi

16 July, 2019

1. 01-07/005
16/07



2. Etta Kencho
For Consideration by
the Committee
17/7/19

REPUBLIC OF KENYA



**THE NATIONAL ASSEMBLY
TWELFTH PARLIAMENT - THIRD SESSION**

In the matters for consideration by the National Assembly:-
1. The Crops (Amendment) Bill (National Assembly Bill No. 25 of 2019)
2. The Data Protection Bill (National Assembly Bill No. 44 of 2019)

SUBMISSION OF MEMORANDA

Article 18(1)(b) of the Constitution provides that: "Parliament shall facilitate public participation and involvement in the legislative and other business of Parliament and its Committees". The National Assembly Standing Order 127(3) provides that: "The Departmental Committee to which a Bill is committed shall facilitate public participation and take into account the views and recommendations of the public when the Committee makes its report to the House".

The Crops (Amendment) Bill, 2019 seeks to amend the Crops Act, 2013 to include Achote as one of the scheduled crops. Achote crop is locally known as 'Mwangi' because of its bright red fruits and is grown largely at the coast but its potential has not been fully utilized. According to the Agricultural experts, the crop matures fully within four to five years and has an economic life span of 20 years but can be harvested even after one year in the farm. The crop is world's second most important natural colourant and makes about 70 percent of the world's natural dyes.

The Data Protection Bill, 2019 seeks to give effect to the right to privacy as provided for in Article 31(c) and (d) of the Constitution by setting out the requirement for the protection of personal data processed by both public and private entities.

The above mentioned Bills have undergone First Reading pursuant to Standing Order 127(3) and stand committed to the Departmental Committee on Agriculture & Livestock and Departmental Committee on Communication, Information & Innovation respectively, for consideration and thereafter report to the House.

Pursuant to the provisions of Article 18(1)(b) of the Constitution and Standing Order 127(3), the respective Committees invite members of the Public to submit representations they may have on the said Bills. The representations may be forwarded to the Clerk of the National Assembly, P.O. Box 41862-00100, Nairobi; hand-delivered to the Office of the Clerk, Main Parliament Buildings, Nairobi; or emailed to clerk@parliament.go.ke to be received on or before Tuesday, 16th July, 2019 at 5.00 pm.

MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

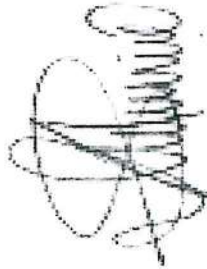
Reference is made to above Notice inviting members of the public to submit representations on the Data Protection Bill, 2019. We thank the Departmental Committee on Communication Information and Innovation for inviting privacy and data protection Technology Rights Defenders to provide input. We appreciate being consulted on the current law before the House.

Article 31 (c) and (d) of the Constitution requires the unwarranted intrusion into privacy with minimal requirement for information relating to family or private affairs unnecessarily or its disclosure which this Bill sets out to effect. Generally, it is our considered view that this Sections 8-10 establish Data Protection Commissioners to whom largely confers the constitutional mandate. The Commissioner is thereafter legally empowered to singly and independently define the rules and application of this Act. This may later be problematic on Delegated Legislation disputes. Further, applying the old test of fullest application of the law against oneself – if owned a small online enterprise collecting personal data raises deep concerns.

Therefore, whereas envisaged to be a person of high integrity and well-intended, and if permitted – analogous to establishing a ‘Morality Commissioner’ – guaranteeing unpredictable enforcement consequences. Besides plausible arbitrariness, the additional bureaucratic registration, certification, license fees requirements, and fines hamper ease of doing business in Kenya when “Ease of Doing Business” is a stated government commitment.

Hereby submit our Memorandum of Views for your consideration and pray that it deserves your due attention and consideration.

Respectfully submitted,



Alex Gakuru
Executive Director,
CODE-IP Trust

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

Section	Title	Proposal	Justification
Part I – Preliminary			
2	Interpretation	<p>Add definition of “data” at the beginning as:- “data” means the factual input processed into information by means of equipment operating automatically in response to instructions given for that purpose, recorded with the intention that it should be processed by means of such equipment, or is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. It need not be held on a computer.</p>	<p>Fundamental definition to guide subsequent interpretations and to expand the scope of data protection to include data on manual records as well as in digital systems, processing and control.</p>
2	Interpretation	<p>Add definition of “metadata” at the beginning as:- “metadata” means data about data and for the purposes of this Act qualifies as data wherever consolidated metadata reveals private data or personally identifiable information</p>	<p>Cure indiscriminate metadata collection, retention, processing and disclosure to third parties See video ‘Metadata Explained Privacy International’ https://www.youtube.com/watch?v=xP_e56DsynA</p>
2	Interpretation	<p>Add definition of “Data Collector” after “Data Commissioner as:- “Data Collector” means a natural or legal person, public authority, agency or other body which alone or jointly with others, collects public data.</p>	<ol style="list-style-type: none"> 1. To expand the scope of privacy protection to include foreign entities collecting private data of Kenyans for inclusion in alien data systems. 2. This category of data handlers is otherwise exempted from provisions of this Bill. 3. Effect Article 31(c) information relating to their family

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

			or private affairs unnecessarily required or revealed;
2	Interpretation	Add definition of "Data Owner" after "Data Subject" as :- "Data Owner" means the same as "Data Subject"	Balancing out normative contextual interpretations over private data 'owner' vs. private data 'subject'
2	Interpretation	Change definition of "profiling" to read as;- "Profiling" means any form of automated processing of personal data consisting of the use of personal data evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects, such as, concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth, personal preferences, interests, behaviour, location of movement, family or private affairs, among others;"	Effect Article 31(c) 'information relating to their family or private affairs unnecessarily required or revealed;'
3(b)	Object and Purpose of this ACT	Consider adding the purpose;- "(e) to establish a framework to protect against the unnecessary collection of information relating to their family or private affairs"	1. Whereas ".....minimisation of collection...." is a stated purpose, nowhere on the Act is the unnecessarily collected personal data given force of law and complies with Sections 25 (c) and (d). 2. Effect Article 31(c) 'information relating to their family or private affairs unnecessarily required or revealed;'
4 (b)	Application	Change to read;- "(b) by a data collector, data controller or data processor who –	To expand the scope of privacy protection to include foreign entities collecting private data of Kenyans for inclusion in alien data systems.

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

		<p>(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or</p> <p>(ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects in Kenya.</p>	
<p align="center">Part III – Registration of Data Controllers and Data Processors</p>			
<p>Part III - sections 18-24</p>	<p>Registration with DPO</p>	<p>Delete requirement for data processors and controllers to register with the Data Protection Office</p>	<p>The proposed legislation requires registration of data processors and controllers in Kenya with the Data Protection Officer including the requirement to document and keep up to date a record of processing activities. The bill contemplates the potential requirement of fees for processors to register with the state and penalties for failure to register.</p> <p>Data Processing and Data Controlling are not business models in the strict sense. They are activities that entities may incidentally engage in during the course of business.</p> <p>The requirement to have all processors and controllers would create an immense implementation burden for the Data Protection Office that would threaten to bog down the office with bureaucratic recordkeeping rather than allowing them to focus on the most serious enforcement issues.</p> <p>Similarly, for processors and controllers, the requirement to update external records of processing each time a change to</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

		<p>processing occurs shifts the focus from improving privacy in areas that present the most risk to a bureaucratic exercise. The requirement for fees also raises issues as this would disproportionately affect smaller data processors and controllers.</p> <p>Even the GDPR does not contain any parallel requirement for registration</p>
Section 25	Principles of Data Protection	<p>Article 31(c) information relating to their family or private affairs unnecessarily required or revealed;</p>
Section 33	Processing of Personal Data relating to a child	<p>This will prevent overzealous law enforcement officers labeling children criminals for life (see Annex I -DCI <i>Criminal Child Data Archiving Notice</i>).</p> <p>And also criminalise archived profiles of child's youthful indiscretions.</p>
Section 43	Notification of data Breach	<p>The proposed legislation requires notification to the Data Protection Officer for all instances of breach and not just those that are likely to have an impact on the rights of the data subject.</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

			<p>As currently drafted could have risk of inundating Data Protection Office with notices for risks that are trivial in terms of impact on rights of individuals. A more efficient and effective means to enforcement would come from narrowing notification to those breaches likely to have an impact on individual rights and freedoms</p>
<p>Sections 48-50</p>	<p>Cross-Border Transfer of Data</p>	<p>Permit transfers to third country where, accounting for the transfer, all of the other requirements set forth in the legislation will continue to be met.</p> <p>Clarify that the conditions listed in part VI are mutually exclusive. Do this by using the term "...may transfer personal data to another country where any of the following conditions is fulfilled" or separate the conditions with the term 'or'.</p>	<p>The proposed legislation bars transfer of data to a third country where there is no decision by the Data Commissioner that adequate safeguards have been made for the protection of that data (adequacy decision).</p> <p>The omission of the word 'or' at the end of the conditions listed in this part gives the interpretation that all of those conditions listed have to be met before data can be transferred across borders. IT appears that this may not have been the intention and that all the conditions listed are mutually exclusive.</p> <p>Requirement for adequacy decision will have undesirable impact on restricting free-flow of data. Concerns may be addressed through alternatives like binding corporate rules, codes of conduct, and certifications.</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

Annex I DCI Criminal Child Data Archiving Notice

DIRECTORATE OF CRIMINAL INVESTIGATIONS

CAUTION TO ALL STUDENTS!

This Is To Warn Every Student From Primary School, Secondary School, College And University That The Directorate Of Criminal Investigations Is Archiving And Consolidating Charges That May Be Preferred To Each And Every Student Involved In Any Crime. Let Each Student Be Informed That It Will Automatically Be Reflected On The Police Clearance Certificate (CERTIFICATE OF GOOD CONDUCT) When such student will apply for one. This will be a permanent criminal mark that will bar many students from achieving their goals as no employer of worth will dare employ such characters. The crimes include armed and unpeaceable demos, arson, drugs, cyber bullying, assault of any degree, drunkenness or any reported crime of any kind. This is therefore to WARN the students and to ask parents, religious leaders, teachers and guardians to take note and advice them accordingly

DIRECTORATE OF CRIMINAL INVESTIGATIONS



The Voice of Private Sector in Kenya

467

1. DICTHO-
S
17/07/19
2. Kendi Ella
Schedule the
Meeting
19/7/19

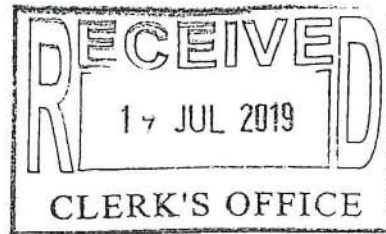
Ref: 173/07-PPD/2019

July 15, 2019

Hon. William Kisang, MP,
Chairperson,
Departmental Committee on Communication, Information and Innovation,
Kenya National Assembly,
Parliament Buildings,
P.O. Box 41842-0010,
Nairobi, Kenya.

Through:

Mr. Michael Sialai, EBS,
The Clerk,
Kenya National Assembly,
Parliament Buildings,
P.O. Box 41842-0010,
Nairobi, Kenya.



Dear Hon. Kisang,

RE: REQUEST FOR A MEETING WITH THE PARLIAMENTARY DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

Receive warm greetings from The Kenya Private Sector Alliance (KEPSA).

We wish to register our deep appreciation for the great support and partnership that the National Assembly has continuously accorded KEPSA. We consider Parliament is a pace setter in economic development, a role which it fulfils by coming up with laws that improve the business environment and the economy whilst protecting and advancing devolution of Government.

In furtherance of this ongoing legislative and policy partnership, we write to cordially request for a meeting with the KEPSA ICT Sector Board Members and the Parliamentary Departmental Committee of Communication, Information and Innovation to discuss the following:

1. Proposed Data Protection Bill 2019
2. Pending legislative issues including but not limited to Critical Infrastructure Protection Bill, Amendments to the Computer and Cybercrimes legislation among others.

We propose that the meeting is held on **Thursday, 25th July 2019, 10:00 am at Parliament Buildings.**

Kindly advise on your concurrence with the date and time or propose an alternative date that is convenient for you.

We thank you for your continued support and cooperation.

Yours Sincerely,



Carole Kariuki, MBS, HSC
Chief Executive Officer



No.	Section as it appears in the Bill	Proposed Amendment	Justification/ Rationale
Sec. 2 (Definitions)	Personal data means any information relating to an identified or identifiable natural person	The section should read as follows: "Sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, religious belief, genetic data, biometric data, sex or the sexual orientation.	Sensitive Personal Data definition makes reference to beliefs, this leaves a wide berth for interpretations and the final section "of the data subject" is repetitive since reference to the natural person has already been made at the start of the definition.
Secs. 8(b), 18, 19, 20, 21 and 22. (which read together provide for the maintenance of a data register)	Sec. 8 (b) The Office (which mean the office of the Data Protection Commissioner) shall establish and maintain a register of data controllers and data processors; Sec. 18(1): Subject to sub-section (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner Sec. 19(1): A data controller or data processor required to register under section 18 shall apply to the Data Commissioner. Sec. 20: A registration certificate issued under section 19 shall be valid for a period	It is recommended that instead of registering of data protection officers and auditors with the Office of Data Commissioner. This ensures that the professionals charged with ensuring data protection are up to the task at hand. Proposed new Sec: 18. No person shall act as a Data Protection Officer unless registered with the Data Commissioner. It is also recommended that the requirement for registration of data controllers/processors as provided for in Secs 18, 19, 20, 21 and 22 be deleted. A similar registration framework that had been promulgated under the E.U. Privacy Directive, in force between 1995 and 2018, was dropped in the	The Bill provides for the establishment and maintenance of a register of data controllers and data processors in Sec 8b. In Sec 18 there is the requirement for the registration of data controllers and processors with the office of the Data Commissioner. As drafted, it is not clear exactly what criteria for registration will be. Such a comprehensive and broad requirement for registration of all data controllers and processors will unnecessarily burden all parties involved with no commensurate business or consumer advantage. Secs 19, 20, 21 and 22 seek to operationalise Sec 18. Currently, all businesses are required to register under the various commercial laws and provide contact details where they can be reached by the relevant Registrar and business customers. The

		<p>It is therefore recommended that the section reads as follows:</p> <p><i>(h) Can be transferred out of Kenya to jurisdictions where the Data Commissioner has verified that there are equivalent levels of data protection and such a transfer shall not require any specific authorisation.</i></p>	
<p>Sec. 31 (Data protection impact assessment)</p>	<p>31(5) Does not exist</p>	<p>Proposed additional Sec to read as follows:</p> <p><i>31(5) The Data Protection Commissioner will issue guidelines on the types of data processing that will require a data protection impact assessment.</i></p>	<p>Lack of the additional sub-Sec may lead to ambiguity in the types of operations that will require a Data Protection Impact Assessment. To avoid this ambiguity, the DPC should give guidelines for this.</p>
<p>Sec. 35(3) (b)</p>	<p>Sec. 35(3) Where a data controller or data processor takes a decision, which produces legal effects or significantly affects the data subject based solely on automated processing-</p> <p>(b) The data subject may, before a reasonable period of receipt of the notification, request the data controller or data processor to-</p> <p>(i) Reconsider the decision; or</p> <p>(ii) Take a new decision that is not based solely on automated processing.</p>	<p>Further amend of Sec 35(3)(b) by replacing the word <i>before</i> with after.</p>	<p>Sec 35(3)(b) makes reference to "<i>before a reasonable period of receipt of notification.</i>" It is preferred to change this to "<i>a reasonable period after receipt of information.</i>"</p>
<p>Sec. 37 (2) (Processing for direct marketing)</p>	<p>Sec. 37(2): A data subject may object to processing of their personal data for such marketing, which includes profiling to the extent related to direct marketing.</p>	<p>Proposed deletion of Sec. 37(2)</p>	<p>Sec 31(1) adequately covers the protection by providing consent in the case of direct marketing however Sec 31 (2) states that the data subject may object to processing of data for the purposes of direct marketing. If consent is required in Sub-section (1) it then goes without saying that the data subject can object therefore sub Sec (2) is unnecessary.</p>

<p>Sec. 40(3) (right of rectification or erasure)</p>	<p>Where a data controller or data processor is required to rectify or erase personal data under sub-section (1), but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead of erasing or rectifying, restrict its processing and inform the data subject within a reasonable time.</p>	<p>The additional subsection allowing for restriction of processing (where it is not technically feasible to delete/erase personal data in question) to read as follows:</p> <p>40(3) <i>Where a data controller or data processor is required to rectify or erase personal data under sub-section (1) and</i></p> <p><i>i) such action is not technically feasible or</i></p> <p><i>ii) the personal data is required for the purposes of evidence</i></p> <p><i>the data controller or data processor shall instead of erasing or rectifying, restrict processing and inform the data subject within a reasonable time.</i></p>	<p>It is proposed to have an additional sub Sec that allows for the restriction of processing where it is not technically feasible to delete/erase personal data in question. Such as in the case of internet search engines results. The search engines are mere processors of content posted online. As processors, search engine businesses cannot delete information posted online by a data controller (author of post), processors can only de-index or delist specific URLs where such de-indexing is justified under law.</p>
<p>Sec. 47(3)</p>	<p>The Data Commissioner may specify other categories of personal data, which may require additional safeguards or restrictions.</p>	<p>It is proposed that the Bill defines a multi-stakeholder approach to reforms/expansion of the scope of the Act via subsidiary legislation in order to ensure all reforms continue to spur business growth for both local and foreign companies active in the Kenyan market.</p>	<p>The Bill authorizes the DPC to create additional categories for sensitive personal data beyond those defined in Sec 2. This approach recognizes that, as technology and society continue to evolve, data protection framework would have to evolve to meet arising needs.</p>
<p>Secs. 48, 49, 50 and 71 (2) (g)</p>	<p>Secs. 48, 49 and 50 make up Part VI- Transfer of Personal Data outside Kenya</p> <p>Sec 48 sets out the conditions for transfer out of Kenya.</p> <p>Sec 49 sets out the safeguards prior to transfer of personal data out of Kenya</p> <p>Sec 50 provides for processing through a data server or data centre in Kenya</p>	<p>It is recommended to delete of the entire Part VI and the adoption of Sec. 25 as drafted herein as it will place all authority on the office of the Data Commissioner to determine jurisdictions that have similar safeguards to allow the transfer of data out of Kenya.</p> <p>Further, delete Sec.71(2)(g).</p>	<p>The Bill outlines conditions that must be met in order for cross-border data to be permissible. This section creates a challenge for industry and regulators, as proving “appropriate safeguards” on a case by case basis is burdensome and legally challenging. It is unclear what exactly “appropriate safeguards,” means. The uncertainty of the interpretation of this phrase presents challenges to growth of the</p>

<p>Sec. 50 (Data Sharing Code)</p>	<p>Sec. 71 (2)(g) states as follows; Without prejudice to the generality of subsection (1), regulations made under that subsection may provide for- The processing of data through data server or data centre in Kenya;</p>	<p>Replace the word "code" with "regulation".</p>	<p>The Bill generally prohibits cross-border data transfers save for outlined exempted circumstances and specifically provides that the Cabinet Secretary can designate categories of critical personal data that can only be processed through a server or data centre in Kenya on grounds of "strategic interests of the state or on protection of revenue."</p> <p>Such a broad and ambiguous drafting significantly hinders growth of businesses that need a predictable business environment for investment and growth. We recommend that Parliament eliminate this requirement.</p>
<p>Sec. 58 And Sec. 73 (1)</p>	<p>The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.</p> <p>Sec. 58 provides for enforcement notices by the Data Commissioner who may serve an enforcement notice on a person who has failed to comply with any provision of the proposed legislation.</p> <p>Sec. 73(1) provides as follows: A person who commits any offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding two years, or to both.</p>	<p>It is proposed that Parliament limit penalties to fines after a proper demonstration of intention to cause harm.</p>	<p>This Sec makes reference to a data sharing code, the use of the word code may be confusing as one may imagine code used in computing, a less confusing word may be adopted.</p>
			<p>Imprisonment as a criminal penalty for violation of privacy is a departure from international norms and is potentially disproportionate penalty for a violation of obligations. Most privacy frameworks around the world depend on civil penalties to address violations, which generally impact the business/organisation rather than the employees charged with executing compliance obligations.</p> <p>Holding individuals criminally accountable for violations that may be as a result of the direction of their employer may prevent highly qualified an</p>

			competent individuals from accepting employment in support of the data protection practices of companies operating in Kenya.
--	--	--	--

Tabled before the Committee on
Tuesday 17th 9th Ptemba, 2019. ~~ETD~~

DATA PROTECTION BILL 2019

Data has been considered the commodity driving the fourth industrial revolution and has changed much of how we live and function. Due to more connectivity using Internet of Things, increased use of social media and digitization of traditional businesses, big data which involves the processing of large volumes of data has become more popular leading to new field of data analytics. Reliance on these data to inform marketing and people's choices even in election has brought positive reports for companies and electoral aspirants but negatively impact the rights and dignity of persons to whom these data belongs to. Such example is use of personal Facebook posts by Cambridge Analytica during 2013 and 2017 General Elections in Kenya to send emotive messages to electorates and influence their choice and vote¹.

To this end we welcome the Government initiative to enact a sound data Protection Act via the Data Protection Bill 2019, whose main aim is to protect the right to privacy under article 31 (c) and (d), establish office of the Data protection commission, regulate processing of personal data and establish rights and obligations of citizens, data controllers and data processors. The bill introduced in the National Assembly has made substantial improvements as compared to the earlier 2018 Data Protection Bill by: requiring informed consent to the processing of personal data, properly establishing the data protection commission as an independent office, providing higher penalties in case of breach, including the right to withdraw consent and right to data portability which is able to promote financial inclusion.

Noting that Kenya has a large unbanked population, portability enables one to transfer their credit history from one financial institution to another. An example is Safaricom a Mobile Network Operator, providing mobile financial services through its M-pesa platform and has developed its own credit score system to be used by other fintech companies and improve access to credit. This is because currently data held by Safaricom was under its control and the consumer was bound to sharing agreements entered into by Safaricom. One fintech company reports use of this credit score has increased accuracy of predicting payment. With the right of data portability, the consumer is able

¹<https://www.theelephant.info/features/2019/08/09/cambridge-analytica-and-the-2017-elections-why-has-the-kenyan-media-remained-silent/>

(e) Nominate three qualified applicants in order of merit for the position of data Commissioner and

(f) Submit the names of persons nominated under paragraph (e) to the cabinet secretary

6 (4) The cabinet secretary shall within fourteen days of receipt of the names of nominated candidates appoint one of the data commissioner

Given the increased use of data and place of data protection in the growing age it is paramount that we continue enhancing the independence of the commission by having the appointment done by the president and approved by the National Assembly. Moreover section 11 of the bill states that a vacancy shall arise in the office of data protection commissioner if *he resigns with a notice in writing addressed to the president*. Therefore, in order to reconcile these two provisions and enhance independence the above recommendation should be enacted.

Subsequently under section 68, the data protection commissioner prepares the annual budget estimates which are submitted to the national assembly by the cabinet secretary. To promote independence of the commission the data commissioner ought to table the budget estimates himself to the national assembly.

b) Constitution

Section 5 states *the office of the data protection commission shall comprise of the data protection officer as its head and accounting officer and other staff appointed by the data protection commission*.

As proposed by the Bill, the commission shall be comprised of only one commissioner and staff. Recognizing the commission shall exercise a quasi-judicial function, the need to ensure independence and proper function of the commission it's our recommendation that the composition be expanded to a board chaired by the data protection commissioner the members who are designated by law and borrow from various expertise in diverse fields.

Registration of data processors and data controllers

Section 18 states no person shall act as a data controllers and data processors unless registered with the data commissioner. This implies a mandatory registration requirement however section 18 (2) states the data commissioner shall prescribe the

threshold required for mandatory registration based on nature of the industry, volumes of data processed, sensitivity of data being processed.

It's evident from the above provisions that the bill ought to do away with mandatory registration for every data controller or processor and only require registration from those who meet the criteria of registration espoused by the commissioner.

Realizing that if threshold is required other persons such as operators of cybercafé in Kenya would be exempted. However, for the purpose of privacy we must recognize that they still come across rich information from data subjects due to the unique nature of their service and are already bound by the data protection bill and principles of data processing. The same is said of individuals who obtain private information from other persons and thus would still be bound by the constitution and the bill with the aim to respect privacy although not registered.

Self-Regulation

The main object of the bill according to the long title is to establish the office of the Data Protection Commissioner as an independent state office to oversee the implementation of the act. The act further through use of the word *shall* mandates the commission to promote self-regulation among all data controllers and data processors. We recognize this obligation is unnecessary as a statutory body established to regulate cannot then be charged with the duty to promote self-regulation. To begin with, without a current regulator, there is adequate room for self-regulation however, significant privacy breaches ensue with little incentive to regulate against it. A study investigating Biometric technology, elections and privacy found that, "there is need for an escrow institution empowered to keep the industry accountable in their data management practices. It is evident that public bodies, corporates, social media platforms have had the means but little incentive to self-regulate."³

Secondly, noting that the law should be clear and objective, it would be wiser if the Bill itself in a separate provision encouraged self-regulation as an internal function of data controllers and data processors. However, the extent to which they are allowed to self-regulate and matters to which they can deal with in the course of self-regulation should also be clearly defined. Data processors and controllers cannot be allowed to form self-

³ <https://blog.cipit.org/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf>

[2019]⁴ where the petitioner argued that the director of public prosecutions violated his right to privacy and that of his clients by obtaining information of his advocate- client account without his consent or any legal basis. The court however determined that the issue of privacy in question belonged to the clients who were the data subjects and proper plaintiffs of the suit. It is thus paramount that any collection of evidence still adheres to the data protection principles and the determination of these appeal will further influence the limit of this provision.

Notification of breach

Section 43 (6) states the communication of breach to a data subject may not be required where the data controller or data processor had implemented appropriate security safeguards which may include encryption of affected personal data.

The duty to notify a data subject of breach of their data should ensue despite having appropriate security measures. In fact, the data subjects ought to be notified of the breach in addition to the necessary security measures that have protected the data. The clause may be relied on by data processors and controllers to avoid informing the data subject of any security breach in order to avoid any liability. It is especially important where it involves the processing of sensitive personal data. Data subjects similarly have a right to be duly informed of any occurrence with their data as security measures can also be overridden.

Alternatively, such breaches must be logged and presented to the data protection commission in the annual audit report.

Processing of personal data

Section 45 ought to expressly include the government and other public authorities which will collect biometric data pursuant to the Registration of Persons Act.

Liability for staff in case of data breach

We welcome section 65 that enables data subjects to claim compensation for damage resulting from a contravention of the bill by data processors and data controllers. In light of the case of *Benedict Kabugi Ndungú v Safaricom PLC*⁵ for breach of privacy of 11.5 million subscribers by exposing their sport betting history and bio data. The

⁴ <http://kenyalaw.org/caselaw/cases/view/177071/>

⁵ <https://calvinayre.com/2019/06/26/business/safaricom-sued-for-losing-private-data-loss-of-11-5-million-gamblers/>

investigations led to the arrest of 2 Safaricom employees and the petitioner who brought suit under article 22 of the constitution would like the subscribers to receive compensation.

The deposit of personal data with a data controller or processor is likened to depositing a valuable in a safety deposit box. If the employees orchestrate the theft of the valuable, they would be criminally liable however the bank would still have to repay you for loss. Therefore, a positive outcome of the above case would improve privacy safeguards within institutions making them adopt more security design features of unauthorized access even from their own employees.

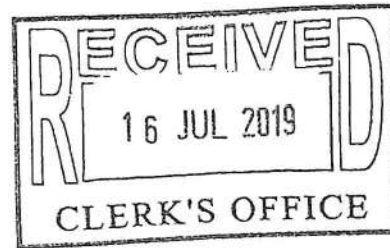
Catherine Muya - 0725953109.
Catherine.muya @lawyershub.ke



D1cmf...
8
16/7/19



Hon. Michael Sialai, EBS.
Clerk of the National Assembly,
Twelve Parliament-Third Session
Main Parliament Building,
P.O Box 41842-00100,
Nairobi, Kenya



Via E-Mail: clerk@parliament.go.ke

Dear Hon. Michael Sialai, EBS.

Submission of Comments on the Kenya Privacy and Data Protection Bill, 2018

We thank you for the opportunity to provide comments on the Kenya Data Protection bill 2019. We commend Kenya for ensuring strong protections for user privacy in this bill and believe that Kenya's law can be a model for other African nations.

We have focused our comments on the areas where we feel protections are missing and where your proposals and recommendations can be strengthened based on our experience and expertise advocating for individual security and privacy all over the world.

We appreciate the bill's aspiration to elaborate Article 31(c) and (d) of the Constitution of Kenya, 2010. We note that the *Data Protection Bill* sets out principles of data protection that are consistent with international standards and commend the approach to place users' rights at the center of the digital economy.

Mozilla is a global community of technologists, thinkers, and builders working together to keep the internet open, accessible, and secure. We are the creators of Firefox, an open source browser that hundreds of millions of people around the world use as their window to the web, as well as other products including Pocket, Rocket, and Focus. To fulfill the mission of keeping the web open and accessible to all, we are constantly investing in the security of our products and the privacy of our users.

Our commitment to user security and privacy can be seen both in the open source code of our products as well as in our policies. Consider, for example, Mozilla's Data Privacy Principles which guide the development of our products and services:

While we take action to protect our users' privacy and security every day, relying on these principles and other policies for guidance, we also believe in the importance of data protection law to ensure data controllers and processors are protecting the rights and interests of internet users. As we will elaborate on in this submission, we believe a strong data protection law requires:



1. The enshrinement of a robust framework of rights of individuals with meaningful user consent at its core;
2. Strong obligations on data controllers reflecting the significant responsibilities associated with collecting, storing, using, analyzing, and processing user data; and
3. Effective enforcement mechanisms including an empowered, independent, and well-resourced Data Protection Authority (DPA).

We look forward to continuing to engage with you and other stakeholders in the Kenyan government as work progresses to craft Kenya's historic first data protection law.

If you have any questions about our submission or if we can provide any additional information that would be helpful, please do not hesitate to contact Mozilla Policy Advisor Alice Munyua (amunyua@mozilla.com).

Executive Summary

Kenya is among the continent's most connected countries as well as a regional hub for digital start-ups and entrepreneurship. Mobile network coverage penetration rate is at 88.7%, with more than 40 million mobile subscriptions. Over 99% of internet subscribers access the internet via mobile phones. Kenya has also seen significant growth in online government services, and processing of personal data by the government is needed in order to access most of these services. Indeed, the Government of Kenya is likely the largest data controller in the country. Kenya has a significant data economy spanning both public and private sector. All of these public and private services have accelerated the collection and analysis of personal data.

While some of this collection and processing is a function of an advancing digital economy, the lack of comprehensive personal data protection legislation exposes Kenyan citizens to risks of misuse of their personal data.

We commend the government for setting out a clear framework based on international good practice, and our comments are intended to support and improve this strong draft.

Independence and powers of the Data Protection Commissioner

To ensure effective enforcement mechanisms of the new Privacy and Data Protection legislation, we strongly support the bill's intention to have an independent Data Protection Commissioner (DPC). Unfortunately, several sections of the bill undermine this provision by subjugating the DPC to the Cabinet Secretary, Ministry of Information and Communication Technology. We recommend that authority to set the qualifications of and nominate the DPC should rest with parliament and appointment should be made by the President. We propose additional powers and responsibilities to be assigned to the DPC, which include issuing regulatory guidance, codes of practice to data controllers and processors, investigatory, adjudicatory, levying penalties and punitive measures, as well as providing redress and compensation to users when their rights have been violated. The DPC should also be empowered to promote public awareness and engage in capacity development activities.



Missing protections on users' rights and data controller/processor obligations

We applaud the comprehensive provisions of rights of access, correction, right to seek confirmation, update, rectify, and object to processing, as well as data portability. We further welcome the restrictions imposed on data controllers and processors around purpose limitation, collection limitation, and data retention limitation.

We however, note that while the policy framework includes the principle of data minimization, the bill does not contain this obligation. We believe this obligation should be added to the legislation and that language should be added to clarify that where information is longer necessary for the purposes for which it was collected, it should be deleted.

We appreciate the importance placed on obtaining user consent in this bill. However, consent must be meaningful. We refer to guidance issued by Article 29 Working Party of the European Union Data Protection Authorities on the elements of valid consent, which must be free, informed, unambiguous, clear, specific, and capable of being withdrawn. This sets a high bar for data controllers and processors seeking to process personal data on the basis of consent. "Explicit consent" must be a requirement for processing of sensitive data. We recommend that the DPC issues guidelines on how requirements around consent in this bill should be interpreted.

Principles and Obligations of Personal Data Protection

We support strong obligations placed on data controllers and processors reflecting the significant responsibilities associated with collecting, storing, using, analyzing, and processing user data. We also propose stiffer penalties that will provide better incentives to data controllers and processors to abide by the provisions of this law. Strong penalties and a strong, independent regulator are critical to the effectiveness of data protection law.

All public and private sector data controllers and processors must be bound by a general duty to process data in a manner that respects the privacy of an individual and that provides security against data breaches.

Data protection officers

We note that the bill requires all controllers and processors to register with the DPC and designate a data protection officer. This obligation would place an undue burden on small and medium enterprises (SMEs) and startups, which play an important role in the Kenya's digital transformation. While we recommend greater regulatory oversight for data controllers and processors who process large volumes of data, particularly sensitive data, or otherwise pose an elevated risk to the privacy rights of users, we do not believe mandatory registration of all data controllers and processors is wise or worthwhile.

Security safeguards

Data controllers and processors should take appropriate and reasonable measures to safeguard the data that they have been entrusted with. The bill appears to obligate controllers and processors to



use pseudonymization as a security tool. We respectfully caution against over reliance on only this technique as a safeguard as it may not be feasible in many use cases. We would instead recommend that all data controllers and processors be obligated to take appropriate and reasonable measures to safeguard the data that they have been entrusted with, whether via encryption, pseudonymization, or other means. Additionally, we recommend an obligation that all data controllers and processors encrypt sensitive personal data.

Data breaches

The bill proposes attribution of breaches that lead to the unauthorized disclosure of personal data, however, this is often very difficult and time consuming, even for the most well-resourced data controllers and processors. Furthermore, notification of an unauthorized disclosure to affected data subjects should not wait for attribution. We propose clarifying this provision to require attribution information to be included "where available." This will go a long way to ensuring that notification occurs in a timely manner and will provide greater legal clarity to data controllers and processors.

Protecting Children Personal Data

We are pleased to note that the bill contains a provision protecting the right to privacy of children as provided under article 19 of the Children Act. We would encourage the Government of Kenya to reconcile this bill with the Children Act, 2001 to ensure legal clarity on the data protection rights of children and the obligations on data controllers and processors who process the personal data of children. We recommend clarifying the language of this section to specify that data controllers and processors should not *knowingly* market, track, or profile children *without the consent of their parental guardian*.

The "parental consent" requirement in the bill raises practical questions regarding its implementation. We propose further reflection on parental permission and recommend that the DPC be mandated to provide guidelines on the impact of data protection law on children and explore these proposed approaches, particularly those relating to age verification mechanisms.

We recommend deletion of the provision that mandates the DPC to appoint data controllers and processors as guardians. This provision creates substantial legal confusion and places additional primary and secondary liability on data controllers and processors who will be designated as guardians.

Protecting Personal Sensitive Data

We note with concern the discrepancy between the definition of sensitive personal data in the policy and in the text of the bill. While we believe the policy, language includes a progressive list of what should be considered sensitive personal data, there are several critical omissions. The list contained in the policy should replace the definition of sensitive personal data in the bill and should be further amended to include: official or national IDs, passwords, financial data, and location information. We also recommend that the DPC is empowered to assess and add to the definition and categories of sensitive data in an open consultation process.



Exemptions

We are concerned that some of the exemptions provided in the Bill do not appear to satisfy Article 24 of the Constitution, which provides for the right to privacy. While, we recognize that there may be legitimate reasons for various parts of the government to share information with each other on a “*need to know basis*,” this provision is quite broadly worded. Furthermore, while the obligation to seek consent may not apply in these scenarios, public authorities should still always be bound by the other principles of data protection including purpose limitation, collection limitation, security safeguards, etc.

In addition, exemptions for the purposes of investigating crimes, or for any other purposes related to maintaining public safety and national security must be understood as exemptions from seeking user consent, not from all data protection requirements. Law Enforcement Agencies must also be bound by requirements around data security, purpose limitation, collection limitation, the right to rectify, the right to erasure, etc. Data processing for public safety, national security and law enforcement must be “necessary and proportionate”, and authorized by law.

The provision to exempt for the purposes of history, research, and statistics could be subject to abuse by data controllers and processors. We recommend clear definitions and limiting scope for research purposes that is aimed at or culminate in commercial exploitation.

Data localization

We note with concern provisions contained in the bill obligating data controllers to “ensure the storage, on a server or data center located in Kenya of at least one serving copy of personal data” and other prohibitions on the transfer of sensitive data outside Kenya.

Requiring data to be localized not only creates a security risk, with a central point of attack or single point of failure, but undermines efficiency and integrity of internet traffic. The requirement to store data or a copy of data locally, introduces potentially higher costs and actual limitations on technology innovation, development, and use, and introduces a conflict of laws situation for multinational companies.

We acknowledge that certain categories of personal data may need to be mandatorily stored within the country, with restricted data flows, due to the strategic and security interests at play. However, the bill leaves the definition of critical personal data entirely open to Government discretion and does not elucidate what such categories might be, nor any parameters to circumscribe this discretion. Since mandating data storage in Kenya generally amplifies the concerns of routing inefficiencies, increased costs, and security risks, this wide discretion is concerning. We recommend that categories of critical personal data that are currently localized in Kenya for strategic or security reasons be clearly stated. The open-ended mandate to the government to notify further categories should be removed.

In addition, we recognize the needs and compelling interests of both private and public data controllers and processors to process sensitive personal data outside of Kenya. For example, financial institutions (whether banks or public authorities) transfer financial information to check for fraud and terrorist financing, for example. This provision as currently written could be read to



preclude Kenya's participation in the SWIFT network, which would be gravely detrimental to Kenya's financial sector and economic standing in the world.

We respectfully recommend that the Government of Kenya is concerned about law enforcement access to data, a legal framework for surveillance with appropriate protections for users is developed, providing a lawful basis for the government to access data necessary for legal proceedings.

Reconciling the Data Protection Act with other laws

Kenya has statutes dating as far back as pre-independence. Some of these statutes contain provisions that override this proposed bill, thereby threatening the good intentions of this framework. Such laws include: Preservation of Public Security Act, Official Secrets Act Cap 187, National Intelligence Service Act, 2012 and The Prevention of Terrorism Act No 30 of 2012 just to name a few. These laws have provisions authorizing the government to collect, process, and share data without consent in circumstances that are not well defined and therefore subject to misuse.

In order to give full effect to the strong protections contained in this legislation, we respectfully recommend a package of amendments be offered to revise the provisions in previous legislation.

Conclusion

In Kenya's new constitution 2010, the government took important action to recognize and protect the right to privacy in Article 31. The data protection legislation under discussion today represents an historic next step in the cause of protecting Kenyans, especially in the face of new technological developments. We commend the Government of Kenya for the thoughtful and thorough framework, which we believe with some amendments has the potential to be a model to all African nations.

We look forward to continuing to work with the Parliamentary Committee as you further develop Kenya's first data protection bill.

Thank you for your consideration of our submission.

For any further questions please consult Mozilla Policy Advisor Alice Munyua (amunyua@mozilla.com).

Respectfully submitted by:

Alice Munyua
Policy Advisor
Mozilla Corporation



preclude Kenya's participation in the SWIFT network, which would be gravely detrimental to Kenya's financial sector and economic standing in the world.

We respectfully recommend that the Government of Kenya is concerned about law enforcement access to data, a legal framework for surveillance with appropriate protections for users is developed, providing a lawful basis for the government to access data necessary for legal proceedings.

Reconciling the Data Protection Act with other laws

Kenya has statutes dating as far back as pre-independence. Some of these statutes contain provisions that override this proposed bill, thereby threatening the good intentions of this framework. Such laws include: Preservation of Public Security Act, Official Secrets Act Cap 187, National Intelligence Service Act, 2012 and The Prevention of Terrorism Act No 30 of 2012 just to name a few. These laws have provisions authorizing the government to collect, process, and share data without consent in circumstances that are not well defined and therefore subject to misuse.

In order to give full effect to the strong protections contained in this legislation, we respectfully recommend a package of amendments be offered to revise the provisions in previous legislation.

Conclusion

In Kenya's new constitution 2010, the government took important action to recognize and protect the right to privacy in Article 31. The data protection legislation under discussion today represents an historic next step in the cause of protecting Kenyans, especially in the face of new technological developments. We commend the Government of Kenya for the thoughtful and thorough framework, which we believe with some amendments has the potential to be a model to all African nations.

We look forward to continuing to work with the Parliamentary Committee as you further develop Kenya's first data protection bill.

Thank you for your consideration of our submission.

For any further questions please consult Mozilla Policy Advisor Alice Munyua (amunyua@mozilla.com).

Respectfully submitted by:

Alice Munyua
Policy Advisor
Mozilla Corporation

TESPOK07/014/19

July 15th, 2019

Mr. Michael Sialai, EBS
Clerk of the National Assembly,
Parliamentary Service Commission,
P.O Box 41842-00100,
NAIROBI

Dear Mr. Sialai,

RE: SUBMISSIONS ON THE DATA PROTECTION BILL, 2019

We the Telecommunications Service Providers association of Kenya (TESPOK) would like to respond to your call for comments in the Daily Nation dated 10th July 2019. Considering the short period provided we have attempted to reach to our 60+ membership of Mobile Network Operators, Internet Service Providers, Carriers, Data Centre Operators and Technology Service Providers for input. We are still receiving input and hope that we can be given a chance to share our consolidated position.

In this regard, please see attached our current submissions on the proposed Data Protection Bill, 2019 for your kind consideration.

We are happy to meet and make oral presentations on the same.

Yours Sincerely,

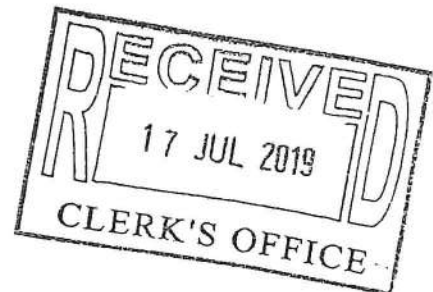


Fiona Asonga
Chief Executive Officer

Cc:

Hon William Kisang, MP
Chairperson,
Departmental Committee on Communication, Information and Innovation,
Kenya National Assembly,
Parliament Buildings,
P.O. Box 41842-0010,
Nairobi, Kenya.

1. D/C - Head
8
17/07/19
2. Kenadi R/A
for consideration
by the Committee
19/7/19



*To be the Voice of Technology Influencing
Policy, Direction and Development in the Industry*

This is a review of the Data Protection Bills currently under consideration by the National Assembly. The National Assembly Bill published the Ministry of ICT's version and read it a first time in the National Assembly. It now stands committed to the Departmental Committee on Communication, Information and Innovation of the National Assembly which is conducting public participation on the Bill. In this regard, the National Assembly through the Clerk has invited members of the public to make its submissions on the same vide a Notice published on 10th July, 2019. **The deadline for submissions is 16th July, 2019.**

The overview herein below highlights the contents of the Bill as well as the highlights on key cross-cutting issues that must be addressed. The streamlining of relevant legislative proposals will provide for a harmonized data protection framework thus creating a conducive environment for private sector business operations.

	NATIONAL ASSEMBLY BILL	PROPOSAL	JUSTIFICATION
1.	Preliminary: Title, Scope, Definitions <ul style="list-style-type: none"> • Short title, Interpretation, Object and Purpose and Scope • The Bill is titled Data Protection Act 2019 • Definitions: Consent- voluntary, specific and 		

	<p>informed expression of will of a data subject to process personal data.</p> <ul style="list-style-type: none"> • Sensitive personal data- data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, sex or the sexual orientation of the data subject. • Data protection principles: lawful processing, minimisation of collection, restriction to further processing, data quality and security safe guards. • The Act to apply to data controller/processors established in Kenya, foreign data controller/processor processing personal data of a Kenyan resident and to automated processing. It applies to non-automated processing forming part of a filing system. The term Filing system is defined as any structured set of personal data which is readily accessible by reference to a data subject or according to a specific criteria whether centralised, decentralised or dispersed on a functional or geographical basis. 	<p>Definitions: Consent: maintain the current definition which refers to <i>voluntary, specific and informed expression of will of a data subject to process personal data.</i></p> <p>Sensitive Personal Data - maintain the current definition</p> <p>Filing system- <i>A decision needs to be made regarding automated /non-automated decisions and filing systems. We recommend deletion of reference to both automated and non-automated systems</i></p> <p>Exemption: Act does not apply to national security agencies. Public bodies required to apply for ex parte orders before processing data unless there is imminent danger to life/property.</p> <p><i>Define term imminent danger or at least list matters court/security agency/third party is to consider in determining whether court orders are needed or not.</i></p>	<p>It aligns to industry best practise</p> <p>It aligns to industry best practise</p> <p>Data Protection Principles that align to GDPR are important to facilitate continued economic activity.</p> <p>To provide clarity for both automated and non-automated decisions and filing systems.</p> <p>Its would be important to determine where the act doesn't apply.</p>
2.	<p>Establishment/Designation of National Data Protection Authority (DPA)</p> <ul style="list-style-type: none"> • Established an independent office of the Data Protection Commissioner as a state office. To 	<p>Support having and Independent office of the Data Protection</p>	<p>To align with global best practise</p>

	<p>be recruited via competitive process by Public Service Commission and appointed by the Cabinet Secretary via Gazette Notice for a single term of 6 years. May resign from office by notice in writing to the president. (S11b)</p>	<p>Commissioner as a state office. We recommend streamlining of appointment and resignation authorities. Same authority to appoint and receive resignation notice.</p>	
3.	<p>Registration of Data Controllers and Processors</p> <ul style="list-style-type: none"> • Data controllers/processors required to register. (S18) • Option to appoint a data protection officer to ensure compliance with Act (S 24) 	<ul style="list-style-type: none"> • We recommend the requirement for registration be deleted. And if retained only for controllers/processors dealing with sensitive/special personal data. 	<ul style="list-style-type: none"> • The scope of those who have to register will be so broad that it will not be practical to register all of them.
4.	<p>Principles and obligations of personal data protection and Processing of special Information</p> <ul style="list-style-type: none"> • Data protection principles: lawful processing, minimisation of collection, restriction to further processing, data quality and security safe guards. • Cross broader data transfers prohibited unless there is proof of adequate data protection safeguards or consent from the data subject. • Data subject rights: to be informed of how their data will be used, to access their data in custody of controller/processor, to object to processing of all or part of their data, to correction/deletion of false data. • Data controller/processor to collect data for a purpose which is lawful, specific and explicitly defined. • Requirement for data protection impact assessment where processing of data is likely to result in a high risk to interfere with rights and freedoms of data subject and consult with the 	<p>We are in support of the Data protection principles as captured. However on the right of the subject to change/ correct or erase their data:</p> <p>We recommend the section to include where erasure is not technically possible, controller/processor to restrict use.</p>	<ul style="list-style-type: none"> •

	<ul style="list-style-type: none"> • DPA before processing. Conditions of consent: It is the data controller/processor with burden to prove that data subject consented to processing of data (S32). In determining whether consent was freely given, the DPA shall consider whether performance of contract/service is conditional on consent to processing of data that is not necessary for contract/service performance. • Duty of data controller/processor to adopt appropriate measures for age verification and the giving of consent for processing of personal data. (S33-2). Mechanisms shall include available technology, volume of personal data processed, proportion of processed data likely to be that of a child, possibility of harm to child arising from processing and other relevant factors. • Data controller/processor to restrict processing of personal data where accuracy of personal data is contested, data is no longer required for purpose of the processing (unless required for legal claim), processing is unlawful and data subject opposes erasure of data and requests restrictions instead, data subject had objected to processing pending verification of the presence of overriding interests. (S34) Data controller/processor to ensure time limits established for restriction, deletion, rectification is observed. • Data subject may object to decisions made via automated processing (S35) • Data subject may object to processing of data unless data controller/processor demonstrate compelling legitimate interests for processing or overriding legitimate interests for processing of data/for establishing a legal claim. 	

	<p>(S 36)</p> <ul style="list-style-type: none"> • Data subject has right to portability. Data controller/processor to comply at reasonable cost and within 30days of request. (S38) • Data subject has a right to rectification and erasure of false/misleading information. Where erasure is not possible, data controller/processor shall be required to restrict processing. (S40-3). • Data controller/processor to notify DPA of breach within 72 hours. Where delay in notifying, to provide reasons for delay. 		
5.	<p>Grounds for processing of sensitive personal data</p> <ul style="list-style-type: none"> • Principles of data protection apply to processing of sensitive personal data. (S44) 	<ul style="list-style-type: none"> • The same principles of data protection apply 	<ul style="list-style-type: none"> •
6.	<p>Transfer of personal data outside Kenya</p> <ul style="list-style-type: none"> • Cross border data transfers only allowed where controller/processor has given DPA proof of adequate safeguards, where data subject consents or transfer is necessary for contract performance, overriding public interest, controller/processor is pursuing compelling legitimate interest. (S48 &49). Burden of proof is on controller/processor • The Cabinet secretary may prescribe certain nature of processing that will only be effected through a server or data centre located in Kenya. For purposes of strategic interests of the state or protection of revenue. (S 50) 	<p>In support of allowing cross boarder data transfer so long as there is proof of adequate safeguards being in place.</p>	<ul style="list-style-type: none"> • The digital economy is dependent on cross boarder interactions that require data to flow across countries and regions.
7.	<p>Exemptions</p> <ul style="list-style-type: none"> • Act does not apply to processing of data for household activities, research history and statistics, processing necessary for national security/public order or for disclosures required 		

	<p>under law, processing for publication of literally or artistic material, processing in public interest or where application of data principles is incompatible with special reasons for processing data. (S 52 & 53)</p>		
<p>8.</p>	<p>Enforcement Provisions</p> <ul style="list-style-type: none"> • DPA to handle complaints. Where not able to resolve complaint within reasonable time, DPA to notify complainant. (S56) • DPA has power to investigate complaints, powers to summon persons and request for books/evidence, administer oaths, power of search and entry, power to seek assistance, serve enforcement notice requiring specific action, or enforce administrative fines. (S57-60) • Enforcement notices- specify enabling section of Act, outline required steps to be taken and timelines (max 21 days), state right of appeal. Failure to comply is an offence and controller/processor liable to max fin of 5 million KES or 2 years imprisonment or both. (S58-3) • Penalty notices- Issued to a controller/processor who fails to comply with enforcement notice for no justifiable cause. The notice administers a fine as a penalty for noncompliance with the enforcement notice. Maximum penalty 5 million KES for or 2% of annual turnover of preceding financial year, whichever is higher. (S63) • Parties have right of appeal to High Court (S 64) • Data controller liable for damage caused by processing of personal data unless they can prove they are not in any way responsible for circumstances causing damage. (S 65 -2-a and 	<ul style="list-style-type: none"> • In support of current enforcement provisions 	<ul style="list-style-type: none"> •

	<p>3)</p> <ul style="list-style-type: none"> Data processors not liable for damage unless processor fails to comply with obligation under the Act or processes information contrary to data controller's lawful instructions. 		
9.	Financial Provisions		
	<ul style="list-style-type: none"> Data Commissioner Office be funded from money allocated by the National Assembly, grants, gifts, donations and money accruing through fines/penalties/performance of office duties. (S67) 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">
10.	Provisions of Delegated Power and Miscellaneous Provisions		
	<ul style="list-style-type: none"> Cabinet secretary may make regulations effecting this Act including regulations for: (s71) Requirements for controllers/processors when processing personal data under the Act Mechanisms of conducting certification programs Content required in notice of registration for controller/processor Information to be provided to a data subject and mode of provision Fees and charges under the Act Measures to safeguard data subject's rights Processing of data through data servers/centres in Kenya Approval of codes of practice/guidelines Data commissioner may prescribe <ul style="list-style-type: none"> other categories of data to be considered sensitive personal data Situations where Act does not apply/exemptions. Develop sector guidelines in areas such as health, financial services, education and social protection. 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> We recommend that collection of data under the Registration of Persons Act should also be subject to data protection principles under the Bill.

1. Scope/application

Under both Bills, the Data Protection Act would apply to data controllers/processors established in Kenya, foreign data controllers/processors processing personal data of a Kenyan resident and to automated processing. It applies to non-automated processing forming part of a filing system.

The draft Bill seem to extend the reach of Kenyan law to foreign jurisdictions in a way that create regulatory uncertainty for global data-intensive businesses. The envisioned Data Protection Law would apply to organisations not established in Kenya but which process personal data of data subjects resident in Kenya. Such a broad application is unjustifiable in an open and democratic society as well as an extreme departure from international norms.

Recommendation:

The exclusion of processing of personal data outside of Kenya from the scope of the Data Protection law. However, should Parliament decide to include it, it is recommended that the limitation of the scope of application to processing of the personal data of Kenyan residents in other jurisdictions only in clear, specific and limited circumstances so as to clarify the basis the provision of extra-territorial jurisdiction. The clear, specific and limited circumstances could include processing the data Kenya residents for the purpose of engaging in commercial transactions with them. The broad provisions in the draft bills will make it difficult and in some cases impossible for organisations to determine whether their processing is subject to Kenya's privacy law.

Many businesses outside of Kenya, including small- and medium-sized enterprises that are not focused on the Kenya market would have no reason to suspect that Kenya's privacy law may apply to their data processing. At the very least, the definition should be narrowed and clarified to enable appropriate compliance and enforcement.

2. Registration of data controllers and processors

The Bill require the registration of data controllers and processors with the Data Protection Authority (DPA).

Recommendation:

Deletion of this requirement: A similar registration framework promulgated under the E.U. Privacy Directive, in force between 1995 and 2018, was dropped after the concept proved unworkable. Such a comprehensive and broad requirement for registration will unnecessarily burden all parties involved with no business or consumer advantage. Currently, all businesses are required to register under the various commercial laws and provide contact details where they can be reached by the relevant Registrar and business customers. The requirement for registration of data controllers and processors would present a further barrier to ease of doing business in Kenya and discourage particularly the small- and medium-sized enterprises, from engaging in the digital economy in Kenya. It may also cause

corporations in multiple states to decrease their Kenyan economical activities and investments due to uncertainty of enforcing such a framework.

3. Principles and Obligations of Personal Data Protection

The Bill prohibits cross- border data transfers and require that where such transfers are to occur, the data controller/processor must satisfy the DPA that the laws of the country to which data is being transferred offer adequate protection of data that is comparable to that offered under Kenyan law. The Bill as drafted do not offer clarity on how the DPA would perform its adequacy determination and, the DPA's interpretation of adequacy may decrease, stifle, interfere with or hinder competition in the digital economy.

Recommendation:

The bills be aligned with international best practice by expressly acknowledging that there are many alternative private frameworks that may provide adequate safeguards, such as the self-regulatory frameworks.

4. Duty to notify data subject of intended recipients of their data before collection of data

The Bill require data controllers and processors to inform data subjects about all persons (natural/legal) who will receive the data subject's data prior to collecting the personal data. The draft bill fail to recognize the potential complexities of such notice requirements. In most cases, it is not always practical for a controller/processor to know all persons who may receive data collected. If implemented as is, this section may limit the ability of companies to alter business relationships, suppliers, vendors and partners.

Recommendation:

Re-drafting of the clauses sections to provide for notice of the categories/classes of persons who would/may receive data.

5. Right to data portability

The Bill establishes a data subjects' right to data portability such that they have "the right to receive personal data concerning them, which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format." Data portability is expensive and difficult for certain organisations, but many businesses are already seeking to provide this service in response to consumer demand.

Recommendation:

It is proposed that Parliament refine this clause with industry input to adhere to what is technically feasible.

The bill requires that portability requests be honoured within 7 days of receipt. Stating a specific timeline for responding to requests for data portability may not adequately provide for the realities on the ground at time of portability request.

6. Right to deletion of personal data records

The Bill provides for the right of the data subject to request erasure or destruction of personal data by the data controller or data processor often dubbed the 'right to be forgotten'. This right raises serious concerns regarding freedom of expression and is inconsistent with the design and workings of the Internet. While individuals should be able to withdraw their consent to data processing, within clear and reasonable limits, implementation of a right to be 'forgotten' creates room for online content censorship. Publicly available information is often available across multiple sites on the Internet, making the proposed notification requirement very difficult and even impossible to implement. Due to the international nature of the internet, such provision also interferes with the preservation of data protected or required under foreign law.

Recommendation:

We recommend modification of this right for information available on the internet.

Further only a court of competent jurisdiction (not a data subject/controller or processor) should be determining what is/ has become 'irrelevant/excessive or illegally obtained' data in need of deletion.

7. Development of further categories of sensitive/special data

The Bill authorizes the respective DPA to create additional categories for sensitive /special personal data beyond those defined in Section 2. This approach recognizes that as technology and society evolve, data protection framework would have to evolve to meet arising needs.

Recommendation:

We recommend that the Bill defines a multi-stakeholder approach to reforms/expansion of the scope of the Act via Guidelines or subsidiary legislation in order to ensure all reforms continue to spur business growth for both local and foreign companies active in the Kenyan market.

8. Cross-border data transfers

The Bill generally prohibits cross-border data transfers save for outlined exempted circumstances. The National Assembly Bill further specifically provides that the Cabinet Secretary can designate categories of critical personal data that can only be processed in Kenya on grounds of "strategic interests of the state or on protection of revenue." Such a broad and ambiguous drafting significantly hinders growth of businesses that need a predictable business environment for investment and growth.

Recommendation:

It is proposed that Parliament eliminate this requirement or, at the very least, to provide clarifications about the "strategic interests and protection of revenue" provision, to alleviate uncertainty for private sector investments and operation in Kenya.

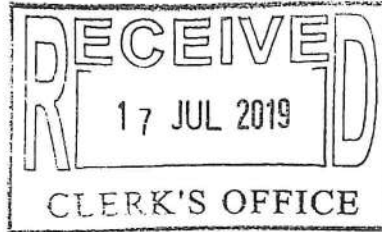


968

Branch International Limited
 Registration Number: CPR/2015/183658
 Reliable Towers, Fourth Floor, Mogotio Rd, Westlands
 P.O. Box 52689- 00100, Nairobi, Kenya
 kenya@branch.co

16 July 2019

Office of the Clerk
 National Assembly
 Main Parliament Buildings
 P. O. Box 41842 - 00100
 Email: clerk@parliament.go.ke
 Website: www.parliament.go.ke
 Nairobi
 Kenya



*1-04 cutler
 17/07/19*

Advance copy by e-mail

Dear Sirs

PROPOSED DATA PROTECTION BILL-2019

Thank you for inviting feedback on the proposed Data Protection Bill, 2019 (the **Bill**).

We, Branch International Limited (**Branch**), identify strongly with the objectives of the Bill. We are a socially conscious financial services company that uses technology to enhance access to financial services in emerging markets. Kenya is a key market for Branch and we have over one million customers registered on our lending mobile phone application.

Technology has enabled us to offer credit to a large number of people who were previously locked out of the formal financial credit system due to lack of traditional proof of income such as pay slips. Through innovation, Branch has been able to use data given by our customers to assess their creditworthiness and avail funds to them. We recognize the instrumental role that data plays in our business and have always strived to adhere to global best practice in protecting our customer's data. Indeed, data privacy is key to our business.

Through this letter we would like to share the benefit of our experience as we believe that through working with yourselves and other stakeholders we can ensure that the proposed legislation achieves its intended objectives.

Please find attached our comments on the Bill. We are available to meet with the Taskforce to discuss the submissions.

Please do not hesitate to contact the undersigned should you require clarification or further information.

Yours faithfully,

Daniel Szapak

Daniel Szapak
 Head of Global Operations
 Branch International
dszapak@branch.co
 0733-333302

Dan Karuga

Dan Karuga
 General Manager
 Branch International
dan.karuga@branch.co
 0792-651384

*Kendrick Ellis
 for consideration
 by the Committee
 19/7/19*





Section	Considerations
<p>Section 50- Safeguards prior to cross boarder transfer.</p>	<p><u>Provision</u></p> <p>The Section allow the Cabinet Secretary to restrict certain data processing to Kenya on the grounds of strategic interests of the state or protection of revenue.</p> <p><u>Concern</u></p> <p>The Cabinet Secretary has been given unfettered rights to prohibit the processing of data outside Kenya to protect revenue.</p> <p>This creates an opportunity for improper exercise of discretion which is further exacerbated by the lack of a mechanism in the Bill to challenge a determination by the Cabinet Secretary.</p> <p><u>Proposal</u></p> <p>We propose that this Section should be amended to introduce a requirement that where data processing is restricted to protect revenue, the cost of processing data in Kenya as well as the applicable capacity should be comparable to what is available cross-order.</p> <p>The Cabinet Secretary should also be required to issue a notice to any affected data controller or data processor before exercising his powers.</p> <p>Further, any data controller or processor likely to be affected by the exercise of the above powers should be given adequate opportunity to be heard and to take any measures to comply or mitigate any adverse effects on its operations.</p> <p>The section should be amended to introduce checks and measures to ensure that the powers are exercised reasonably and not abused.</p>
<p>Section 35(3) and (4)</p>	<p><u>Provision</u></p> <p>The section provides that the data subject has the right to require that the decision based on automated data processing be reconsidered</p>



Branch International Limited
Registration Number: CPR/2015/183658
Reliable Towers, Fourth Floor, Mogotio Rd, Westlands
P.O. Box 52689- 00100, Nairobi, Kenya
kenya@branch.co

<p>Decision making based on automated data processing</p>	<p>or that a new decision that is not based solely on automated processing be taken.</p> <p>Proposal</p> <p>We propose that this Section should be amended to provide that the above rights of data subject does not apply to circumstances where the data subject has given prior consent to decisions being made solely based on automated data processing.</p>
--	--



BOWMANS

1006

① D/C M...
8/23/19

COULSON HARNEY LLP
5th Floor, West Wing, ICEA Lion Centre
Riverside Park, Chiromo Road
PO Box 10643-00100, Nairobi, Kenya
+254 20 289 9000 | +254 709 966 000
+254 20 444 8614 | +254 734 993 739
PIN No. POS1229962P | VAT No. 0191639L

www.bowmanslaw.com

Our Reference: JNS/ATI
Direct Line: +254 20 289 9000
Email Address: john.syekei@bowmanslaw.com

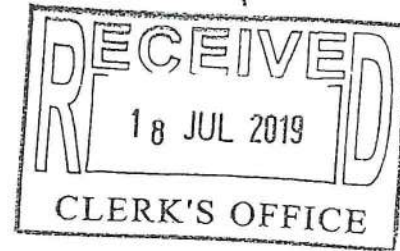
Your Reference: 16.07.2019
Date:

② EMB/ET
Please deal
HT
23/7/19

The Clerk of the National Assembly
The Office of the Clerk
Main Parliament Buildings
Nairobi

Sent via email to: clerk@parliament.go.ke

Dear Mr Michael Sialai, EBS



SUBMISSION OF MEMORANDA: THE DATA PROTECTION BILL 2019

In accordance with the provisions of Article 118(1)(b) of the Constitution and Standing Order 127(3), we hereby submit our representations on the Data Protection Bill 2019 ("Bill") as published in the Kenya Gazette Supplement No. 93 (National Assembly Bills No.44) as follows:

Section	Representations
Section 4(b)(ii)	To be clarified to include the following underlined words: "(ii) <i>not established or ordinarily resident in Kenya, but processing personal data of data subjects <u>located</u> in Kenya</i> ";
Section 18(2)	The Bill should not stifle small and medium enterprises. In our view certain provisions of this Bill may place unnecessary obligations and administrative burdens on small and medium enterprises. The requirement to register with the Data Commissioner should not be mandatory on all data controllers and data processors, and in making such determination, the Data Commissioner should also consider the number of employees employed by the data controller and data processor (for example, the registration requirements should only apply where an entity employs 100 or more persons) and/or should also meet



	<p>a certain turnover threshold requirement. This will create certainty across all sectors.</p> <p>Alternatively, whilst registration may be mandatory for all data controllers and processors, a helpful example is that taken from the GDPR which applies certain exemptions for small and medium sized enterprises. The GDPR requires small and medium sized organisations with fewer than 250 organisations to document processing activities in specific limited circumstances.</p> <p>In our view, certain exemptions to mandatory registration by data controllers and data processors should be taken into consideration to protect small and medium sized enterprises.</p>
28(2)(b)	<p>To be clarified to include the following underlined words:</p> <p><i>"the data subject has deliberately <u>and manifestly</u> made the data public"</i></p>
28(2)(c)	<p>This section should be deleted.</p> <p>The narrow exceptions where personal data can be collected indirectly should be finite and limited. By allowing for the indirect collection of personal data where the data subject has consented to the collection from another source, limits and conflicts with the data subjects rights under Section 25(g), 26, 35, 36, 38, 39 and 40 of the Bill. The data subject loses control of his/her personal data which should not be the intention of the Bill and deprives the data subject of his or her remedies under the Bill.</p>
48(a)	<p>The Data Commissioner should establish at the outset what the "appropriate safeguards" are to be applied in the context of any cross-border transfer. There is no clarity as to whether or not this requires that certain technical and security measures must be in place or what the minimum threshold should be prior to transfer out of Kenya.</p>
48(a)	<p>To be amended to include the following underlined wording:</p> <p><i>"the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data <u>and on condition that enforceable data subject rights and effective legal remedies for data subjects are available"</u></i></p>



BOWMANS

50 and 71 (2) (g)	<p>This should be deleted.</p> <p>If personal data is to be processed in Kenya, the security and integrity of the data may be at risk and international data controllers may not be able to be assured of the level of technical and network security integrity. Kenya may not also be able to guarantee an international standard of systems infrastructure.</p> <p>If Kenya is to be an international player in the technology sector, it cannot impose territorial limits on the processing of certain types of data which will be at the discretion of the Cabinet Secretary. This concern has been raised on several occasions during previous public participation forums.</p>
30(1)(v), 30(1)(vii) and 51(2)(b)	<p>There should be strict limits on the avoidance of the application of the Bill for national security reasons, by any person in the public interest, national security or public order.</p> <p>Any attempt by any person or public body to circumvent the Bill should be a necessary and proportionate measure to safeguard national security, defence and public security and it should not be an exemption that is flagrantly and easily breached. The rights of data subjects should have priority as a first principle and any person or entity or public body seeking to avoid the rights conferred on data subjects under the Bill should be subject to a higher standard of proof and should be required indicate beyond reasonable doubt why the right of the data subject should not be protected.</p>
63	<p>The reference to "undertaking" in the context of an administrative fine needs to be clarified.</p> <p>It should be clarified to include the following underlined words:</p> <p><i>"...in the case of an undertaking <u>established in Kenya</u>, up to two per centum of its annual turnover..."</i></p>

Yours faithfully

Coulson Harney LLP
per: John Syekei.

② Ameyo
Please note
FA
30/7/19

① Director
8/26/19

Google

Google Kenya
7th Floor, Purshottam Place, Westlands Road
P.O. Box 66217-00800 Westlands Tel: +254(0)20 515 4027
Nairobi-Kenya
www.google.co.ke

July 16, 2019

The Clerk of the National Assembly
P.O. Box 41842-00100
Nairobi

Dear Sir,

Re: Memorandum of views on the Data Protection Bill, 2019

I refer to the notice to members of the public to submit comments on the Data Protection Bill, 2019, which was published in the local dailies on July 10, 2019.

First, I wish to thank the National Assembly for the opportunity to contribute to the formulation of a legal framework for privacy and data protection in Kenya.

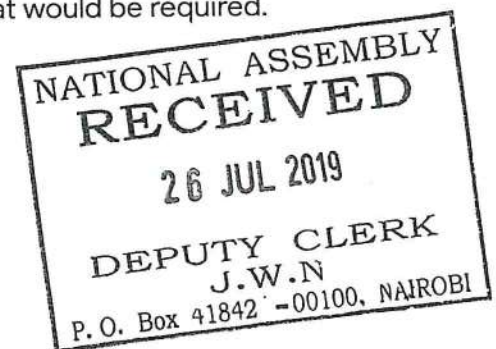
We have set out in this memorandum changes that we propose to certain segments of the bill, the rationale and the comparative provisions from Europe's General Data Protection Regulations (GDPR) of 2018.

We would be pleased to provide any further clarifications that would be required.

Most sincerely,



Michael M. Murungi
Government Affairs & Public Policy Lead, East Africa
+254 722 366 900
michaelmurungi@google.com



Issue 1. Registration of Data Controllers and Data Processors Part 18-24:

- Issue: The proposed legislation requires registration of data processors and controllers in Kenya with the Data Protection Officer including the requirement to document and keep up to date a record of processing activities. The bill contemplates the potential requirement of fees for processors to register with the state and penalties for failure to register.
- Recommendation: Strike out entirely requirement for data processors and controllers to register with the Data Protection Office
- Rationale: Data Processing and Data Controlling are not business models in the strict sense. They are activities that entities may incidentally engage in during the course of business. The requirement to have all processors and controllers would create an immense implementation burden for the Data Protection Office that would threaten to bog down the office with bureaucratic recordkeeping rather than allowing them to focus on the most serious enforcement issues. Similarly, for processors and controllers, the requirement to update external records of processing each time a change to processing occurs shifts the focus from improving privacy in areas that present the most risk to a bureaucratic exercise. The requirement for fees also raises issues as this would disproportionately affect smaller data processors and controllers.
- GDPR Equivalent Language: N/A no parallel requirement for registration in GDPR

Issue 2: Part IV - Principles and Obligations of Personal Data Protection - Erasure - Section 40

- Issue: Does not clarify that the right to erasure is based on areas where the processing is based on consent and such consent has been revoked
- Recommendation: Clarify that erasure rights are associated with where processing is occurring on the basis of consent
- Rationale: In cases where the processing is not based on consent the legitimate interest may persist even after consent of the individual has been revoked if that interest persists and continues to justify processing
- GDPR Equivalent Language: Article 17 - Right to erasure ('right to be forgotten') The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
 - (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
 - (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
 - (d) the personal data have been unlawfully processed;
 - (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
 - (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Issue 3: Part VI - Transfer of Personal Data Outside Kenya - sections 48-50

- Issue: This part bars transfer of data to another country where there is no decision by the Data Commissioner that adequate safeguards have been made for the protection of that data (adequacy decision). The omission of the word 'or' at the end of the conditions listed in this part gives the interpretation that all of those conditions listed have to be met before

data can be transferred across borders. IT appears that this may not have been the intention and that all the conditions listed are mutually exclusive.

- Recommendation:
 - Permit transfers to third country where, accounting for the transfer, all of the other requirements set forth in the legislation will continue to be met.
 - Clarify that the conditions listed in part VI are mutually exclusive. Do this by using the term "...may transfer personal data to another country **where any of the following conditions is fulfilled**" or separate the conditions with the term 'or'.
- Rationale: Requirement for adequacy decision will have undesirable impact on restricting free-flow of data. Concerns may be addressed through alternatives like binding corporate rules, codes of conduct, and certifications.
- GDPR Equivalent: Article 49 - Derogations for specific situations 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
 - (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
 - (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
 - (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
 - (d) the transfer is necessary for important reasons of public interest;
 - (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
 - (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
 - (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.
- Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

Issue 4: Notification of breach - section 43

- **Issue:** The proposed legislation requires notification to the Data Protection Officer for all

instances of breach and not just those that are likely to have an impact on the rights of the data subject.

- Recommendation: Revise to require notification only where breach is likely to result in a risk to the rights and freedoms of natural persons
- Rationale: As currently drafted this could risk inundating the Data Protection Office with notices for risks that are trivial in terms of impact on rights of individuals. A more efficient and effective means to enforcement would come from narrowing notification to those breaches likely to have an impact on individual rights and freedoms
- GDPR Equivalent: Article 33 - Notification of a personal data breach to the supervisory authority: In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Issue 5: Penalties

- Issue: The fines set forth in the proposed legislation are not clearly mapped to the likelihood or severity of the breach.
- Recommendation: Affirm that the penalties accorded for violations of data protection rules should be commensurate to the nature, gravity, and extent of the infringement
- Recommendation: Lack of clarity on how fines will be applied creates significant ambiguity for processors about how penalties will be assessed and could have a chilling effect considering the steep penalties contemplated.
- GDPR Equivalent: Article 84 - Penalties: Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive

Issue 6: Part V - Grounds for Processing of Sensitive Personal Data Sections 44-47

- Issue: Special personal data may not be processed according to all legitimate bases and exceptions provided are very narrow (e.g. religious and political institutions for their membership) even where other parties may have legitimate interests
- Recommendation: Allow processing according to all of the lawful/legitimate bases provided, provided that the unique sensitivity of the data must be accounted for in assessing the processing and necessary safeguards
- Rationale: There may be strong legitimate interests in processing of sensitive data categories that are not provided for by the close-ended list of exceptions. Where data controllers are accounting for the nature of the data in assessing whether the interests are legitimate and in determining what safeguards are required processing may still be considered lawful.
- GDPR Equivalent Language: 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
- 2. Paragraph 1 shall not apply if one of the following applies:
 - (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate. to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.



BOWMANS

RECEIVED

25 SEP 2019

LEGAL COMMITTEE SERVICES

① D/Coms
Please deal
@Juli
25/09/19

COULSON HARNEY LLP
5th Floor, West Wing, ICEA Lion Centre
Riverside Park, Chiromo Road
PO Box 10643-00100, Nairobi, Kenya
+254 20 289 9000 | +254 709 966 000
+254 20 444 8614 | +254 734 993 739
PIN No. PO51229962P | VAT No. 0191639L
www.bowmanslaw.com

Our Reference: JNS/ATI
Direct Line: +254 20 289 9000
E-mail Address: John.syekei@bowmanslaw.com
Ariana.issaias@bowmanslaw.com

② KINA
Please deal
FA
25/9/19

Your Reference: TBA
Date: 24 September 2019

The Clerk of the National Assembly
The Office of the Clerk
Main Parliament Building
Nairobi



Sent via email to: clerk@parliament.go.ke

Dear Mr Michael Sialai, EBS;

FURTHER SUBMISSIONS OF MEMORANDA: THE DATA PROTECTION BILL 2019 (the "Bill")

Further to the public hearing and stakeholders meeting held before the Departmental Committee on Communication Information and Innovation (the "**Committee**") on Tuesday 17th September 2019, stakeholders were invited to provide further comment and clarification on certain of the oral submissions presented before the Committee.

Our further submissions should be read together with our initial submissions submitted on 16 July 2019 (a copy of which is enclosed with this letter) (referred to as the "**Initial Submissions**").

No.	Section	Comments	Proposal
Thresholds for data processors and controllers			
1.	Section 18 (1) and (2)	As presented in our Initial Submissions and as discussed by various stakeholders, the current drafting of the Bill may place unnecessary obligations and administrative, financial and bureaucratic burdens on small and medium enterprises as regards the registration requirements placed on all data controllers and data processors under Part III of the Bill. In our view, registration should not be mandatory on all data controllers and processors. In making such a determination our submission is that a threshold to the registration requirement or alternatively an exemption to registration should be introduced to the Bill. This can be linked to turnover, employee numbers or according to the number of data	The Committee may consider including the following thresholds into the Bill which if met by the relevant data controller or data processor, would remove the obligation to register with the Data Commissioner: (i) The requirement to register should not apply to enterprises or organisations employing fewer than two hundred and fifty (250) employees; and/or (ii) Where the data controller or processor does not meet a certain annual turnover requirement in each relevant fiscal year. For example, in Australia the annual turnover requirement as provided for under the Privacy Act 1988 is circa KES 200 million; and/or (iii) In Nigeria, we understand that the



		<p>subjects processed.</p> <p>To reiterate, a requirement not to register does not remove the requirement to comply with the provisions of the Bill and importantly with the Bill's data protection principles.</p>	<p>basis for registration or notification under the draft legislation is per database and accordingly where a data controller processes personal data of more than 1,000 data subjects in a period of six months or more than 2,000 data subjects in 12 months, then the registration requirement applies; and/or</p> <p>(iv) in the United Kingdom, prior to the enactment of the Data Protection Act 2018, the Data Protection Act 1998 provided for certain exemptions to notification with the Information Commissioner's Office (the "ICO") which was based on the type of activities carried out by the organisation: where processing related to staff administration, account and records or where data is processed solely for the purposes of maintaining a public register.</p> <p>There were certain categories of processing which were detailed in the guidance issued by the ICO at that time and where as a result of such processing, registration was an absolute requirement: for example, processing for the purposes of canvassing political support among the electorate, advertising, accountancy, pensions administration, health administration, credit referencing and childcare; and/or,</p> <p>(v) The UK's Data Protection Act 1998 also included a two-tiered structure to notification with the ICO that was based on whether the organisation had a turnover of over KES 3,350,000,000 or more and whether the organisation had 250 or more members of staff. One of the distinctions between a Tier 1 organisation and Tier 2 organisation was the fee payable for registration and renewal (which was considerably less for Tier 1 organisations, circa KES 4,000 per annum). Note that public authorities were considered as Tier 2 organisations, regardless of the size.</p> <p>Alternatively, the Bill could introduce the following exemptions to</p>
--	--	---	--



			<p>compliance with certain provisions of the Bill:</p> <p>(i) the obligation for data controllers and data processors and their representatives to maintain a record of all processing activities under their responsibility not to apply to enterprises or organisations employing fewer than two hundred and fifty (250) employees. This exception should not apply if the processing is likely to result into a risk of rights and freedoms, occasional, or includes personal data relating to criminal convictions and offences. This exclusion has been included in the GDPR (Article 30).</p>
Obtaining of the personal data from persons other than the data subject			
2.	Section 28(2)(c)	<p>The narrow exceptions where personal data can be collected indirectly should be finite and limited. By allowing for the indirect collection of personal data where the data subject has consented to the collection from another source, limits and conflicts with the data subject rights under the Bill. In addition, it conflicts with the definition of "consent" as referred to in Section 28(2)(c) as follows:</p> <p><i>"Despite sub-section (1), personal data may be collected indirectly where...the data subject has <u>consented</u> to the collection from another source"</i></p> <p><i>"Consent" under the Bill means "any voluntary, specific and informed expression of will of a data subject to process personal data".</i></p> <p>In the context of any indirect collection of personal data, the data subject will not have given his/her consent to such collection. Moreover, the data subject will not have any information or knowledge about which data processor or data controller has obtained his/her personal data through such indirect means under the current provisions of the Bill.</p> <p>These concerns are even more</p>	<p>It is proposed that where personal data is obtained from a person other than the data subject, the data subject is required to be provided with:</p> <p>(i) the identity and the contact details of the controller or its representative;</p> <p>(ii) the contact details of the data protection officer, where applicable;</p> <p>(iii) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;</p> <p>(iv) the categories of personal data concerned;</p> <p>(v) the recipients or categories of recipients of the personal data, if any;</p> <p>(vi) where the controller intends to transfer personal data to a recipient in third country or to an international organisation, that the adequate safeguards applying to cross-border transfers have been satisfied.</p> <p>Where the origin of the personal data cannot be provided because various sources have been used, general</p>



		<p>heightened where in the time of increased exposure of data subjects to online applications and services, these consents could be hidden within lengthy terms and conditions or privacy policies which users are often obliged to accept and agree to without any further thought. Ultimately, it may result in the data subject signing their personal data away without complete knowledge and control.</p>	<p>information should be provided.</p> <p>These provisions are also contained in the GDPR, Article 14(1) and the Explanatory Notes in paragraph (61).</p>
Cross-border data transfer			
3.	Section 50 and 71(2)(g)	<p>The discretionary reservation of rights to the Cabinet Secretary to prevent the cross-border transfer of rights must be revised.</p> <p>Practically, if personal data is to be processed in Kenya, the security and integrity of the data may be at risk and may not be able to be assured a high level of technical and network security integrity.</p> <p>If Kenya is to be an international player in the technology sector, it cannot impose territorial limits on the processing of certain types of data and this cannot be at the discretion of the Cabinet Secretary. This concern has been raised on several occasions during previous public participation forums.</p>	<p>At the minimum, all derogations or revisions to the Bill must be at all times exercised in accordance with the Constitution of Kenya 2010 and with the data protection principles contained in the Bill, regardless of whether such requirement is introduced for the purposes of national security, public interest or any other strategic interests of the state, protection of revenue and so on.</p> <p>Moreover, any such proposed exercise at rights must be afforded a level of public and parliamentary scrutiny.</p>
Data relating to deceased and elderly persons			
4.	-	<p>This comment and query was raised by the Hon. Gathoni Wamuchomba, HSC regarding protection, preservation and safeguarding of data belonging to the deceased, elderly or vulnerable.</p> <p>Research into international data protection legislation revealed the following:</p> <p>(i) While the GDPR expressly states that it does not apply to data relating to a deceased person, in other jurisdictions such as France, from the year 2016 individuals could regulate the processing of their personal data after their</p>	



		<p>death.</p> <p>(ii) Individuals can give to data controllers general or specific indications about the retention, erasure, and communication of their personal data after their decease.</p> <p>(iii) In July 2018, the German Federal Court of Justice (the <i>Bundesgerichtshof</i>, BGH) jumped to similar conclusions in a case involving Facebook. According to the German judges, heirs have the right to access the Facebook accounts of their dead relatives. A social media profile is inheritable as physical goods.</p>	
--	--	--	--

Yours faithfully,

Coulson Harney LLP
Per: John Syekei.

Encl: Letter dated 16th July 2019 (Initial Submissions)



COULSON HARNEY LLP
 5th Floor, West Wing, ICEA Lion Centre
 Riverside Park, Chiromo Road
 PO Box 10643-00100, Nairobi, Kenya
 +254 20 289 9000 | +254 709 966 000
 +254 20 444 8614 | +254 734 993 739
 PIN No. POS1229962P | VAT No. 0191639L

www.bowmans.com

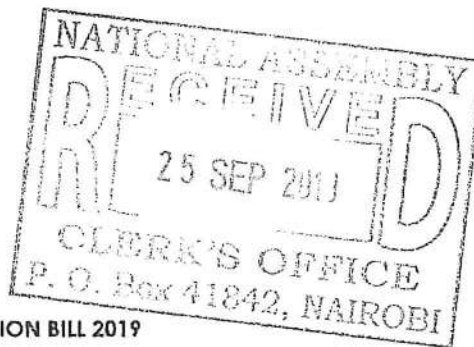
Our Reference: JNS/ATI
 Direct Line: +254 20 289 9000
 Email Address: john.sykei@bowmanslaw.com

Your Reference:
 Date: 16.07.2019

The Clerk of the National Assembly
 The Office of the Clerk
 Main Parliament Buildings
 Nairobi

Sent via email to: clerk@parliament.go.ke

Dear Mr Michael Sialai, EBS



SUBMISSION OF MEMORANDA: THE DATA PROTECTION BILL 2019

In accordance with the provisions of Article 118(1)(b) of the Constitution and Standing Order 127(3), we hereby submit our representations on the Data Protection Bill 2019 ("Bill") as published in the Kenya Gazette Supplement No. 93 (National Assembly Bills No.44) as follows:

Section	Representations
Section 4(b)(ii)	To be clarified to include the following underlined words: "(ii) <i>not established or ordinarily resident in Kenya, but processing personal data of data subjects <u>located</u> in Kenya</i> ";
Section 18(2)	The Bill should not stifle small and medium enterprises. In our view certain provisions of this Bill may place unnecessary obligations and administrative burdens on small and medium enterprises. The requirement to register with the Data Commissioner should not be mandatory on all data controllers and data processors, and in making such determination, the Data Commissioner should also consider the number of employees employed by the data controller and data processor (for example, the registration requirements should only apply where an entity employs 100 or more persons) and/or should also meet



BOWMANS

	<p>a certain turnover threshold requirement. This will create certainty across all sectors.</p> <p>Alternatively, whilst registration may be mandatory for all data controllers and processors, a helpful example is that taken from the GDPR which applies certain exemptions for small and medium sized enterprises. The GDPR requires small and medium sized organisations with fewer than 250 organisations to document processing activities in specific limited circumstances.</p> <p>In our view, certain exemptions to mandatory registration by data controllers and data processors should be taken into consideration to protect small and medium sized enterprises.</p>
28(2)(b)	<p>To be clarified to include the following underlined words;</p> <p><i>"the data subject has deliberately <u>and manifestly</u> made the data public"</i></p>
28(2)(c)	<p>This section should be deleted.</p> <p>The narrow exceptions where personal data can be collected indirectly should be finite and limited. By allowing for the indirect collection of personal data where the data subject has consented to the collection from another source, limits and conflicts with the data subjects rights under Section 25(g), 26, 35, 36, 38, 39 and 40 of the Bill. The data subject loses control of his/her personal data which should not be the intention of the Bill and deprives the data subject of his or her remedies under the Bill.</p>
48(a)	<p>The Data Commissioner should establish at the outset what the "appropriate safeguards" are to be applied in the context of any cross-border transfer. There is no clarity as to whether or not this requires that certain technical and security measures must be in place or what the minimum threshold should be prior to transfer out of Kenya.</p>
48(a)	<p>To be amended to include the following underlined wording:</p> <p><i>"the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data <u>and on condition that enforceable data subject rights and effective legal remedies for data subjects are available"</u></i></p>



BOWMANS

50 and 71 (2)(g)	<p>This should be deleted.</p> <p>If personal data is to be processed in Kenya, the security and integrity of the data may be at risk and international data controllers may not be able to be assured of the level of technical and network security integrity. Kenya may not also be able to guarantee an international standard of systems infrastructure.</p> <p>If Kenya is to be an international player in the technology sector, it cannot impose territorial limits on the processing of certain types of data which will be at the discretion of the Cabinet Secretary. This concern has been raised on several occasions during previous public participation forums.</p>
30(1)(v), 30(1)(vii) and 51(2)(b)	<p>There should be strict limits on the avoidance of the application of the Bill for national security reasons, by any person in the public interest, national security or public order.</p> <p>Any attempt by any person or public body to circumvent the Bill should be a necessary and proportionate measure to safeguard national security, defence and public security and it should not be an exemption that is flagrantly and easily breached. The rights of data subjects should have priority as a first principle and any person or entity or public body seeking to avoid the rights conferred on data subjects under the Bill should be subject to a higher standard of proof and should be required indicate beyond reasonable doubt why the right of the data subject should not be protected.</p>
63	<p>The reference to "undertaking" in the context of an administrative fine needs to be clarified.</p> <p>It should be clarified to include the following underlined words:</p> <p><i>"...in the case of an undertaking <u>established in Kenya</u>, up to two per centum of its annual turnover.."</i></p>

Yours faithfully

Coulson Harney LLP
per: John Syekei.

Ref:001/02

23rd September, 2019.

The Clerk National Assembly,
P. O. Box 41842-00100, Nairobi.

① D/Coms
Please deal.
Gali
24/09/19

Dear Sir,

Re: SUPPLEMENTARY MEMORANDUM.

The Technology Service Association of Kenya welcomes the Data Protection Bill as a step towards the realization of right to privacy in Kenya. TESPOK has reviewed the proposed law and submitted supplementary comments of the bill following our engagement with the National Assembly Committee on ICT on 17th September 2019.

Kindly find the attached supplementary memorandum on the Data Protection Bill for your consideration.

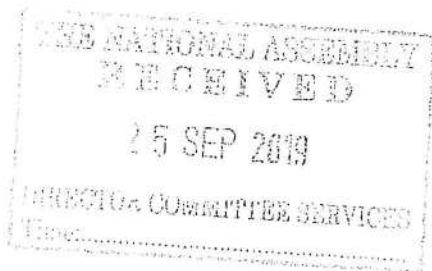
TESPOK is greatly encouraged by the development of this legislative and regulatory framework.

Yours Faithfully,



Fiona Asonga.
Chief Executive Officer.

② KINA
Please deal
FA
25/9/19





*To be the Voice of Technology influencing
Policy, Direction and Development in the Industry*

SUPPLEMENTARY MEMORANDUM

A. INTRODUCTION

This is a review of the Data Protection Bills currently under consideration by the National Assembly. The National Assembly Bill published the Ministry of ICT's version and read it a first time in the National Assembly. It now stands committed to the Departmental Committee on Communication, Information and Innovation of the National Assembly which is conducting public participation on the Bill. In this regard, the National Assembly through the Clerk has invited members of the public to make its submissions on the same vide a Notice published on 10th July, 2019.

We have had an engagement with the committee on the 17th September 2019 where we agreed to provide further details on key cross-cutting issues as follows:

B. OVERVIEW OF THE DATA PROTECTION BILL.

	NATIONAL ASSEMBLY BILL	PROPOSAL	JUSTIFICATION
1.	Establishment/Designation of National Data Protection Authority (DPA)		
	<ul style="list-style-type: none">Qualifications of Data Commissioner A person shall be qualified for appointment as the Data Commissioner if that person – a) Holds a degree from a University recognised	It would be important for the Data Commissioner be able to demonstrate:	

	<p>in Kenya in</p> <ul style="list-style-type: none"> i. Data Science ii. Law iii. Information Technology; or iv. Any other related field <p>b) Has knowledge and relevant experience of not less than ten years and</p> <p>c) Meets the requirements of Chapter Six of the Constitution.</p> <ul style="list-style-type: none"> • Established an independent office of the Data Protection Commissioner as a state office. To be recruited via competitive process by the Service Commission and appointed by the Cabinet Secretary via Gazette Notice for a single term of 6 years. May resign from office by notice in writing to the president. (S11b) 	<ul style="list-style-type: none"> - An understanding of Information Technology systems and data handling processes both manual and automated - Knowledge of sector specific data handling practises <p>Support having and Independent office of the Data Protection Commissioner as a state office. <i>We recommend streamlining of appointment and resignation authorities. Same authority to appoint and receive resignation notice.</i></p>	<p>The data to be considered should be both manual and automated data</p> <p>This will ensure the streamline of data handling legislation for various sectors.</p> <p>To align with global best practise</p>
<p>2.</p>	<p>Registration of Data Controllers and Processors</p> <ul style="list-style-type: none"> • Data controllers/processors required to register. (S18) • Option to appoint a data protection officer to ensure compliance with Act (S 24) 	<ul style="list-style-type: none"> • <i>We recommend the requirement for registration be set within a set threshold for controllers/processors dealing with sensitive/special personal data.</i> • <i>We also recommend an additional clause that will list sensitive/special personal data as information relating to</i> <ul style="list-style-type: none"> i. <i>the race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, age, physical,</i> 	<ul style="list-style-type: none"> • The scope of those who have to register will be restricted to the level of sensitivity of the data being handled • To Align with Access to Information Act and provide clarity on what constitutes sensitive personal data so that it is handled appropriately

		<p><i>psychological or mental health, disability, religion, belief, culture, language, birth and death of an individual.</i></p> <ul style="list-style-type: none"> ii. <i>Identification and Biometric details</i> iii. <i>Personal contact details</i> iv. <i>Child criminal records</i> 	
<p>3.</p>	<p>Grounds for processing of sensitive personal data</p> <ul style="list-style-type: none"> • Principles of data protection apply to processing of sensitive personal data. (S44) • Time frame for storing sensitive data 	<ul style="list-style-type: none"> • We recommend that as soon as an individual is pronounced dead entities handling their data will apply the principles of data protection that deal with sensitive personal data. • To align to existing laws that require data to be stored for various periods for the different sectors. 	<ul style="list-style-type: none"> • This provides for sanity in addressing succession issues to enable only registered next of kin to handle the information with relevant entities
<p>4.</p>	<p>Transfer of personal data outside Kenya</p> <ul style="list-style-type: none"> • Cross border data transfers only allowed where controller/processor has given DPA proof of adequate safeguards, where data subject consents or transfer is necessary for contract performance, overriding public interest, controller/processor is pursuing compelling legitimate interest. (S48 &49). Burden of proof is on controller/processor 	<p>In support of allowing cross boarder data transfer so long as there is proof of adequate safeguards being in place. The proof of the safeguards in place lays in the contracts and service level agreements the various service providers have with their respective customers.</p>	<ul style="list-style-type: none"> • The digital economy is dependent on cross boarder interactions that require data to flow across countries and regions.



*To be the Voice of Technology influencing
Policy, Direction and Development in the Industry*

SUPPLEMENTARY MEMORANDUM

A. INTRODUCTION

This is a review of the Data Protection Bills currently under consideration by the National Assembly. The National Assembly Bill published the Ministry of ICT's version and read it a first time in the National Assembly. It now stands committed to the Departmental Committee on Communication, Information and Innovation of the National Assembly which is conducting public participation on the Bill. In this regard, the National Assembly through the Clerk has invited members of the public to make its submissions on the same vide a Notice published on 10th July, 2019.

We have had an engagement with the committee on the 17th September 2019 where we agreed to provide further details on key cross-cutting issues as follows:

B. OVERVIEW OF THE DATA PROTECTION BILL

	NATIONAL ASSEMBLY BILL	PROPOSAL	JUSTIFICATION
1.	Establishment/Designation of National Data Protection Authority (DPA)		
	<ul style="list-style-type: none">Qualifications of Data Commissioner A person shall be qualified for appointment as the Data Commissioner if that person – a) Holds a degree from a University recognised	It would be important for the Data Commissioner be able to demonstrate:	

	<p>in Kenya in</p> <ul style="list-style-type: none"> i. Data Science ii. Law iii. Information Technology; or iv. Any other related field <p>b) Has knowledge and relevant experience of not less than ten years and</p> <p>c) Meets the requirements of Chapter Six of the Constitution.</p> <ul style="list-style-type: none"> • Established an independent office of the Data Protection Commissioner as a state office. To be recruited via competitive process by Public Service Commission and appointed by the Cabinet Secretary via Gazette Notice for a single term of 6 years. May resign from office by notice in writing to the president. (S11b) 	<ul style="list-style-type: none"> - An understanding of Information Technology systems and data handling processes both manual and automated - Knowledge of sector specific data handling practises <p>Support having and Independent office of the Data Protection Commissioner as a state office. <i>We recommend streamlining of appointment and resignation authorities. Same authority to appoint and receive resignation notice.</i></p>	<p>The data to be considered should be both manual and automated data</p> <p>This will ensure the streamline of data handling legislation for various sectors.</p> <p>To align with global best practise</p>
<p>2.</p>	<p>Registration of Data Controllers and Processors</p> <ul style="list-style-type: none"> • Data controllers/processors required to register. (S18) • Option to appoint a data protection officer to ensure compliance with Act (S 24) 	<ul style="list-style-type: none"> • We recommend the requirement for registration be set within a set threshold for controllers/processors dealing with sensitive/special personal data. • We also recommend an additional clause that will list sensitive/special personal data as information relating to <ul style="list-style-type: none"> i. the race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, age, physical, 	<ul style="list-style-type: none"> • The scope of those who have to register will be restricted to the level of sensitivity of the data being handled • To Align with Access to Information Act and provide clarity on what constitutes sensitive personal data so that it is handled appropriately

		<p><i>psychological or mental health, disability, religion, belief, culture, language, birth and death of an individual.</i></p> <p>ii. <i>Identification and Biometric details</i> iii. <i>Personal contact details</i> iv. <i>Child criminal records</i></p>	
3.	<p>Grounds for processing of sensitive personal data</p> <ul style="list-style-type: none"> Principles of data protection apply to processing of sensitive personal data. (S44) Time frame for storing sensitive data 	<ul style="list-style-type: none"> We recommend that as soon as an individual is pronounced dead entities handling their data will apply the principles of data protection that deal with sensitive personal data. To align to existing laws that require data to be stored for various periods for the different sectors. 	<ul style="list-style-type: none"> This provides for sanity in addressing succession issues to enable only registered next of kin to handle the information with relevant entities
4.	<p>Transfer of personal data outside Kenya</p> <ul style="list-style-type: none"> Cross border data transfers only allowed where controller/processor has given DPA proof of adequate safeguards, where data subject consents or transfer is necessary for contract performance, overriding public interest, controller/processor is pursuing compelling legitimate interest. (S48 &49). Burden of proof is on controller/processor 	<p>In support of allowing cross boarder data transfer so long as there is proof of adequate safeguards being in place. The proof of the safeguards in place lays in the contracts and service level agreements the various service providers have with their respective customers.</p>	<ul style="list-style-type: none"> The digital economy is dependent on cross boarder interactions that require data to flow across countries and regions.

Chairperson: Hon. Florence Kajuju, MBS
Vice-Chairperson: Mr. Washington Sati
Commissioner: Mrs. Lucy Ndung'u, EBS, HSC



THE NATIONAL ASSEMBLY
COMMISSION ON ADMINISTRATIVE JUSTICE
"Office of the Ombudsman"
27 SEP 2019
DIRECTOR COMMITTEE SERVICES

Our Ref: CAJ/LEG/34

① Dlcoms
Please deal.

25th September 2019

Mr. Michael Sialai, EBS
Clerk of the National Assembly
First Floor, Parliament Buildings
P. O. Box 41842 – 00100
NAIROBI.

Handwritten signature

② KINA

NATIONAL ASSEMBLY
MAIN RECORDS UNIT
25 SEP 2019
RECEIVED (4)
NAIROBI - KENYA

please deal

③ CHENWANG
Please note
FA
30/9/19

FA
30/9/19

Dear Mr. Sialai

RE: SUBMISSIONS ON DATA PROTECTION BILL 2019

Kindly receive warmest compliments from the Commission on Administrative Justice (Office of the Ombudsman).

Further to our letter dated 23rd September 2019 submitting the Commission's views on the Data Protection Bill, 2019.

We hereby forward additional comments as directed by the Departmental Committee on Communication, Information and Innovation during the meeting held on Monday, 23rd September 2019.

We thank you for your continued support and assure you of our highest regards.

Yours sincerely,

HON. FLORENCE KAJUJU, MBS
CHAIRPERSON OF THE COMMISSION

NATIONAL ASSEMBLY
RECEIVED
26 SEP 2019
CLERK'S OFFICE
P. O. Box 41842, NAIROBI



THE COMMISSION ON ADMINISTRATIVE JUSTICE

"Office of the Ombudsman"

REVIEW OF LEGISLATIVE PROPOSALS

THE DATA PROTECTION BILL, 2019 (NATIONAL ASSEMBLY BILLS NO. 44)

INTRODUCTION

The National Assembly invited the Commission on Administrative Justice (hereinafter the "Commission") to make oral submissions on the above bill to the Departmental Committee on Communication, Information and Innovation on 23rd September, 2019 at Windsor Hotel, Nairobi.

The Commission tabled its memorandum and arising from the presentation, the Committee directed the Commission to submit additional information on matters canvassed during the meeting.

Therefore, the Commission further submits as hereunder:

1. Legislative Guarantee of Independent Oversight in the Implementation of a Fundamental Right

The right to protection of personal data provided for under the proviso of privacy stipulated in **Article 31 of the Constitution** is a fundamental right recognized under the bill of rights in **Chapter 4 of the Constitution**. The fact that this right is therefore sacrosanct and must be highly safeguarded cannot be gainsaid.

In its earlier memorandum, the Commission guided by international best practice had substantially enumerated why the oversight of the implementation of this right ought to be given to an independent institution. In order to ensure that the Office of the Data Commissioner is independent, impartial and most importantly not subservient to the Executive, the Commission had gone further to emphasize that the institution tasked with

2. Leverage on Existing Implementation Framework

With the enactment of the Access to Information (ATI) Act in 2016 and the subsequent appointment of the current commissioners in August 2018, the Commissioners set out the structures towards the operationalization of the ATI Act by:

- i. designating one of its commissioners as an "Access to Information Commissioner". This Commissioner, as provided under **section 20(3)** of the ATI Act is specifically responsible for performing the functions assigned to the CAJ under the (ATI) Act.
- ii. designating officers to specifically handle requests on access to information who have further been trained on the same.
- iii. Equipping regional offices and its officers to handle ATI requests, reviews and redress such that Kenyans do not have to physically come to the Commission's head office in Nairobi.
- iv. The Commission in the proposed Strategic Plan (2019-2023) is introducing a strategic objective on access to information which was not there in the previous strategic plan and which creates structures of implementing the ATI function from the national to the grassroots level. With the launch of this new strategic plan, the CAJ will approach the National Treasury for additional budgetary allocation through the supplementary budget as advised by the latter. In addition, the CAJ has been directed by the National Assembly Justice and Legal Affairs Committee to strategize on the actualization of the ATI Act.
- v. As required under the ATI Act, the CAJ has ensured that all public institutions at both levels of government have appointed Information Access Officers and furnished CAJ with their contacts for ease of coordination and collaboration. These Officers have been sensitized and trained on their obligations under the ATI Act.
- vi. trained journalists on access to information and proactive disclosure and how it aids in investigative journalism while focusing on their role in ensuring the respect for the right to information and the protection of personal data.
- vii. actively sensitizing and educating members of the public and its other stakeholders on its social media platforms.

- viii. developed and published information, communication and education (IEC) materials to guide public officers on proactive disclosure and aid in public education namely:
- Handbook on Best Practices on Implementation of Access to Information in Kenya, 2018
 - A Guide on Proactive Disclosure for Public Entities at National and County Government Level in Kenya, 2018
 - Simplified Version of the Access to information Act

In order to mainstream ATI within public institutions, CAJ championed for the inclusion of an indicator on implementation of the Act under Performance Contracting guidelines. As a result, Ministries, Departments and Agencies (MDAs) submit quarterly reports to the Commission on their compliance with the ATI Act. CAJ is then statutorily required to table an annual report on the same to Parliament as well as the Cabinet Secretary and has been doing so diligently.

To operationalize the ATI Act at the county level, the County Governments Act, 2012 in **section 96(3)** requires county governments to domesticate the ATI Act. The Commission therefore carried out a survey assessing public institutions on the level of compliance with the requirements of the ATI Act. The findings of the survey were wanting which prompted the CAJ to issue a circular (CAJ Circular No. 1 of 2019 signed by CAJ Chairperson) to all public entities listing the information that should be proactively disclosed as identified by the ATI Act.

The need for regulations propelled the CAJ commissioners to spearhead the development of regulations under **section 25** of the ATI Act by constituting a multi-agency taskforce chaired by the CAJ Access to Information Commissioner and with representation from the Ministry of ICT, Kenya Law Reform Commission, National Council of Persons Living with Disability and other Commission staff. The Commission is planning to hold a series of stakeholder engagement and public participation on the draft regulations before the same is presented to parliament. Notably, the CAJ is currently in consultation with the relevant parliamentary committees in a bid to fast track the passage of these regulations.

Given that the right to access to information is a facilitative right, the Commission's mandate on oversight and enforcement of the ATI Act is crucial not only to the realization of the President's "Big Four" Agenda and Kenya's Vision 2030 but also implementation of Kenya's international obligations under SDG 16 on peace, justice and strong institutions. In order to ensure the country's compliance with its international treaty obligations relating to the right of access to information and protection of personal data, the CAJ has established mutual cooperation and strategic partnerships with local and international bodies. Notably, the Commission is an accredited member of the International Conference of Information Commissioners (ICIC). The Commissioner in charge of ATI at the Commission is a Co-convenor and a member of the OGP Steering Committee¹.

It is worthy note that the Commission also has funds albeit minimal, some of which has been separately allocated for the discharge of functions which has enabled CAJ achieve the above highlighted achievements.

With these concrete and firm structures as highlighted above, CAJ has made remarkable progress on implementation of access to information and proactive disclosure by public entities in particular. And indeed the recommendation by CIC to anchor ATI within CAJ was well informed and therefore the Commission proposes that the enforcement of data protection be anchored within the CAJ. In light of this, the Commission proposes the attached structure for the Office of the Data Commissioner, herein marked as *annexture 4*.

Consequential Amendments to Existing Legislation

In the event Parliament in its wisdom, gives the data protection function to the CAJ, some consequential amendments will follow as a matter of fact.

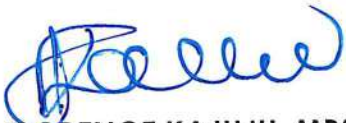
- i. This is in respect to the quorum of the commissioners as well as the qualifications for appointment as a commissioner at CAJ in **section 9** and **10** of the CAJ Act, 2011 respectively. **Section 9** of the CAJ Act

¹ Open Governance Partnership (OGP) is an initiative that brings together government reformers and civil society leaders to create action plans that make governments more inclusive, responsive and accountable.

should be amended to make provision for the Office of the Data Commissioner by increasing the number of the commissioners which must also not be even in number for ease in voting and decision making.

- ii. Given that data protection is a technical function, **section 10** on the qualifications should be amended to make provision for knowledge in data science and information technology as proposed under **clause 7** of the Data Protection Bill. A caveat must also be introduced to the effect that the selection panel must ensure that one of the commissioners is well versed and possesses expertise in data science and information technology.
- iii. In addition, the selection panel responsible for the recruitment of CAJ commissioners in **section 11(2)** needs to include representation of the Ministry responsible for matters relating to ICT given that data protection and Access to information have a close relationship with the overall function of the Ministry.

I hereby submit.



HON. FLORENCE KAJUJU, MBS
CHAIRPERSON OF THE COMMISSION



Commission for the Implementation of the Constitution

Utekelezaji wa katiba, jukumu la wote

PARKLANDS PLAZA, CHIROMO LANE,
WESTLANDS

P.O. BOX 48041 - 00100, NAIROBI

Tel. No: 0202462374, 0708326404,

Email: manager@cickenya.org, chairperson@cickenya.org, Website: www.cickenya.org

Ref No: CIC/3/32/Vol. 1

20th September 2012

Mr. Otiende Amollo
Chairperson
Commission on Administrative Justice
Prime Minister's Office Building
Harambee Avenue
NAIROBI



Dear *Chair,*

**RE: ROUNDTABLE MEETING ON THE FREEDOM OF INFORMATION BILL
2012 AND THE DATA PROTECTION BILL 2012**

Reference is made to the above subject matter.

This is to forward copies of the above draft Bills on Articles 35 (on right to access information) and 31 (right to privacy) for your consideration. The Bills were forwarded to the Commission for the Implementation of the Constitution (CIC) in July 2011 and have been processed in consultation with various stakeholders including your office.

The bills were finally considered by the CIC at plenary held on September 4th - 5th 2012 which resolved to give the mandate of monitoring the provisions of these laws to the Commission on Administrative Justice. As you are aware, the constitutional responsibility for monitoring the implementation of human rights lies, in the long run on the Article 59 Commissions. We have considered the state responsibility in respect of Article 35 and 31 and are persuaded that the best institution to oversee these laws is the CAJ rather than a statutory body as suggested by the Ministry of Information and Communication.

We have scheduled a roundtable meeting with the Attorney General (AG), Kenya Law Reform Commission (KLRC), the Ministry of Information and Communication and your office to finalize on the bills, to be held on a **Monday 1st - Tuesday 2nd October 2012** at CIC boardroom from 9:00 am each day.

We would like to invite you to participate in the roundtable discussions where you may wish to make your comments on the additional responsibilities added to the CAJ.

Kindly confirm your attendance with Christine Njeru at cnjeru@cickenya.org or **0721827674**.

Yours



Charles Nyachae
CHAIRPERSON



Commission for the Implementation of the Constitution

Utekelezaji wa katiba, jukumu la wote

CIC AUDIT REPORT ON THE FREEDOM OF INFORMATION BILL 2012 AND DATA PROTECTION BILL 2012.

The Commission on the Implementation of the Constitution (CIC) received the Freedom of Information Bill and Data Protection Bill in July 2011. The Bills as received had been consolidated prior to the promulgation of the Constitution and therefore required to be realigned to the provisions of the Constitution of Kenya 2010. CIC appointed to focus on the bills in tandem as the two bills are greatly dependant on each other and further opted to prioritize the bills given their impact. This was undertaken bearing in mind that the bills are among those scheduled for enactment within five years.

CIC held an internal audit of the bills before engaging the services of a consultant in August 2011 to work with CIC in auditing the bills to ensure compliance with the letter and spirit of the Constitution as well as the provisions of international instruments which subject to article 2 of the Constitution form part of the laws of Kenya. CIC also held a meeting with the Ministry of Information and Communication to discuss some of the concerns arising from the initial audit.

CIC held a number of stakeholder consultations which brought together representatives from Government Ministries and Departments, Non-Governmental Organizations and academia to deliberate upon the provisions of the Bills. In one of the consultations the stakeholders were advised that the Freedom of Information network had worked on a separate Freedom of Information Bill and the meeting resolved that the two bills should be consolidated, which was subsequently undertaken. In addition, the stakeholders noted the need for further consultations on the Data Protection Bill due to the complexity of the content, and as a resolve the Ministry of Information and Communication developed an explanatory memo to guide stakeholders.

The stakeholder consultations were followed by a plenary held on 4th and 5th September 2012 to review the Bills to ensure compliance with the letter and spirit of the Constitution.

KEY ISSUES ARISING FROM THE FREEDOM OF INFORMATION AND DATA PROTECTION BILLS:

1. Oversight Mechanism under the Freedom of Information and the Data Protection Bills 2012:

Following extensive consultations as to the most effective mechanism to oversee and ensure effective realization of the right to privacy (article 31) and the right of access to information (article 35), CIC plenary resolved that that articles 31 and 35 relate to the rights under the Bill of Rights whose oversight mechanism is as provided under article 59 of the Constitution. After assessment of the mandates of the different Constitutional Commissions established under article 59 the plenary concluded that the Commission on Administrative Justice (hereinafter 'Commission'), being a constitutional commission, was the most suitable entity to carry out these functions. The plenary noted that not only is there a constitutional duty to enforce these rights, but also that the Commission on Administrative Justice is also assured of funding and infrastructural accommodations to easily and readily enforce the provisions of the two laws.

It was also noted that the membership of the Commission is subject to the most penetrating scrutiny by the National Assembly. The Commission was also established for among other reasons to guarantee the constitutional rights of citizens to fair administrative action as provided in article 47 of the Constitution and equally, concerns raised as to the oversight mechanism being a specialized entity can always be catered for under the mandate of the Commission wherein the Commission has constitutional powers to get this specialized expertise within its own internal mechanisms.

Moreover, under comparative and international practice, the constitution's supremacy in article 2 (5) and (6) provides that "the general rules of international law" and "any treaty or convention ratified by Kenya shall form part of the law of Kenya". As such, international best practice relating to FOI oversight indicates that there are four main types of oversight bodies:

- (a) Office of the Information Commissioner (as in the UK, Ireland, Slovenia, Serbia and Hungary). In Hungary, both the FOI and Data Protection functions are combined in one office-Data Protection and Information commissioner
- (b) Commission or Institute (Mexico, Portugal)
- (c) Ombudsman is given the right of oversight (Sweden, Norway, Bosnia, New Zealand)
- (d) Other body given the oversight of the right (South Africa, Turkey)

It is pertinent to note that international law does not oblige states to create an oversight body for freedom of information but there are collateral obligations that implicitly suggest the need for such a body.

- (i) The Human Rights committee in General Comment no 34 on article 19 imposes an affirmative obligation to enact the necessary procedures whereby one may gain access to information.

(ii) This obligation was further enunciated by the Inter American Court on Human Rights in *Claude Reyes et al vs. Chile* where it was found that the obligation "includes establishing an appropriate administrative procedure for processing and deciding requests for information.

(iii) The Council of Europe in a 2002 recommendation on access to official documents stated an applicant should have access to a review procedure before a court of law or another independent and impartial body established by law.

(iv) Under the 2002 Declaration of Principles on Freedom of Expression in Africa, a refusal to disclose information shall be subject to appeal to an independent body and/or the Courts.

Further in providing for the Commission as the suitable mechanism to receive and redress complaints in cases where the right is violated, the Bill further provides for appeal of the decision of the Commission to the High Court of Kenya.

2. Enhancing Access to Information

The Freedom of Information Bill 2012 was duly redrafted to ensure that emphasis on the bill is on the right of access to information as opposed to the oversight mechanism as was initially drafted.

In addition the Bill was reviewed to ensure that access to information relates not only to information held by public entities but also private individuals.

3. Limitation to the right to privacy and the duty to notify.

The Data Protection Bill 2012 further limits the right to privacy under article 31 to information that is in the public domain.

The Bill further emphasizes upon the need for an agency collecting personal information to duly notify the data subject of among other issues the purpose of its collection and the intended recipients.

Concluding Remarks:

As mentioned above, in review of the bills, CIC ensured that the Bills complied with the letter and spirit of the Constitution. In addition, CIC also ensured that the Bills were not in conflict with other existing legislation including the recently enacted National Intelligence Service Act 2012.

ARRANGEMENT OF CLAUSES*Clause***PART I – PRELIMINARY**

- 1— Short title.
- 2— Interpretation.

PART II – PERSONAL INFORMATION PROTECTION PRINCIPLES

- 3— Objects of this Act.
- 4— Principles of data protection.
- 5— Right to protection of privacy.
- 6— Limitation.
- 7—Data processing.
- 8—Collection of personal information.
- 9— Exemption.
- 10— Duty to notify.
- 11— Protection and security of personal information.
- 12— Access to information.
- 13—Correction of information.
- 14— Use of information.
- 15— Storage of information.
- 16— Misuse of information.
- 17— Commercial use of data
- 18— Use of unique identifiers.
- 19— Interference with personal information

**PART III – CONFERMENT ON THE COMMISSION OF OVERSIGHT AND
ENFORCEMENT FUNCTIONS AND POWERS**

20— Role of the Commission on Administrative Justice.

21— Functions of the Commission.

PART IV- COMPLAINTS, PROCEEDINGS AND SETTLEMENTS

22— Inquiry into complaints.

23— Proceedings on complaints

24— Settlement of complaints.

PART V- POWERS AND REMEDIES

25— Powers and Remedies of the Board on the complaint

26— Damages.

PART VI – MISCELLANEOUS PROVISIONS

27— Protection against certain actions.

28— Offences.

29— Regulations.

THE PERSONAL DATA PROTECTION BILL, 2012

A Bill for

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to regulate the collection, retrieval, processing, storing, use and disclosure of personal data and for connected purposes

PART I— PRELIMINARY

Short title. 1. This Act may be cited as the Personal Data Protection Act, 2012.

Interpretation. 2.(1) In this Act, unless the context otherwise requires —

“agency” includes public entities and private bodies;

"Cabinet Secretary" means the Cabinet Secretary responsible for information and communications;

“Commission” means the Commission on Administrative Justice established by section 3 of the Commission on Administrative Justice Act, 2011;

No....of 2012.

" Court" means the High Court or any other court with jurisdiction under any law to adjudicate over matters relating to data protection;

"data" means information which—

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

(d) where it does not fall under paragraph (a), (b) or (c), forms

part of an accessible record;

- (e) is recorded information held by public entity and does not fall within any of paragraphs (a) to (d);

"data controller" means a person who, either alone or with others, controls the contents and use of personal information;

"data equipment" means equipment for processing data;

"data processor" means a person who processes personal information on behalf of a data controller but does not include an employee of a data controller who processes such information in the course of his or her employment;

"data subject" means an individual who is the subject of personal information;

"disclosure", in relation to personal information, includes the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed;

"person" has the meaning assigned to it in Article 260 of the Constitution;

"personal information" means information about a person, including, but not limited to —

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical 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 or contact details including telephone numbers of the individual;
- (e) 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 to a third party;
- (f) a person's views or opinions about another person ; and
- (g) any information given in support or relation to a grant, award or prize proposed to be made to an individual;

"processing" means performing automatically logical or arithmetical operations on data and includes—

- (a) extracting any information constituting the data; and
- (b) in relation to a data processor, the use by a data controller of data equipment in the possession of the data processor and any other services provided by him for a data controller, but does not include an operation performed solely for the purpose of preparing the text of documents;

"public entity" means— —

- (a) any public office, as defined in Article 260 of the Constitution; or
- (b) any entity performing a function within a commission, office, agency or other body established under the Constitution;

No....of....

"record" in relation to an agency, means a document or any other source of information compiled, recorded or stored in written form, on film, by electronic process or in any other manner or a record made or kept by a person acting under the authority of law or exercising other official function;

“secretary” has the meaning assigned to it by section 2 of the Commission on Administrative Justice Act, 2011;

**PART II – OBJECTS AND PERSONAL INFORMATION
PROTECTION PRINCIPLES**

Objects of this Act.

3. The objects of this Act include to —

- (a) give effect to the right of every person to privacy as provided under Article 31 (c) and (d) of the Constitution;
- (b) protect a person’s right to privacy for their personal data with regard to their private and family life subject to this Act; and
- (c) safeguard personal data from use or disclosure which is not in the interest of the data subject except in terms of this Act.

Principles of data protection.

4.(1) The principles of data protection include that —

- (a) information is collected or stored if it is necessary for or directly related to a lawful, explicitly defined purpose and does not intrude upon the privacy of the data subject to an unreasonable extent;
- (b) information is collected directly from and with the consent of the data subject;
- (c) data subject is informed of the purpose of any collection of information and of the intended recipients of the information, at the time of collection;
- (d) information is not kept for any longer than is necessary for achieving the purpose for which it was collected;
- (e) information is not distributed in a way incompatible with the purpose for which it was collected that is with direct consent and subject to any notification that would attract objection;
- (f) reasonable steps are taken to ensure that the information

processed is accurate, up to date and complete;

(g) appropriate technical and organizational measures are taken to safeguard the data subject against the risk of loss, damage, destruction of or unauthorized access to personal information; and

(h) data subjects are allowed a right of access to their personal information and a right to demand correction if such information turns out to be inaccurate.

Right to protection of privacy.

5. Every person has a right to privacy with respect to their personal data relating to their private and family life.

Limitation.

6. (1) The right to privacy may be limited in order to safeguard overriding legitimate interests of another person and the limitation must be carried out using the method that is least intrusive to the data subject.

(2) The right to privacy is presumed to be lost due to the general availability of the data being in the public domain

Data processing.

7. Where personal data concerning a data subject is destined for automated or manual processing the data subject shall have the right on request to the following—

- (i) information on the person processing data concerning him or her;
- (ii) place of origin of the data;
- (iii) use of the data collected;
- (iv) any other person to whom the data is transmitted;
- (v) rectification of incorrect data and the right to erasure of illegally processed data.

Collection of personal information.

8. (1) Personal information shall not be collected, stored or used by a person—

(a) by unlawful means; or

(b) by means that, in the circumstances, intrude to an unreasonable extent, upon the personal affairs of the

data subject except in terms of this Act or any other written law.

(2) A data controller shall, with respect to personal information kept by him or her, comply with the following limitations —

(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

(3) An agency which collects personal information may collect the information directly or indirectly from the data subject concerned.

Exemptions.

9. Notwithstanding the provisions of section 8 (2), , an agency shall not be held to have collected the information unnecessarily where it can demonstrate on reasonable grounds that —

(a) the information is publicly available information;

(b) the data subject authorised collection of the information from someone else;

(c) non-compliance would not prejudice the interests of the data subject;

(d) non-compliance is necessary —

(i) to avoid prejudice to the maintenance of law and order by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) or the enforcement of a law imposing a pecuniary penalty;

(iii) for the protection of the public revenue and property;

(iv) for the conduct of proceedings before any Court or the Commission, being proceedings that have been commenced or are reasonably

in contemplation; or

- (v) for purposes of exemptions set out in the Freedom of Information Act;
- (e) compliance would prejudice the purposes of the collection;
- (f) compliance is not reasonably practicable in the circumstances of the particular case;
- (g) the information —
 - (i) will not be used in a form in which the data subject is identified; or
 - (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the data subject; or
- (h) the collection of the information is in accordance with an authority granted under this Act or any other written law.

Duty to notify.

10. (1) Where an agency collects personal information directly from a data subject, the agency shall take such steps as are in the circumstances reasonable to ensure that the data subject is aware of —

- (a) the fact that the information is being collected;
- (b) the purpose for which the information is being collected;
- (c) the intended recipients of the information;
- (d) the name and address of the agency that is collecting the information and the agency that will hold the information and whether or not any other agency will receive the information;

(2) A person who holds personal information shall, if so requested by the data subject or on his or her own initiative, take steps to correct, or delete untrue or misleading information.

(3) A denial of a request made under subsection (1) shall be in writing disclosing the grounds for the denial of the request.

(4) A request for correction may be denied on the basis that the request does not amount to a correction.

(5) Where an agency that holds personal information denies a request by the data subject to correct, or delete untrue or misleading, information, the agency shall, if so requested by the data subject, attach to the information that it holds, in such a manner that it will be read with the information that it holds, a statement provided by the data subject making the request.

(6) Where the agency has taken steps under subsection (5), the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(7) Where an agency receives a request made pursuant to subsection (1), the agency shall inform the data subject of the action taken as a result of the request.

Use of information.

14. An agency that holds personal information shall not use the information without taking reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Storage of information.

15. An agency that holds personal information shall not keep the information for longer than is required for the purposes for which the information may lawfully be used.

Misuse of information.

16. An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose.

Commercial use of data.

17. A person shall not use for commercial purposes personal information obtained pursuant to the provisions of this Act unless—

- (a) given express consent by data subject; or
- (b) authorised to do so under any other written law.

Use of unique identifiers.

18. (1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

*

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those two agencies are associated persons within the meaning of the Income Tax Act.

Chapter 470

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those

Interference with personal information.

19. For the purposes of this Act, a person who interferes with personal information of a data subject or practices breaches in relation to personal information that relates to the data subject commits an offence and is liable, on conviction, to a fine not exceeding Kshs. 100,000 and to a term of imprisonment not exceeding two years, or to both .

PART III – CONFERMENT ON THE COMMISSION OF OVERSIGHT AND ENFORCEMENT FUNCTIONS AND POWERS

Role of the Commission.

20. (1) The Commission on Administrative Justice is hereby granted the powers of oversight and enforcement of this Act.

(2) In the performance of its functions under this Act, the Commission shall be guided by the national values and principles of

the Constitution.

Functions of the
Commission.

21. (1) The functions of the Commission include- —

- (a) investigating any complaint relating to a violation of any person's rights under this Act;
- (b) providing a framework or mechanisms for effective conflict management or dispute resolution on matters relating to this Act; and
- (c) taking such further action as is contemplated by this Part.

(2) The Commission shall, in performing its functions —

- (a) have regard to all applicable international information management and dissemination standards relating to data protection; and
- (b) ensure that public authorities provide adequate safeguards for protection of personal information.

(2) The Commission shall have all the powers necessary for the performance of its functions under this Act.

PART IV- COMPLAINTS, PROCEEDINGS AND SETTLEMENT

Inquiry into
complaints.

22. (1) A data subject who is aggrieved by any decision of any person under this Act may make a complaint to the Commission in accordance with the procedure provided in the Freedom of Information Act.

(2) A person wishing to lodge a complaint under this Act shall do so orally or in writing addressed to the secretary or any other person as may be duly authorised by the Commission for that purpose.

(3) The Commission shall develop mechanisms and procedures to deal with oral complaints and recording of oral complaints.

(4) A complaint under subsection (1) shall contain such particulars as the Commission may prescribe.

(5) The Commission may, notwithstanding subsection (1), commence an investigation on its own initiative.

(6) Upon receipt of a complaint under subsection (1), the Commission may —

- (a) call for information or a report regarding such complaint from the agency within such reasonable time as may be specified by the Commission:

Provided that -

- (i) if the information or report is not received within the time stipulated by the Commission, the Commission may proceed to inquire into the complaint without the information or report;
 - (ii) if, on receipt of the information or report, the Commission is satisfied either that no further action is required or that the required action has been initiated by the agency, the Commission shall, in writing, inform the complainant accordingly and take no further action;
- (b) without prejudice to paragraph (a), initiate such inquiry as it considers necessary, having regard to the nature of the complaint.

Proceedings on
complaints.

23. On the receipt of a complaint in terms of section 22, the Commission may take no action or, as the case may require, take no further action on any complaint if, in the opinion of the Commission —

- (a) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;
- (b) the subject-matter of the complaint is trivial;

- (c) the complaint is frivolous or vexatious or is not made in good faith;
- (d) the individual alleged to be aggrieved does not desire that action be taken or, as the case may be, continued;
- (e) the complainant does not have sufficient personal interest in the subject-matter of the complaint;
- (f) where —
 - (i) the complaint relates to a matter in respect of which a code of practice issued under this Act is in force; and
 - (ii) the code of practice makes provision for complaints procedure and the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue; or give the person a place of referral; or
- (g) there is in all the circumstances an adequate remedy, or other right of appeal other than to the Commission, that it would be reasonable for the individual alleged to be aggrieved to exercise.

(2) Notwithstanding anything in subsection (1), the Commission may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Commission that, having regard to all the circumstances of the case, any further action is unnecessary.

(3) In any case where the Commission decides to take no action, or no further action, on a complaint, the Commission shall inform the complainant of that decision and the reasons for it

Settlement of complaints.

24. Where it appears from a complaint, or any written response made in relation to a complaint under section 23, that it may be possible to secure a settlement between any of the parties concerned and, if appropriate, a satisfactory assurance against the repetition of any action that is the subject-matter of the complaint or the doing of further actions of a similar kind by the person concerned, the Commission may, without investigating the complaint or, as the case may be, investigating the complaint further, to secure such a settlement and assurance.

PART V – POWERS AND REMEDIES

Powers and remedies of the Commission on the complaint.

25. (1) If in any proceedings under section 23 or section 24, the Commission is satisfied on a balance of probabilities that any action of the defendant is an interference with the data protection under this Act, it may grant one or more of the following remedies- —

- (a) a declaration that the action of the defendant is an interference with the data protection in relation to the individual;
- (b) an order restraining the defendant from continuing or repeating the interference, or from engaging in, or causing or permitting others to engage in, conduct of the same kind as that constituting the interference, or conduct of any similar kind specified in the order;
- (c) an order that the defendant perform any acts specified in the order with a view to remedying the interference; or
- (d) such other relief as the Commission thinks fit.

(2) In any proceedings under section 23 or 24, the Commission may award such costs against the defendant as the Commission thinks fit, whether or not the Commission makes any other order, or may award costs against the plaintiff, or may decline to award costs against either party.

(3) It shall not be a defence to proceedings under section 23 or 24

that the interference was unintentional or without negligence on the part of the defendant, but the Commission shall take the conduct of the defendant into account in deciding what remedy to grant.

Damages.

26. In any proceedings under section 23 or 24, the Commission may advise the complainant to seek damages in Court against the defendant for an interference with the data protection of a data subject in respect of any one or more of the following—

- (a) pecuniary loss suffered as a result of, and expenses reasonably incurred by the aggrieved individual for the purpose of, the transaction or activity out of which the interference arose;
- (b) loss of any benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably have been expected to obtain but for the interference;
- (c) humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.

PART V – MISCELLANEOUS PROVISIONS

Protection against certain actions.

27. (1) Where any personal information is made available in good faith pursuant to of this Act —

- (a) no proceedings, civil or criminal, shall lie against the agency in respect of the making available of that information, or for any consequences that follow from the making available of that information; and
 - (b) no proceedings, civil or criminal, in respect of any publication involved in, or resulting from, the making available of that information shall lie against the author of the information or any other person by reason of that author or other person having supplied the information to an agency.
- (2) The making available of, or the giving of access to, any personal information in consequence of a request made under section 12 shall not be taken, for the purposes of the law relating to defamation or breach of confidence or infringement of copyright, to constitute an authorisation or approval of the publication of the document or of its contents by the individual to whom the information is made

available or the access is given.

Offences.

28. (1) A person who —

- (a) without reasonable excuse, obstructs, hinders, or resists the Commission or any other person in the exercise of their powers under this Act;
- (b) makes any statement or gives any information to the Commission or any other person exercising powers under this Act, knowing that the statement or information is false or misleading;
- (c) represents directly or indirectly that he or she holds any authority under this Act when he or she does not hold that authority;

commits an offence and is liable, on conviction, to a fine not exceeding Kshs 100,000 and to a term of imprisonment not exceeding two years, or to both.

Regulations.

29. (1) The Cabinet Secretary may, after consultation with the Commission, make regulations prescribing anything required by this Act to be prescribed or generally for the better carrying out of the provisions of this Act.

(2) Without prejudice to the generality of subsection (1), the regulations may provide for —

- (a) the manner in which applications under this Act are to be made;
- (b) the form in which information requested under this Act is to be supplied;
- (c) the procedure for the service of notices and documents under this Act: or
- (d) providing for such matters as are contemplated by or necessary for giving full effect to this Act and for its due administration.

MEMORANDUM OF OBJECTS AND REASONS

The Ministry of Information and Communications has formulated the Bill herein with a view to protecting personal information that is collected by persons and processed automatically. The Bill recognizes that data protection in relation to personal information is a corollary to expectation of privacy, a human right that is in keeping with best international practice. It also spells out the mechanisms for enhancing data protection. The Bill is borne of the realization that data protection is crucial for the promotion of e-transactions in the global digital economy where a lot of information is processed automatically.

Part I of the Bill contains preliminary provisions.

Part II contains provisions on principles of personal information protection. Clause 8 provides for collection of personal information, clause 8 provides for exemptions, Clause 10 provides for notice to persons on information collection, , Clause 11 provides that information should be protected, Clauses 12 and 13 provides for access to information and correction of information, Clause 14 provides for the parameters on use of information, Clause 15 provides for storage of information, Clause 16 provides for protection against misuse of information, Clause 17 prohibits a person from using personal data without the express consent of the data subject, Clause 18 provides for protection against use and disclosure of unique identifiers and Clause 19 provides for protection against interference with the personal information .

Part III contains provisions, under clauses 20 and 21, conferring on the Commission on Administrative Justice oversight functions and powers.

Part IV contains provisions on data protection, clause 22 pertains to inquiry into complaints, Clause 23 governs conduct of proceedings and Clause 24 is on settlement of complaints.

Part V contains powers and remedies of the Commission in relation to violation of data protection principles. It provides at Clause 26 for damages that may be awarded.

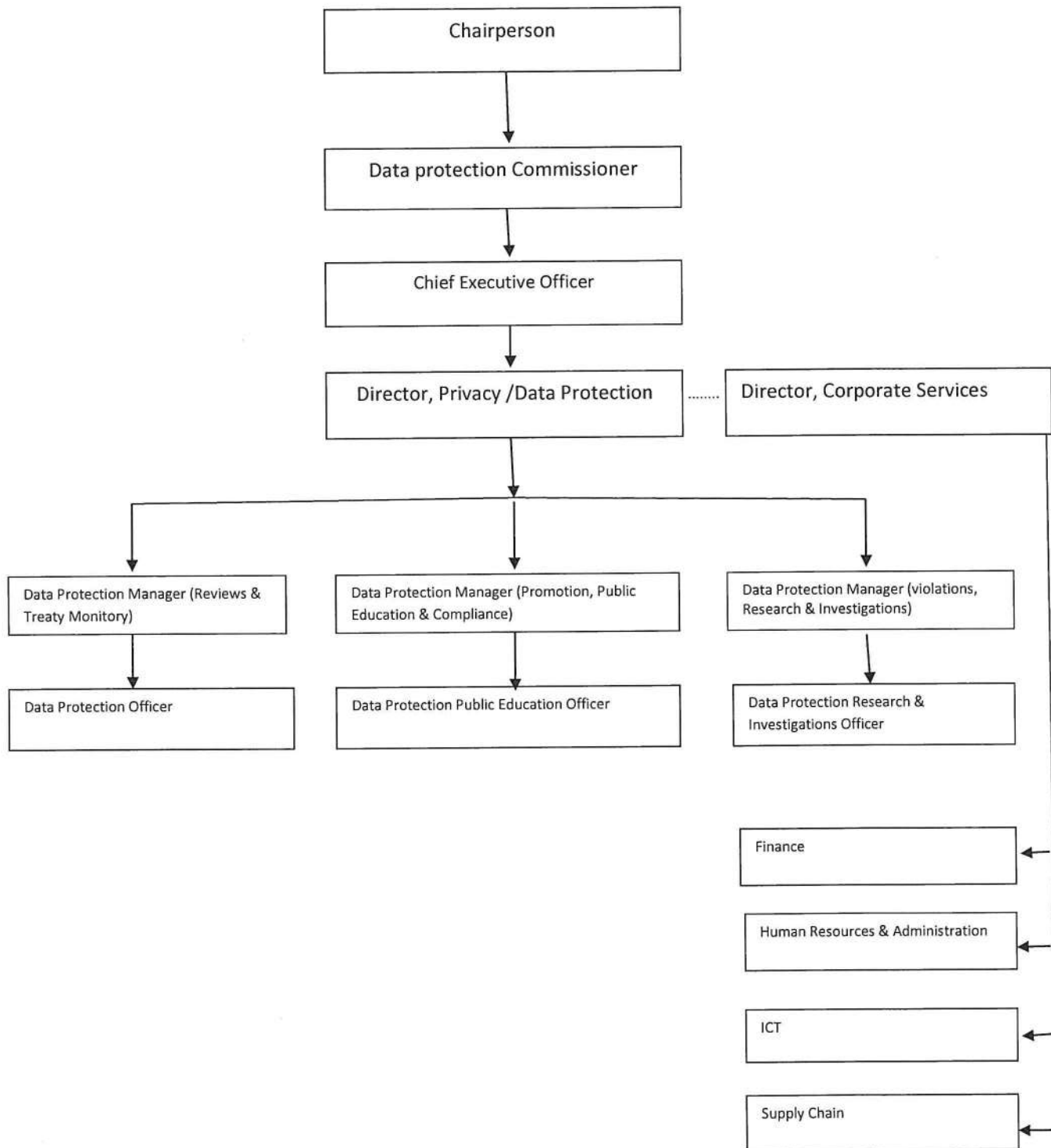
Part VI contains miscellaneous provisions

The enactment of this Bill will not occasion additional expenditure of public funds.

Dated the2012.

SAMUEL POGHISIO,
Minister of Information and Communications.

Annexure No. 1: Proposed Data Protection Directorate Structure



labeled on 17 Sep, 2019.



**MEMORANDUM ON DATA PROTECTION BILL PRESENTED TO THE NATIONAL ASSEMBLY
OF KENYA DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND
INNOVATION.**

17 September 2019

Amnesty International Kenya welcomes the Data Protection Bill as a step towards the right direction in the realization of the right to privacy in Kenya. We appreciate that the principal object of the Bill is to give effect to Article 31(c) and (d). We also acknowledge that the Bill sets out requirements for the protection of personal data processed by both private and public bodies.

The 21st century has been characterized as the digital age or information age that has seen our social, economic and political activities dependent on the information and communication technologies. With this widespread use of digital technologies, protection of data processed, shared, stored and transmitted through these technologies is very important.

Amnesty International Kenya calls upon the Committee on Communication, Information and Innovation to make the following changes: -

1. Ensure that the Office of the Data Protection Commissioner is financially and functionally independent.
2. Ensure that the exemptions contemplated in the Bill are in accordance with the limitations to the right to privacy contemplated under Article 24 of the Constitution of Kenya.
3. Review the lenient penalties contemplated in the Bill and provide for more deterrent penalties for breach of the Data Protection Act.
4. Ensure that all data collected, processed, shared or stored by operation of any other Act of Parliament be in accordance with the Data Protection Act.

ESTABLISHMENT OF THE OFFICE OF DATA PROTECTION COMMISSIONER

Clause 5 of the Bill proposes the establishment of the Office of the Data Protection Commissioner. Amnesty strongly supports the intentions of the Bill to have an independent Data Protection Commissioner to ensure enforcement and implementation of the Act. Several clauses of the Bill do not promote the independence of the Data Protection Commissioner such as placing the Office directly under the Cabinet Secretary of Information and Communication Technology.

Appointment of Data Protection Commissioner

Clause 6 elaborates on the process of appointment of a Data Protection Commissioner through the Public Service Commission (PSC), it further provides that the PSC considers, shortlists, interviews and nominates three qualified persons for appointment by the Cabinet Secretary. This process of appointment connotes that the Data Protection Commissioner reports to the Cabinet Secretary which negates the independence of the office. This subjugation to the Cabinet Secretary is further evidenced under Part IX of the Bill, Clause 68 provides that the Data Commissioner shall submit annual financial estimates to the Cabinet Secretary who then tables in the National Assembly. Clause 70 similarly provides that the Data Commissioner shall submit annual reports to the Cabinet Secretary who shall within three months submit the annual report to the National Assembly.

Amnesty International proposes that the Data Commissioner reports to the National Assembly. The Clause 6 on appointment of the Data Commissioner be amended to provide that the **President gazettes the vacancy in the office of the Data Commissioner and constitutes a selection panel for the purposes of appointment. We propose that Clause 6 provides for a selection panel that is comprised of a chairperson selected by the President and one representative from each of the following; Ministry responsible for Information, Communication and Technology; Kenya National Commission on Human Rights; one data science professional of at least fifteen years' experience; one information technology professional of at least fifteen years' experience; the Association of Professional Societies of East Africa; and the Law Society of Kenya.**

The selection panel shall hold its proceedings in public and submit a report to the National Assembly a report of the interview proceedings, which should include the scores of each candidate interviewed together with the criteria for selection. The selection panel should forward three names to the President for nomination, the President then nominates one person for National Assembly approval.

Commissioner should report to National Assembly instead of Cabinet Secretary

We further propose an amendment to Clause 68 to provide that the Data Protection Commissioner prepares and tables before the National Assembly their annual financial estimates. Further, Clause 70 be amended to provide that the Data protection Commissioner to gazette and forward the annual report to the Clerk of the National Assembly for debate and adoption. These proposals allow for financial and functional independence of the Data Protection Commissioner.

Security of office is also key to the independence of the office; Clause 12 provides for the removal of the Data Protection Commissioner through the Public Service Commission. **We propose that the removal of the Data Protection Commissioner be in accordance with Article 251 of the Constitution. The office established as a state office under Article 260, requires that the removal process reflects the removal process of a state officer.** We propose that the removal of the Data Protection Commissioner be commenced through a petition to the National Assembly, which if satisfied, will send the petition to the President for the formation of a

tribunal to investigate the conduct of the Commissioner and recommend to the President action.

- ✧ Amnesty International reiterates that the independence of the Data Protection Commissioner is pivotal to the implementation and enforcement of the Act.

Exemptions to Data Protection Requirements

Amnesty International is also concerned with the exemption clauses contained in the Bill. We acknowledge that it is international practice for a law to contemplate exemptions to the data protection laws, however, these limitations must meet the criteria laid down under Article 24 of the Constitution of Kenya. Article 24 provides for the limitation of rights and fundamental freedoms in Kenya. Article 24 of the Constitution requires that any limitation to fundamental rights and freedoms must be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. Article 31 is expressly limited for persons serving in the Kenya Defence Forces or the National Police Service. This therefore connotes that for the right to privacy to be limited, it must satisfy the criteria laid down in the Constitution.

The exemption for the purposes of national security or public order from the provisions of the Bill is of serious concern to us due to over broad nature of national security and public order. The blanket exemption from data protection will be prone to abuse by the State if left in the ambiguous wording it has currently. This ambiguity does not satisfy the principle of legality. **The courts have severally determined that laws, especially those that limit fundamental rights and freedoms, must be clear enough to be understood and must be precise enough to cover only the activities connected to the law's purpose. Moreover, the extent of national security or public order is not well defined, as such risks invalidity as the Bill does not specifically express the intention to limit Article 31 as required by Article 24 of the Constitution.**

We propose that State agencies responsible for national security and public order be bound by the general rules of data protection such as security of data, collection limitation, purpose limitation among other rules. It must be clearly provided in law the nature and extent of data that may be collected for the purposes of national security and public order. We propose the only allowable exemption be limited to seeking consent of data subject's access, analyze, process and store data. We hence propose an amendment to Clause 51(2)(b). We also propose an amendment to Clause 51(2)(c) that gives a blanket exemption to all disclosures required by law and orders of the court. This Clause provides an opportunity for the State to circumvent the Data Protection Act by enacting laws that allow for disclosures. This Clause equally does not meet the criteria set under Article 24.

Clause 54 provides that the Data Protection Commissioner may provide instances where certain provisions of the Act may be exempted. **In our view, these exemptions should be set out clearly in the law and the Commissioner in the exercise of this function should be bound by the rules of limitations laid down under Article 24 namely, that any limitation to a fundamental right must be clearly and concisely provided in law; must be necessary and proportionate in an open and democratic society; and, must pursue a legitimate aim.**

Penalties

Clause 58 provides for enforcement notices where non-compliance attracts upon conviction a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years or both. Clause 61 provides for the offence of obstruction of the Data Protection Commissioner where upon conviction, a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years or both.

Clause 63 also provides for administrative fines for infringement of the Act by setting out the maximum sentence of up to five million shillings or two per centum of the annual turnover, whichever is higher. Further, Clause 73 provides for the general penalty set to a maximum of three million shillings or to an imprisonment term not exceeding two years or both.

Amnesty International Kenya is concerned that these penalties proposed are lenient to the extent that they may not serve the deterrence effect they are intended to have – especially where big corporations with high financial muscle are concerned. **Penalties should be designed to make non-compliance costly for persons or companies that infringe. The European Union General Data Protection Rules (GDPR) provides for penalties that make large and small corporations weigh cost of compliance against business costs.**

Data Protection Bill and other laws

While the Bill provides for consequential amendments in the Second Schedule, the pieces of legislation listed are not exhaustive as there are other Acts of Parliament that have provisions that negate the data protection provisions of the Bill. The existence of other laws allowing the government agencies to collect, process, share and store data without regard to any data protection safeguards is a point of concern.

We propose the inclusion of a clause to provide that **all data collected, processed, stored or shared in Kenya shall be subject to the provisions of the Data Protection Act.**

END

935

clerk@parliament.go.ke

Zimbra

DATA PROTECTION BILL MEMORANDUM

From : Executive Officer <executiveofficer@kma.co.ke>
Subject : DATA PROTECTION BILL MEMORANDUM
To : clerk@parliament.go.ke

Mon, Jul 15, 2019 07:52 PM
1 attachment

Dear Sir/madam,
Please find our input on the proposed data protection bill of 2019 attached to this email.

Best regards,

Dr. Elizabeth Gitau -Maina, MBChB, MBA-HCM

CEO | Kenya Medical Association

KMA Centre | 4th Floor | Chyulu Road, Upper Hill

P.O. Box 48502 NAIROBI - 00100

(+254 20) 2679322 | (+254 722) 275 695

(+254 726) 552437

s: www.kma.co.ke

Twitter: @KenyaMedics_KMA

Facebook: <https://www.facebook.com/KenyaMedicalAssociation>

*1. D/centHos
2
16/07
2. Kendi 8/19*

DATA PROTECTION BILL MEMORANDUM.pdf
153 KB



MEMORANDUM

**PROPOSED AMENDMENTS THE DATA PROTECTION BILL NO.
44 OF 2019**

**SUBMITTED
TO
THE NATIONAL ASSEMBLY DEPARTMENTAL COMMITTEE ON
COMMUNICATION, INFORMATION AND INNOVATION.**

Submitted by Kenya Medical Association (KMA)

Contact details:

Elizabeth Gitau

executiveofficer@kma.co.ke ; 0726552437 / 0722275695

15th July, 2019

1. INTRODUCTION

The Kenya Medical Association (KMA) is a membership organization representing medical and dental practitioners registered to practice in Kenya with a twin mission of championing the welfare of doctors and advocating for the provision of quality healthcare for all. Kenya Medical Association.

(KMA) is a voluntary membership organization open to all medical and dental practitioners registered in the Republic of Kenya.

Despite short notice on submission of memoranda, the Kenya Medical association has gone through the draft bill and noted a gap which we propose for amendment. Given more time, the Kenya Medical Association would like to engage the committee on communication, information and innovation on matters regarding this bill.

2. PROPOSED AMMENDMENT

CLAUSE 1: Establishment of the Office.

LEADERSHIP/COMPOSITION OF DATA PRIVACY COMMISSION.

KMA proposes that the act be amended to include a data privacy commission /committee who will provide diversity and technical expertise on health data protection.

JUSTIFICATION

“health data” means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services;

The establishment of office has direct impact on the execution of the mandate of **article 46** of the proposed bill.

Due to the nature and sensitivity of personal data and specifically health data, the proposal of the Kenya Medical association is to have a Data privacy committee with representation from the legal and medical professional societies giving guidance on the unique nature of medical data both personal and aggregate data

ARTICLE 19

Tabled before the
Committee on 17th Sep,
2019.

- DRAFT -

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.

<i>Executive Summary</i>	2
<i>About the Article 19 Transparency Programme</i>	4
<i>I. Introduction</i>	5
<i>II. Analysis of the Draft Law</i>	5
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 the Kenya Office at 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.¹

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

¹ 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 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.²

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.

² 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."³ 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;

³ 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.⁴

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

⁴ 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.

② HOLLER
KINA
Please deaf
FA
09/9/19

① D1cutto3
8
319/19

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019



Prepared by;

Content Development & Intellectual Property (CODE-IP) Trust
Box 75474-00200 City Square,
Nairobi

Submitted to:

The Departmental Committee on Communication Information and Innovation,
The National Assembly, Twelve Parliament of Kenya,
Nairobi

16 July, 2019

THE NATIONAL ASSEMBLY
RECEIVED
09 SEP 2019
DIRECTOR GENERAL SERVICES
Time:

NATIONAL ASSEMBLY
RECEIVED
02 SEP 2019
DEPUTY CLERK
J.W.N
P. O. Box 41842 - 00100, NAIROBI

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

Reference is made to above Notice inviting members of the public to submit representations on the Data Protection Bill, 2019. We thank the Departmental Committee on Communication Information and Innovation for inviting privacy and data protection Technology Rights Defenders to provide input. We appreciate being consulted on the current law before the House.

Article 31 (c) and (d) of the Constitution requires the unwarranted intrusion into privacy with minimal requirement for information relating to family or private affairs unnecessarily or its disclosure which this Bill sets out to effect. Generally, it is our considered view that Sections 8-10 establish Data Protection Commissioners to whom largely confers the constitutional mandate. The Commissioner is thereafter legally empowered to singly and independently define the rules and application of this Act. This may later be problematic on Delegated Legislation disputes. Further, applying the old test of fullest application of the law against oneself – if owned a small online enterprise collecting personal data raises deep concerns.

Therefore, whereas envisaged to be a person of high integrity and well-intended, and if permitted – analogous to establishing a 'Morality Commissioner' – guaranteeing unpredictable enforcement consequences. Besides plausible arbitrariness, the additional bureaucratic registration, certification, license fees requirements, and fines hamper ease of doing business in Kenya when "Ease of Doing Business" is a stated government commitment.

Hereby submit our Memorandum of Views for your consideration and pray that it deserves your due attention and consideration.

Respectfully submitted,



Alex Gakuru
Executive Director,
CODE-IP Trust

RECEIVED
COMMUNICATIONS AND INFORMATION
DEPARTMENT
11/01/2019
11:00 AM

RECEIVED
COMMUNICATIONS AND INFORMATION
DEPARTMENT
11/01/2019
11:00 AM

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

Section	Title	Proposal	Justification
Part I – Preliminary			
2	Interpretation	<p>Add definition of “data” at the beginning as:-</p> <p>“data” means the factual input processed into information by means of equipment operating automatically in response to instructions given for that purpose, recorded with the intention that it should be processed by means of such equipment, or is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. It need not be held on a computer.</p>	<p>Fundamental definition to guide subsequent interpretations and to expand the scope of data protection to include data on manual records as well as in digital systems, processing and control.</p>
2	Interpretation	<p>Add definition of “metadata” at the beginning as:-</p> <p>“metadata” means data about data and for the purposes of this Act qualifies as data wherever consolidated metadata reveals private data or personally identifiable information</p>	<p>Cure indiscriminate metadata collection, retention, processing and disclosure to third parties</p> <p>See video ‘Metadata Explained Privacy International’ https://www.youtube.com/watch?v=xP_e56DsymA</p>
2	Interpretation	<p>Add definition of “Data Collector” after “Data Commissioner as:-</p> <p>“Data Collector” means a natural or legal person, public authority, agency or other body which alone or jointly with others, collects public data.</p>	<p>1. To expand the scope of privacy protection to include foreign entities collecting private data of Kenyans for inclusion in alien data systems.</p> <p>2. This category of data handlers is otherwise exempted from provisions of this Bill.</p> <p>3. Effect Article 31(c) information relating to their family</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

			or private affairs unnecessarily required or revealed;
2	Interpretation	Add definition of "Data Owner" after "Data Subject" as :- "Data Owner" means the same as "Data Subject"	Balancing out normative contextual interpretations over private data 'owner' vs. private data 'subject'
2	Interpretation	Change definition of "profiling" to read as;- "Profiling" means any form of automated processing of personal data consisting of the use of personal data evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects, such as, concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth, personal preferences, interests, behaviour, location of movement, family or private affairs, among others;"	Effect Article 31(c) 'information relating to their family or private affairs unnecessarily required or revealed;'
3(b)	Object and Purpose of this ACT	Consider adding the purpose;- "(e) to establish a framework to protect against the unnecessary collection of information relating to their family or private affairs"	1. Whereas "...minimisation of collection..." is a stated purpose, nowhere on the Act is the unnecessarily collected personal data given force of law and complies with Sections 25 (c) and (d). 2. Effect Article 31(c) 'information relating to their family or private affairs unnecessarily required or revealed;'
4 (b)	Application	Change to read;- "(b) by a data collector, data controller or data processor who –	To expand the scope of privacy protection to include foreign entities collecting private data of Kenyans for inclusion in alien data systems.

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

		<p>(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or</p> <p>(ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects in Kenya.</p>	
Part III – Registration of Data Controllers and Data Processors			
Part III - sections 18-24	Registration with DPO	Delete requirement for data processors and controllers to register with the Data Protection Office	<p>The proposed legislation requires registration of data processors and controllers in Kenya with the Data Protection Officer including the requirement to document and keep up to date a record of processing activities. The bill contemplates the potential requirement of fees for processors to register with the state and penalties for failure to register.</p> <p>Data Processing and Data Controlling are not business models in the strict sense. They are activities that entities may incidentally engage in during the course of business.</p> <p>The requirement to have all processors and controllers would create an immense implementation burden for the Data Protection Office that would threaten to bog down the office with bureaucratic recordkeeping rather than allowing them to focus on the most serious enforcement issues.</p> <p>Similarly, for processors and controllers, the requirement to update external records of processing each time a change to</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

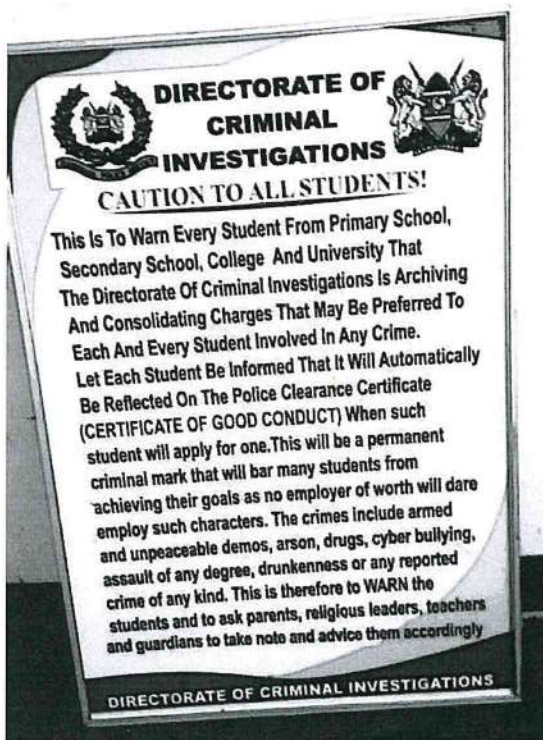
			<p>processing occurs shifts the focus from improving privacy in areas that present the most risk to a bureaucratic exercise. The requirement for fees also raises issues as this would disproportionately affect smaller data processors and controllers.</p> <p>Even the GDPR does not contain any parallel requirement for registration</p>
Section 25	Principles of Data Protection	<p>Add new Sub-section after (d) and before (e):-</p> <p>“(d.1) A valid explanation must be provided whenever information relating to family or private affairs is necessarily to be collected”</p>	<p>Article 31(c) information relating to their family or private affairs unnecessarily required or revealed;</p>
Section 33	Processing of Personal Data relating to a child	<p>Add new Sub-section after (c):-</p> <p>“(c) all personal data relating to a child collected, processed and or archived subject to subsection (b) must be deleted upon the child becoming an adult.”</p>	<p>This will prevent overzealous law enforcement officers labeling children criminals for life (see Annex I -<i>DCI Criminal Child Data Archiving Notice</i>).</p> <p>And also criminalise archived profiles of child’s youthful indiscretions.</p>
Section 43	Notification of data Breach	<p>Revise to require notification only where breach is likely to result in a risk to the rights and freedoms of natural persons</p>	<p>The proposed legislation requires notification to the Data Protection Officer for all instances of breach and not just those that are likely to have an impact on the rights of the data subject.</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

			<p>As currently drafted could have risk of inundating Data Protection Office with notices for risks that are trivial in terms of impact on rights of individuals. A more efficient and effective means to enforcement would come from narrowing notification to those breaches likely to have an impact on individual rights and freedoms</p>
<p>Sections 48-50</p>	<p>Cross-Border Transfer of Data</p>	<p>Permit transfers to third country where, accounting for the transfer, all of the other requirements set forth in the legislation will continue to be met.</p> <p>Clarify that the conditions listed in part VI are mutually exclusive. Do this by using the term "...may transfer personal data to another country where any of the following conditions is fulfilled" or separate the conditions with the term 'or'.</p>	<p>The proposed legislation bars transfer of data to a third country where there is no decision by the Data Commissioner that adequate safeguards have been made for the protection of that data (adequacy decision).</p> <p>The omission of the word 'or' at the end of the conditions listed in this part gives the interpretation that all of those conditions listed have to be met before data can be transferred across borders. IT appears that this may not have been the intention and that all the conditions listed are mutually exclusive.</p> <p>Requirement for adequacy decision will have undesirable impact on restricting free-flow of data. Concerns may be addressed through alternatives like binding corporate rules, codes of conduct, and certifications.</p>

MEMORANDUM OF VIEWS ON THE DATA PROTECTION BILL, 2019

Annex I DCI Criminal Child Data Archiving Notice



949

1. DIC-11001
8
16/07



P.O Box 16872 – 00100 Nairobi, Kenya

Your Ref: TBA

Date: 15th July, 2019

Our Ref: DLAK/ICT-16/2019/7

Mr. Michael Sialai, EBS
Clerk of the National Assembly,
Parliamentary Service Commission,
P.O Box 41842-00100,
NAIROBI

2. Eli Kende
for consideration by
committee
17/7/19

Dear Mr Sialai,

RE: SUBMISSIONS ON THE DATA PROTECTION BILL, 2019

Receive warm greetings from the Digital Lenders Association of Kenya (“DLAK”).

DLAK is the apex national membership society of leading digital lenders who collectively, represents approximately a quarter of the new digital loans originated in Kenya each month. Leading actors in the digital lending space, including Tala, Alternative Circle, Zenka Finance, Kuwazo Capital, Stawika Capital, MyCredit, Okolea, LPesa, KopaCent and Finance Plan LTD, recognized the need for accountability to our users and regulators. We formed DLAK to bring accountability by protecting consumers and embodying responsible lending with our Code of Conduct.

DLAK further seeks to influence and engage regulators and policy makers on laws and policies that promote an enabling environment to conduct digital lending business and to enhance Kenya’s competitiveness by reducing the cost of doing business.

In this regard, kindly find attached herewith our submissions on the proposed Data Protection Bill, 2019 for your kind consideration.

We are happy to meet and make oral presentations on the same.

Sincerely,

Robert Masinde
Chairperson of the Digital Lenders Association of Kenya

Encls.

Cc:

Hon William Kisang, MP
Chairperson,
Departmental Committee on Communication, Information and Innovation,
Kenya National Assembly, Parliament Buildings,
P.O. Box 41842-0010,
Nairobi, Kenya.



THE DATA PROTECTION BILL 2019

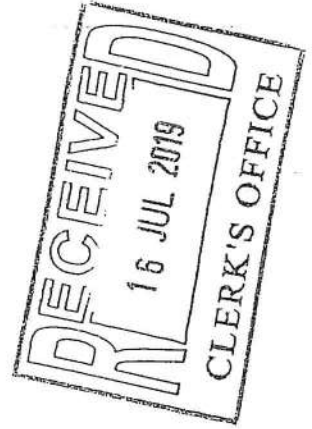
Globally and broadly there have been three approaches to data protection laws namely the Omnibus EU approach, the USA Sectoral Approach and China's approach to data protection for averting national security risks. Kenya has adopted mostly the GDPR approach with the bill drafted from the ICT Ministry having similarities to the GDPR. This is in line with global trends as countries seek to have an Omnibus approach as opposed to the USA sector approach that has been criticized as not being comprehensive and leading to vulnerability of data information and a breach to privacy.

However, Kenya needs to also borrow from India's approach as India's approach is to develop a bill suitable for "developing countries" and has departed from some stringent provisions of the GDPR.

Kenya is also set to launch the National Integrated Identity Management System (NIIMS) that will collect biometric information from Citizens and Non-Citizens in Kenya. This system could borrow from India's Aadhaar Biometric and India's open API architecture that has powered India Stack system. The Aadhaar like the expected NIIMS will accord a natural person with a unique identifier number linked to one's biometric. If Kenya adopts the Indian model, it could potentially mean more integration and availability of big data to third party players which information can be used for legitimate purposes. India has faced challenges with the Aadhaar system especially as regards data protection, data security and possibility of Government spying but the Courts in India have continued to hold that the benefits of the Aadhaar system far outweighs the negatives and thus Aadhaar has continued to allow the Aadhaar System with recorded success.

It is therefore important that the Data Protection Bill aligns with aspirations for innovation and use of big data while balancing the rights of privacy guaranteed under the Constitution of Kenya and the right of Access as provided in the Access to Information Act 2016 and the Constitution of Kenya 2010.

We have reviewed the Data Protection Bill 2019 and below are our comments:



THE DATA PROTECTION BILL 2019

The Clause	Current Clause	Proposed Clause RECOMMENDATIONS	Justification
Definition of "Sensitive Personal Data"	Data revealing a natural person's race, health status, ethnic social origin, conscience, generic data, biometric data, sex or the sexual orientation of the data subject	Add "religious or political belief or affiliation" to "belief" as part of definition of sensitive data	To provide for clarity on the meaning of belief.
Clause 7 (2) Term of the Data Commissioner	The Data Commissioner shall be appointed for a single term of 6 years and shall not be eligible for a re-appointment	The Data Commissioner shall be appointed for a term of three years which shall be subject to renewal for a further final term of three years.	The term of 6 years is very long for such an office and based on other terms of service for such positions in the public service, a term of three years renewable is fair.
Clause 18,19,20,21,22 Registration of Data Controllers and Data Processors	The Act requires mandatory registration of Data Controllers and Processors and registration	Propose deletion of Clause 18, 19,20,21,22 and replace with a Clause "No person shall act as a Data Protection	This requirement for registration is not provided for in the GDPR or in the Indian Bill or the South African Act. GDPR approach is cooperation and enforcement. This clause is not necessary as compliance can still be

	<p>by the Data Commissioner and requires the Data Commissioner to set threshold to exempt small companies</p>	<p>Officer unless one is registered and accredited by the Data Commissioner"</p> <p>Amend Clause 24 to provide for Registration and Accreditation of Data Officers</p>	<p>achieved outside registration in addition it may be cumbersome, ambiguous and difficult to enforce and even then it will be problematic to set thresholds as collection and processing differs per industry or per process etc.</p> <p>Best practice adopted in the GDPR is to do away with mandatory registration but adopt the GDPR model of cooperation, enforcement and data protection by design.</p> <p>We propose registration and accreditation of Data Protection Officer as a mechanism for control by the Data Commissioner</p>
<p>Clause 25 (c) and (g) Principles of Data Protection</p>	<p>Every Data Controller and Processors shall ensure that personal data is:</p> <ul style="list-style-type: none"> a) b) c) Collected for explicit, 	<p>Data Controller and Processors should ensure data is processed:</p> <ul style="list-style-type: none"> a) b) c) Collected and processed for explicit, specific, legitimate or for any 	<p>1. On the purpose principle, we could adopt the reasonability and incidental test included in the India model where the purpose is interpreted widely to allow for reasonable and incidental collection of data. The clause will adopt the reasonability test which departs</p>

	<p>specific and legitimate purpose and not further processed in a manner incompatible with those purposes-;</p> <p>g) Is transferred to third parties only with the consent of data subject;</p>	<p>incidental purposes that may be reasonably inferred having regard to the specific purposes, and the context and circumstances in which the personal data is collected including transfer to third parties with prior notification and consent;</p> <p>g) Delete.</p>	<p>from the strict GDPR interpretation that has led to exposure for data collectors and processors.</p> <p>2. Add the word "processed" in clause 25 © to include both collection and processing of data</p> <p>3. Delete Clause 25 (g) transfer to third parties on consent as a principle but rather part of legitimate purpose, Clause 25 (c) which must be disclosed to the data subject or subject to notification. This would allow legitimate transfer of information to third parties (similar to the GDPR)</p> <p>4. Consider definition of legitimate purposes</p>
<p>Clause 26 Rights of Data Subject</p>	<p>Data subject have a right to:</p> <p>a) Be informed of the use of their personal data;</p> <p>b) Access data stored by</p>	<p>Data subject have a right to:</p> <p>a) Be notified of the use of their personal data;</p> <p>b) Access data stored by data</p>	<p>The Data subject rights are not as wide as provided in the GDPR especially as regards information on third party data, modalities of the exercise of the right of the Data Subject, the right to withdraw consent, the right to</p>

	<p>data controllers and processors;</p> <p>c) Object to processing of their data also expounded in Section 36;</p> <p>d) Correct false or misleading data;</p> <p>e) Delete false or misleading data</p>	<p>controllers and processors;</p> <p>c) Object to processing of their data also expounded in Section 36;</p> <p>d) Correct false or misleading data;</p> <p>e) Delete false or misleading data</p>	<p>be forgotten which have not been limited. The Indian Act is comprehensive on Data Subject Rights and this clause may borrow some of the comprehensive clauses especially to balance the rights of the data subject and the interest of the data processors to process data, store and use.</p>
<p>Clause 31 Data Protection Impact Assessment</p>	<p>This clause provides for Data Protection Impact Assessment for "high risk "operations. However high risk is not defined and for clarity , the section can empower the Data Commissioner to issue guidelines on High Risk operations requiring impact assessment</p>	<p>Amend Section 31 (3) to provide for the Data Commissioners power through guidelines published in the Gazette Notice to provide guidance on the processes that may be high risk requiring Data Protection Impact Assessment.</p> <p>Clause 31 (2) on consultation should be deleted.</p> <p>Introduce a new Clause 31 (4) providing that</p>	<p>Amendment to Clause 31 (3) is to provide clarity on "high risk operations by the Data Commissioner". This is in line with the GDPR which requires the supervisory authority to specify the high risk processes that may require Data Protection Assessment.</p> <p>Inclusion of a new Clause 31 (4) is to provide timelines for submissions of Data Protection Impact Assessment Reports</p>

	<p>Data Protection Impact Assessment Reports shall be submitted within 60 days from the date of publication as per clause 31 (3)</p>	
<p>Clause 32 (2) Withdrawal of Consent of the Data Subject</p>	<p>Unless otherwise provided in this Act, a Data Subject shall have the right to withdraw consent at any time and the Data Controller or Data Processor shall notify the Data Subject of the procedure for withdrawal of the Consent prior to obtaining consent to receive personal data. Provided further that withdrawal shall not be arbitrary and shall be subject to the overriding legitimate grounds of the data controller or data processor as provided in Clause 34 (d).</p>	<p>Withdrawal should not be arbitrary especially for service providers that rely on consent for provision of service and further the Data Subject must be informed of the process and grounds for withdrawal at the time they are giving consent</p>
<p>Clause 35 (3) and (4) Automated individual decision making</p>	<p>Delete Clause 35(3) and (4) and replace with the clause “ the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention</p>	<p>The GDPR does not create a duty of notification to the data subject once an automated decision is made as this is a cumbersome process. The Indian Act does not have provision for this right Remove Section 35 (3) the right to notification as it is</p>

		<p>on the part of the controller, to express his or her point of view and to contest the decision.”</p>	<p>not necessarily being cumbersome to implement. Replace with the clause that guides the Data Controller and Processors to safeguard and protect the rights and freedoms of data subject. This proposal is in line with the GDPR</p>
<p>Clause 36 Objection to processing</p>	<p>A data subject has the right to object to the processing of their personal data unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment exercise or defence of a legal claim</p>	<p>A data subject has the right to object to the processing of their personal data under Clause 30 (iv) and 37 unless the data controller or data processor demonstrates compelling legitimate public interest for the processing which overrides the data subject's interests, or for the establishment exercise or defence of a legal claim</p>	<p>The right to object needs to be restricted to certain cases in line with the same clause in the GDPR. If the clause is left to blanket objection ten data processors and controllers may be faced with continuous objection which may be cumbersome. The objections should not be arbitrary and that is why we are proposing objections only on Clause 30 (iv).</p>
<p>Clause 43 Notification and Communication of Breach</p>	<p>Section 43 obligates the Data Controllers to notify the Data Commissioner within 72 hours of becoming aware of breach of data (unauthorized access or risk of harm) and where the</p>	<p>This Clause does not provide for thresholds and may obligate parties to report non-material breaches. The Clause should include a proviso empowering the Data Commissioner to issue guidelines on thresholds for reporting.</p>	<p>Amend Section 43 on notification of breach to put thresholds as it will not make sense to keep reporting non-material breaches.</p>

	<p>personal data subject can be identified, notify them within reasonable time. The Data processors is obligated to notify within 48 hours (Section 43 (3) and I both cases the Data Processor and Controller must take reasonable steps to put security safeguards to stop the breach.</p>	<p>Amend Clause 43 1 as follows: <i>"Where personal data has been accessed and acquired by unauthorized person , and such access or authorization meets the threshold prescribed by the Data Commissioner... a data controller shall"</i></p>	
<p>Clause 45 Grounds for processing sensitive data</p>	<p>This clause does not provide for processing by a Government Agency such as NIMS System</p>	<p>Propose for inclusion of a clause as below <i>" Collection or processing of sensitive information by a Government Agency carrying out a legitimate purpose "</i></p>	<p>Clause to be added to include the role of Governments in collecting sensitive data</p>
<p>Clause 48 and 49 Transfer of Data Outside Kenya</p>	<p>Clause 48 and 49 provide for grounds for transfer of data outside Kenya. Transfer of Personal Data make be done subject to conditions provided under Section 48 (1) including proof of appropriate safeguards,</p>	<p>Amend Clause 48 (1) as follows <i>"The Data Controller or Data Processors has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of personal data and the appropriate safeguards include jurisdictions with commensurate Data</i></p>	<p>The amendment is necessary to define "appropriate safeguards" and remove ambiguities so it is clear how a party can demonstrate appropriate safeguards and further the Data Commissioner is empowered to approve certain jurisdiction as safe for transfer</p>

	<p>consent of data subject and this is also provided in Clause 49 (2) where the Act makes reference to appropriate security safeguards to transfer sensitive data.</p>	<p><i>Protection Laws and approved by the Data Commissioner"</i></p> <p>Amend Clause 49 (1) and (2) and add where the term appropriate safeguards appear "<i>appropriate safeguards include jurisdictions with commensurate Data Protection Laws and approved by the Data Commissioner"</i></p>	
<p>Clause 50 Processing through a Data Centre in Kenya</p>	<p>This Clause empowers the Cabinet Secretary to prescribe processing of certain data in Kenya</p>	<p>We propose deletion of this Clause-</p>	<p>In this era of cloud services and technological advancement, there should not be restrictions or an overriding power to force a data processor or controller to hold their data in local servers. This restriction is not in the GDPR and should be removed as it is subject to abuse.</p> <p>If the Clause is retained the same should be subject to consultation with the Data Commissioner and Clause 40 and the Data Processor or Controller shall have a right of appeal of the Cabinet Secretary Decision in the High Court.</p>
<p>Clause 51</p>	<p>Clause provides for exemption</p>	<p>Include the exemption to apply for both</p>	<p>Need to provide for exemption in the case of sensitive</p>

Exemptions	of Personal Data but does not provide for exemption for Sensitive Data	personal and sensitive data	data
<p>Clause 58 (3), 61 Enforcement</p>	<p>Clause 58 (3) and 61 is too punitive. Especially for small players .</p>	<p>We propose reduction of the fine to Kenya Shillings Five Hundred Thousand (Kshs. 500,000) and removal of the jail term.</p>	<p>The high fines may kill small companies. The GDPR has been criticized due to the high fines and has even exposed firms to blackmail and red-tape. To avoid this the fines and penalties should only be deterrent but not punitive</p>
<p>Clause 63 Administrative Fines</p>	<p>Clause 63 is too punitive</p>	<p>"We propose reduction of the fine to Kenya Shillings Two Million (Kshs. 2,000,000) or 0.2 % of the annual turnover for the entity in Kenya whichever is higher"</p>	<p>Reduce the fine to protect small players and also define turnover for entities in Kenya to provide clarity for multinational companies.</p>
<p>Clause 64 Right of Appeal</p>	<p>The Clause only provides the right of Appeal to the High Court. The matters under this Bill are specialized in nature and the High Court may not be appropriate as the first place for appeal</p>	<p>We propose creating of the Data Protection Tribunal to handle all appeals from the administrative Actions of the Data Commissioner and Cabinet Secretary and thereafter Appeal to the High Court</p>	<p>To provide for appeal to the Data Protection Tribunal</p>
<p>Clause 65 (4)</p>	<p>In this section "damages"</p>	<p>This Clause is too wide and leads to unclear</p>	<p>Amend to provide for direct , special financial loss</p>

