(2) Hon, Tabled Other To Registrar, acknowledge receipt, card Cause Tabling & Committee response 5 17/1/22

REPUBLIC OF KENYA

MINISTRY OF ICT, INNOVATION AND YOUTH AFFAIRS

Office of the Cabinet Secretary

Telephone: +254-20-4920000/100
Fax: +254-20-3316004
Email: cabinet.secretary@ict.go.ke

Telposta Towers, 10th Floor
P. O. Box 30025-00100
NAIROBI – KENYA

When replying please quote:

(1) DLSP. 17/1/22

Ref: MIIYA/CONF/12/23

Date: 22nd December, 2021

Michael Sialai, EBS
Clerk of the National Assembly
Parliament Buildings
NAIROBI

Dear Mr. Sialai

STATUTORY INSTRUMENTS UNDER THE DATA PROTECTION ACT, 2019

Article 31 of the Constitution of Kenya gives every citizen the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed.

The Data Protection Act, 2019 gives effect to Articles 31(c) and (d) of the Constitution to establish the Office of the Data Protection Commissioner; 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; and for connected purposes.

On 7th January 2021, the Cabinet Secretary for ICT, Innovation and Youth affairs appointed a Taskforce for the development of Data Protection Regulations. Consequently, the following statutory instruments were formulated:

1. Data Protection (General) Regulations, 2021
2. The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021
3. The Data Protection (Compliance and Enforcement) Regulations, 2021

It is expected that the Regulations will benefit Government in the following ways:

1. Planning: The processing of personal data for specific lawful purposes such as the design of policies, planning of interventions, anticipation of possible change and the forecasting of needs.
2. Delivery: Use of personal data to inform and improve the implementation of policy, responsiveness of government and provision of public services.
3. Evaluation and monitoring: Anonymization of personal data involved in measuring impact, auditing decisions and monitoring performance.

The anticipated benefits to the private sector include the following:

1. Assist the private sector to meet compliance requirements;
2. Prevent breaches that hurt companies and other entities;
3. Prevent breaches that hurt data subjects;
4. Maintain and improve brand value;
5. Strengthen and grow businesses seen to comply with privacy legislation;
6. Support business ethics;
7. Maintain public investor and consumer trust; and
8. Build customer loyalty.

The Ministry therefore encloses the necessary documentation herewith for tabling before Parliament.

We thank you for your continued support and collaboration.

Yours Sincerely

JOE MUCHERU, EGH
CABINET SECRETARY

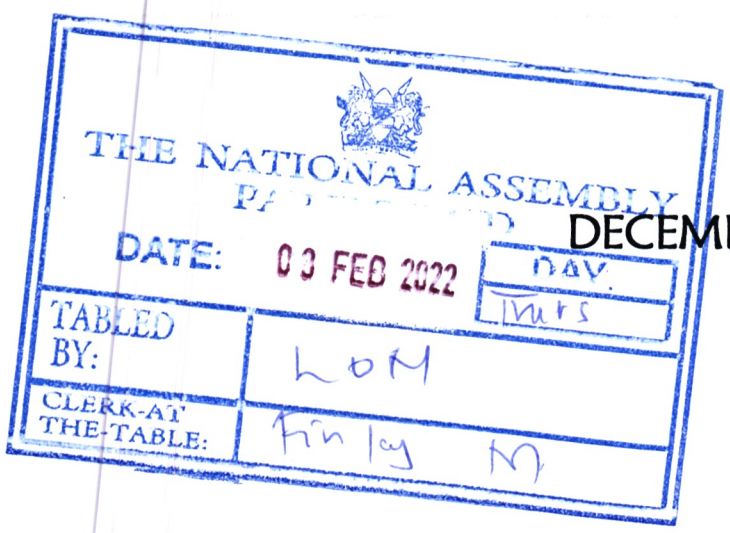
Copy to: **Jerome Ochieng, CBS**
Principal Secretary
State Department of ICT and Innovation
Ministry of ICT, Innovation and Youth Affairs
NAIROBI

Immaculate Kassait, MBS
Data Commissioner
Office of the Data Protection Commissioner
CA Centre, Waiyaki Way
NAIROBI

REPUBLIC OF KENYA

MINISTRY OF ICT, INNOVATION AND YOUTH AFFAIRS

SCHEDULE OF DOCUMENTS SUBMITTED TO THE NATIONAL ASSEMBLY FOR STATUTORY INSTRUMENTS UNDER THE DATA PROTECTION ACT, 2019 PURSUANT TO SECTION 5A OF THE STATUTORY INSTRUMENTS ACT 2019



DECEMBER 2021

SCHEDULE OF DOCUMENTS

1. Explanatory Memorandum (Annex 1)

    a. The Data Protection (General) Regulations, 2021
    b. The Data Protection (Compliance and Enforcement) Regulations, 2021
    c. The Data Protection (Compliance and Enforcement) Regulations, 2021

2. Statutory Instruments (Annex 2)

    a. The Data Protection (General) Regulations, 2021
    b. The Data Protection (Compliance and Enforcement) Regulations, 2021
    c. The Data Protection (Compliance and Enforcement) Regulations, 2021

3. Data Protection Act (Annex 3)

    The parent law, being the Data Protection Act No. 24 of 2019

4. Evidence of public participation as required by Section 5 of the Statutory Instruments Act, 2013.

    a) The Taskforce on 13th April 2021 issued a Public Notice on the call for comments on the draft regulations, requiring that memoranda on the draft regulations be submitted to the Taskforce by 27th April 2021 on *Annex 4.*

    b) Following various requests from the Stakeholder on the extension of the period for submission of comments, the Taskforce on 27th April 2021 issued another Public Notice extending the period of submission of the written memordanda from 27th April 2021 to 11th May 2021. *Annex 5*

    c) On 13th May 2021, the Taskforce published in the Kenya Gazette via *Gazette Notice No 4697* the notice informing the members of the public of the Regulatory Impact assessment on the Data Protection (Registration of Data Controllers and Data Processors) Regulations. *Annex 6*

    d) Subsequently, on 18th May 2021, a Public Notice was published in My Gov notifying the general public of the Regulatory Impact Assessment statement for the Data Protection (Registration of Data Controllers and Data Processors) dated 18th May 2021. *Annex 7.*

    e) Based on the public notices issued, the Taskforce was able to receive and review various memoranda submitted on the draft regulations, attached is a scheduled of all the memoranda submitted. *Annex 8.*

f) The Taskforce undertook the review of the comments received from the public from 23rd May 2021 to 8th June 2021. A schedule of the compiled comments for the 3 sets of regulations is available for review.

g) Due to the restriction imposed by the COVID-19 Pandemic, the Taskforce conducted all its consultative meetings with both stakeholders and the public virtually. The Taskforce conducted its public consultations two fold. It engaged targeted stakeholder and the public for a period of two weeks from 19th April 2021 to 3rd April 2021. The schedule of engagement of the stakeholders as well as the attendance for the engagement have been attached as ***Annex 9***

h) The Public consultation forums were held on dates outline below:

i. **27th April 2021** the public was taken through the *Data Protection (General) Regulation 2021.*
ii. **28th April 2021** the Public was taken through the *Data Protection (Compliance and Enforcement) Regulations, 2021*
iii. **29th April 2021** the public was taken through the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

Both the registration and attendance schedule for the stakeholder engagement and public participation have been attached as ***Annex 10.***

ANNEX 1

EXPLANATORY MEMORANDUM TO THE DATA PROTECTION (GENERAL) REGULATIONS, 2021

PART I

Name of the Statutory Instrument: Data Protection (General) Regulations, 2021

Name of the Parent Act: Data Protection Act, 2019

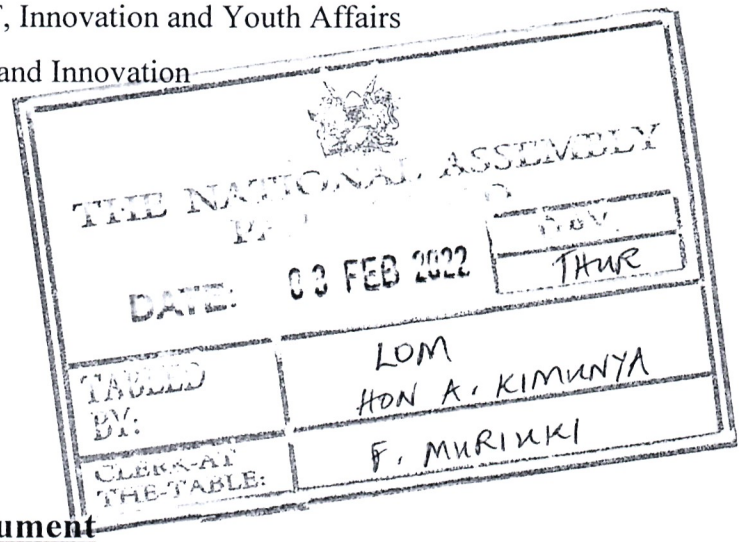
Enacted Pursuant to: Section 71 of the Data Protection Act, 2021

Name of the Ministry: Ministry of ICT, Innovation and Youth Affairs

Department: State Department of ICT and Innovation

Gazetted on:

Tabled on:



PART II

1. Purpose of the statutory instrument

1.1. The purpose of the statutory instrument is to give effect to the Data Protection Act and for prescribing anything required or necessary to be prescribed by or under the Act.

1.2. The Regulations prescribe and guide on data protection prerequisites such as: requirement of consent of the data subject for processing of personal data; collection of personal data; actualization of the rights of data subjects; commercial use of personal data; obligations of data controllers and data processors; data protection by design or default; notification of personal data breaches; transfer of personal data outside Kenya; and the process of undertaking data protection impact assessments.

2. Legislative Context

2.1. The Constitution of Kenya gives every citizen the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed.

2.2. The Data Protection Act, 2019, is the principal legislation under which these Regulations are anchored, seeks to provide a framework for the processing of personal data, and provides for the rights of data subjects and obligations of data controllers and processors. The Act applies to the processing of personal data entered in a record, by or for a data controller or processor, by making use of automated or non-automated means.

2.3. The object and purpose of these Regulations is to operationalize Data Protection Act, 2019, on the regulation of the processing of personal data to ensure that the privacy of individuals is protected.

PART III

3. Policy Background

3.1 On 7th January 2021, the Cabinet Secretary for ICT, Innovation and Youth affairs appointed a Taskforce for the development of Data Protection Regulations.

3.2 The Taskforce made several recommendations one of which was the formulation of General Regulations to give effect to the provisions of the Data Protection Act, 2019 pursuant to section 71 of the Act.

4. Consultation outcome

4.1. Pursuant to Article 10 of the Constitution, the Ministry of ICT, Innovation and Youth Affairs held extensive public consultations as well as stakeholder consultations on the draft Data Protection (General) Regulations.

4.2. A Public notice calling for comments from the members of the public on the draft Data Protection (General) Regulations dated 13th April 2021 was published in *My Gov*. The notice invited the members of the public to review the regulations and submit their written memorandums though the offices of the Data Protection Commissioner. Further an email address: dataprotectionregulations@odpc.go.ke was provided. Tens of Kenyans emailed their submissions. A subsequent public notice extending the deadline for submission of comments from 27th April 2021 to 11th May 2021 was published on 27th April 2021 in *My Gov.*

4.3. The Taskforce also held virtual meeting with the identified stakeholders from 19th April 2021 to 3rd May 2021 on the draft Data Protection (General) Regulations, keeping in line with the Ministry of Health Protocols on the Covid-19 Pandemic

4.4. Additionally, the Ministry held the public virtual hearings from the 27th April 2021 to 929th April 2021 in line with the Ministry of Health Protocols on the Covid-19 pandemic:

4.5. In this process of public consultations, members of the public acknowledged that the formulation of the Data Protection (General) Regulations would protect the privacy of personal data for Kenyans. Further, valuable input and recommendations were made during oral hearing and through the written memorandum.

4.6. To sufficiently consider these views, the Ministry, in collaboration with the Office of the Data Commissioner, the Office of the Attorney General, the Kenya Law Reform Commission, The Commission on Administrative Justice, the Communications Authority of Kenya and representatives from other relevant government agencies, held a workshop on 23rd – 29th May 2021 in Nakuru. All the views were analyzed and the draft was substantially amended to reflect

them. A Matrix on some of the concerns raised and how they were incorporated is annexed to this explanatory memorandum.

5. Guidance

The Ministry and the Office of the Data Commissioner will continue to proactively sensitize and build capacity for national and county government institutions, data controllers and data processors as well as the public on the provisions and implementation of the Data Protection (General) Regulations in order to ensure that the Regulations serve the public good.

6. Impact

6.1. **The Impact on Fundamental Rights and Freedoms:** These Regulations do not limit fundamental rights and freedoms

6.2. **The impact on the Private Sector**: The private sector will substantially benefit from positive externalities emanating from the protection of the right to privacy. The benefits of the Regulations will *inter alia*:

a) Assist the private sector to meet compliance requirements;
b) Prevent breaches that hurt companies and other entities;
c) Prevent breaches that hurt data subjects;
d) Maintain and improve brand value;
e) Strengthen and grow businesses seen to comply with privacy legislation;
f) Support business ethics;
g) Maintain public investor and consumer trust; and
h) Build customer loyalty.

6.3. **The impact on the Public Sector**: The implementation of data protection principles will benefit Government in the following ways:

a) Anticipation and planning: The processing of personal data for specific lawful purposes such as the design of policies, planning of interventions, anticipation of possible change and the forecasting of needs.

b) Delivery: Use of personal data to inform and improve the implementation of policy, responsiveness of government and provision of public services.

c) Evaluation and monitoring: Anonymization of personal data involved in measuring impact, auditing decisions and monitoring performance.

7. Monitoring and review

7.1 The Ministry shall monitor the implementation of the Regulations.

8. Contact

The contact person at the Ministry of ICT, Innovation and Youth Affairs are:

Joe Mucheru, EGH
Cabinet Secretary
Ministry of ICT, Innovation and Youth Affairs
P.O. Box 30025-00100
NAIROBI
Telephone: 020-4920002
Email: joe.mucheru@ict.go.ke
Or
Jerome Ochieng, CBS,
Principal Secretary
State Department of ICT and Innovation
10th floor Telposta Towers
P.O. Box 30025-00100
NAIROBI
Telephone: 020-4920000
Email: ps@ict.go.ke

EXPLANATORY MEMORANDUM TO THE DATA PROTECTION (COMPLIANCE AND ENFORCEMENT) REGULATIONS, 2021

PART I

Name of the Statutory Instrument: The Data Protection (Compliance and Enforcement) Regulations, 2021.

Name of the Parent Act: The Data Protection Act, No. 24 of 2019.

Enacted Pursuant to: Section 71 of the Data Protection Act, No. 24 of 2019.

Name of the Ministry/ Department: Ministry of Information, Communications, Technology, Innovation and Youth Affairs.

Gazetted on:

Tabled on:

PART II

1. Purpose of the Statutory instrument the Data Protection (Compliance and Enforcement) Regulations, 2021.

1.1. The purpose of these Regulations is to is to give effect to section 56 of the Data Protection Act, No.24 of 2019 of the Laws of Kenya.

1.2. The Regulations provide for, among other things, the manner of lodging of a complaint, criteria for admission of complaints, discontinuation of a complaint, withdrawal of a complaint, joint consideration of complaints and the language of proceedings before the Data Commissioner.

2. Legislative Context

2.1. The Data Protection Act, No.24 of 2019, was assented to on the 8th November, 019 and came into force on the 25th November, 2019.

2.2. Section 71(1) of the Data Protection Act, No.24 of 2019 provides that the Cabinet Secretary may make regulations to give effect to the Act, and for prescribing anything required or necessary to be prescribed by or under the Act.

3. Policy Background.

3.1. Parliament enacted the Data Protection Act, No.24 of 2019 in November, 2019 and over the past two years and Data Controllers have been complying with the provisions of the Act. The Act on its own, however, is not sufficient since it does not provide guidelines on all matters relating to lodging of complaints with the Data Commissioner pursuant to section 56 of the Act and the manner of determining the complaints. In order to provide further clarity on various aspects of complaints management, it is therefore necessary to have regulations to govern complaints lodged by any person or by a data subject in accordance with section 56 of the Data Protection Act, No.24 of 2019.

3.2. These Regulations have been divided into three parts namely: -Part I: Preliminary; Part II: Complaint Handling Procedure; and Part III: Enforcement Provisions.

4. Consultation outcome

4.1. The Data Protection (Compliance and Enforcement) Regulations, 2021, have taken into account the views of key stakeholders such as the key data holders, the academia, the Judiciary, international organizations, government ministries, departments and agencies, the civil society organization involved in activities of personal data processing in the country, the general public among others.

5. Guidance

5.1. The Ministry of Information, Communications, Technology, Innovation and Youth Affairs will sensitize stakeholders including Parliament, key data handlers and the general public, on the provisions of, the Data Protection (Compliance and

Enforcement) Regulations, 2021, and the monitoring and evaluating mechanism, to ensure that the Regulation serve the purpose for which they have been made.

6. Impact

6.1. **The Impact on Fundamental Rights and Freedoms:** Alternative Dispute Resolutions are necessary in order to dispose of disputes to avoid participating in lengthy and traumatizing court trials. These Regulations therefore do not limit fundamental rights and freedoms.

6.2. **The impact on the Private Sector**: Alternative Dispute Resolution Mechanisms expedite the disposal of disputes involving the private sector, allowing private sector actors to speedily return to their business and economic activities. This will have a positive impact on national economic growth and performance.

6.3. **The impact on the Public Sector**: Alternative Dispute Resolution Mechanisms are a good avenue to save on public resources. When parties have entered into the agreements, the same reduces the time and cost of trial and saves resources that can be utilized in other more complex and convoluted trials.

7. Monitoring and review

7.1. The Ministry of Information, Communications, Technology, Innovation and Youth Affairs shall monitor the implementation of the Data Protection (Compliance and Enforcement) Regulations, 2021 and this shall be done through quarterly reports from the Office of the Data Commissioner.

8. Contact.

The contact person at the Ministry of ICT, Innovation and Youth Affairs are:
Joe Mucheru, EGH
Cabinet Secretary
Ministry of ICT, Innovation and Youth Affairs
P.O. Box 30025-00100
NAIROBI
Telephone: 020-4920002

Email: joe.mucheru@ict.go.ke
Or

Jerome Ochieng, CBS,
Principal Secretary
State Department of ICT and Innovation
10th floor Telposta Towers
P.O. Box 30025-00100
NAIROBI
Telephone: 020-4920000
Email: ps@ict.go.ke

EXPLANATORY MEMORANDUM TO

THE DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATIONS, 2021

PART I: PARTICULARS OF THE STATUTORY INSTRUMENT

Name of the Statutory Instrument:	The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021
Name of the Parent Act:	Data Protection Act, No. 24 of 2019
Enacted Pursuant to:	Sections 18 (2) of the Data Protection Act, No. 24 of 2019
Name of the Ministry:	Ministry of ICT, Innovation and Youth Affairs
Department:	State Department for ICT & Innovation

Gazetted on:

Tabled on:

PART II: OBJECTS AND PURPOSE OF STATUTORY INSTRUMENT

1. Purpose of the Statutory instrument

1.1. The purpose of the Statutory Instrument is to give effect to section 18 (2) of the Data Protection Act, 2019 which provides for the requirement for registration of data controllers and data processors by the Office of the Data Commissioner. The Regulations stipulates the procedure for registration of data controllers and data processors by the Office of the Data Commissioner and specifically specify the categories of data controllers and data processors required for mandatory registration

4.7. Another concern that arose during the consultations was, the registration renewal period which had been suggested to be annually. This too was revised and proposed to be every two (2) years.

4.8. Ultimately the public participation acknowledged that the public and Kenya at large is ripe and ready to tap into the opportunities that come with being on the digital map at the same time cognizant of the conversation around the world on the use and protection of personal data.

4.9. In this regard, it is summed that the proposed Regulations have been exposed to an extensive public participation program and attains the public participation threshold as required by the Statutory Instruments Act, 2013.

5. Guidance

The Ministry of Information, Communications, Technology, Innovation and Youth Affairs will sensitize key stakeholders including public and private bodies, National Government Ministries and Independent Offices on the provisions of the regulations and the implementation mechanism, to ensure that the Act and Regulations serve the purpose for which they have been made.

6. Impact

6.1. **The Impact on Fundamental Rights and Freedoms**: These Regulations do not limit any fundamental rights and freedoms. The draft Regulations are not expected to have a negative impact on fundamental rights of persons or institutions that are subject to it. The Regulations seeks to ensure actualization of the Bill of Rights, particularly on the right to privacy under Article 31 of the Constitution.

6.2. The Regulations do not have any possible negative impact on the environment or environmental rights of the people.

6.3. The draft Regulations does not contain any provisions that are likely to impair or prejudice the right to any fair administrative action of an individual.

6.4. **The impact on the Private Sector**: The Regulations imposes additional costs on the private sector by requiring registration and the renewal fees in registering as data controllers or data processors. The fees payable are set out under the Second Schedule to the draft Regulations.

6.5. However, despite these additional costs, it is expected the registration of data controllers and data processors would motivate the legal compliance of all entities that are processing personal data. This will consequently enhance the business management aspect of processing personal data by behooving a better management and storage of personal data, leading to better business practices.

6.6. The requirement to register, which attracts this cost, would equally enhance customer security given that all persons processing personal data would register. This would ensure personal data of citizens is handled in accordance with the Law.

6.7. **The impact on the Public Sector**: The Regulation imposes additional costs on the public sector by requiring entities within the public sector to register either as data controllers or data processors. The Regulations imposes registration and renewal fees set out in the Second Schedule. These costs are additional compliance costs that would be borne by the public sector.

6.8. The anticipated benefit for the public sector gains is the assurance to the general public and business community that the public sector entities have committed to handling personal data of data subjects in compliance with the Data Protection Act specifically in adherence to the principles of data protection. A positive externality will flow from this imposition to extent that it would directly create demand for more business, hence contributing to the growth of the gross domestic product (GDP). Additionally, simplified provisions of registration reduce the compliance costs.

7. Monitoring and review

The Office of the Data Commissioner shall monitor the implementation of these Regulations. This shall be done through periodic audits of compliance with the law. The Office of the Data Commissioner shall prepare annual reports on its activities an up to date register and checking the compliance of data controllers and data processors to the Ministry and National Assembly.

8. Contact

The contact person at the Ministry of ICT, Innovation and Youth Affairs are:

Joe Mucheru, EGH
Cabinet Secretary
Ministry of ICT, Innovation and Youth Affairs
P.O. Box 30025-00100
NAIROBI
Telephone: 020-4920002
Email: joe.mucheru@ict.go.ke

Or

Jerome Ochieng, CBS,
Principal Secretary
State Department of ICT and Innovation
10th floor Telposta Towers
P.O. Box 30025-00100
NAIROBI
Telephone: 020-4920000
Email: ps@ict.go.ke

ANNEX 2

SPECIAL ISSUE 1977

Kenya Gazette Supplement No. 236 *31st December, 2021*

(Legislative Supplement No. 106)

LEGAL NOTICE NO. 263

THE DATA PROTECTION ACT

(*No.* 24 *of* 2019)

THE DATA PROTECTION (GENERAL) REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation

THE DATA PROTECTION ACT, 2019

(No. 24 of 2019)

IN EXERCISE of the powers conferred by section 71 of the Data Protection Act, 2019, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs makes the following Regulations—

THE DATA PROTECTION (GENERAL) REGULATIONS, 2021

PART I—PRELIMINARY

Citation.

1. These Regulations may be cited as the Data Protection (General) Regulations, 2021.

Interpretation.

2. In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection Act, 2019;

"Data Commissioner" means the person appointed as such pursuant to section 6 of the Act; and

No. 24 of 2019.

"Office" has the meaning assigned to it under the Act.

Exemption.
L. N. No.196 of 2020.

3. These Regulations shall not apply to civil registration entities specified under the Data Protection (Civil Registration) Regulations, 2020.

PART II— ENABLING THE RIGHTS OF A DATA SUBJECT

Processing on the basis of consent.

4. (1) Where processing is based on consent in accordance with section 32 of the Act, a data controller or data processor shall, in seeking consent prior to the processing, inform the data subject of'—

(a) the identity of the data controller or data processor;

(b) the purpose of each of the processing operations for which consent is sought;

(c) the type of personal data that is collected and used;

(d) information about the use of the personal data for automated decision-making, where relevant;

(e) the possible risks of data transfers due to absence of an adequacy decision or appropriate safeguards;

(f) whether the personal data processed shall be shared with third parties;

(g) the right to withdraw consent; and

(h) the implications of providing, withholding or withdrawing consent.

(2) The information under sub-regulation (1) may be presented to the data subject through a written notice, oral statement, audio or video message.

(3) In obtaining consent from a data subject, a data controller or a data processor shall ensure that the—

(a) data subject has capacity to give consent;

(b) data subject voluntarily gives consent; and

(c) consent is specific to the purpose of processing.

(4) Pursuant to section 32(4) of the Act, consent shall be considered to have been given freely, unless where —

(a) it is presumed on the basis that the data subject did not object to a proposal to processing of their personal data in a particular manner;

(b) it is presented as a non-negotiable part of the terms and conditions for processing;

(c) the data subject is unable to refuse or withdraw their consent without detriment;

(d) the data controller or data processor merges several purposes for processing without seeking specific consent for each purpose; or

(e) the intention of the data subject is ambiguous.

(5) Where the data subject withdraws consent to any part of the processing, the data controller or data processor shall restrict the part of the processing in respect of which consent is withdrawn, subject to section 34 of the Act.

Lawful basis for processing.

5.(1) A data controller or data processor may process data without consent of a data subject if the processing is necessary for any reason set out in section 30(1) (b) of the Act.

(2) Processing under sub-regulation (1) shall only rely on one legal basis for processing at a time, which shall be established before the processing.

(3) The legal basis relied on under sub-regulation (1) shall be demonstrable at all times and where a data controller uses multiple bases for different processing, the data controller shall—

(a) distinguish between the legal bases being used; and

(b) respond to any data subject rights requests.

Mode of collection of personal data.

6. (1) Pursuant to section 28(2) of the Act, a data controller or data processor may collect personal data indirectly from—

(a) any person other than the data subject;

(b) publications or databases;

(c) surveillance cameras, where an individual is identifiable or reasonably identifiable;

(d) information associated with web browsing; or

(e) biometric technology, including voice or facial recognition.

(2) A data controller or data processor shall, in collecting personal data—

(a) ensure that processing is limited to personal data which the

data subject has permitted the data controller or data processor to collect;

(b) undertake steps to ensure that personal data is accurate, notin excessive and up to date;

(c) undertake processes to secure personal data; and

(d) comply with the lawful processing principles set out under part IV of the Act.

(3) Where a data controller or data processor collects personal data indirectly, the data controller or data processor shall within fourteen days inform the data subject of the collection.

(4) Where a data controller or data processor intends to use personal data for a new purpose, the data controller or data processor shall ensure that the new purpose is compatible with the initial purpose for which the personal data was collected.

(5) Where the new purpose is not compatible with the initial purpose, a data controller or data processor shall seek fresh consent from the data subject in accordance with regulation 4.

Restriction to processing

7. (1) Pursuant to section 34 of the Act, a data subject may request a data controller or data processor to restrict the processing of their personal data on grounds that—

(a) the data subject contests the accuracy of their personal data;

(b) the personal data has been unlawfully processed and the data subject opposes the erasure and requests restriction instead;

(c) the data subject no longer needs their personal data but the data controller or data processor requires the personal data to be kept in order to establish, exercise or defend a legal claim; or

(d) a data subject has objected to the processing of their personal data under regulation 8 and a data controller or data processor is considering legitimate grounds that override those of the data subject.

(2) A request for restriction to processing of personal data on any of the grounds provided under section 34 of the Act may be made in Form DPG 1 set out in the First Schedule.

(3) A data controller or data processor shall within fourteen days of the request for restriction pursuant to sub-regulation (2), and without charging any fee—

(a) admit and implement the request;

(b) indicate on the data controller or data processors system that the processing of the personal data has been restricted; and

(c) notify any relevant third party of the restriction where personal data, subject to such restriction, may have been shared.

(4) A data controller or a data processor may implement a

restriction to processing request by—

(a) temporarily moving the personal data to another processing system;

(b) making the personal data unavailable to third parties; or

(c) temporarily removing published data specific to the data subject from its website or other public medium in its control.

(5) A data controller or data processor may decline to comply with a request for restriction in processing, where such request is manifestly unfounded or excessive.

(6) Where a data controller or data processor declines a request on any of the grounds provided under section 34(2) of the Act, the data controller or data processor shall within fourteen days of the refusal, notify the data subject of the refusal, in writing, and shall provide the reasons for the decision.

(7) A data controller or data processor shall not process personal data that has been restricted, except to store the personal data, in accordance with section 34(2)(a) of the Act.

Objection to processing.

8. (1) Pursuant to section 36 of the Act, a data subject may request a data controller or data processor not to process all or part of their personal data, for a specified purpose or in a specified manner.

(2) A request to object the processing may be made in Form DPG 1 set out in the First schedule.

(3) A data controller or data processor shall, without charging any fee, comply with a request for objection under sub-regulation (2) within fourteen days of the request.

(4) The right to object to processing applies as an absolute right where the processing is for direct marketing purposes which includes profiling to the extent that it is related to such direct marketing.

(5) Where the data subject objects to processing for direct marketing purposes, the personal data shall not be processed for such purposes.

(6) Where the right to object to processing is not absolute and the request by a data subject has been declined, the data controller or data processor shall inform the data subject of—

(a) the reasons for declining the request for objection; and

(b) the right to lodge a complaint to the Data Commissioner where dissatisfied.

(7) Where a 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, the data controller or data processor shall inform the data subject of—

(a) the reasons for declining the request for objection; and

(b) the right to lodge a complaint to the Data Commissioner where dissatisfied.

Data access request.

9. (1) A data subject has a right to obtain from the data controller or data processor confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data and the information as to—

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in other countries or territories;

(d) where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and

(e) where the personal data is not collected from the data subject, any available information as to the source of collection.

(2) A data subject may request to access their personal data in Form DPG 2set out in the First Schedule.

(3) A data controller or data processor shall—

(a) on request, provide access to a data subject of their personal data in its possession;

(b) put in place mechanisms to enable a data subject to proactively access or examine their personal data; or

(c) provide the data subject with a copy of their personal data.

(4) A data controller or a data processor shall comply with a request by a data subject to access their personal data within seven days of the of the request.

(5) Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(6) Compliance with a request for access to personal data shall be free of charge.

Rectification of personal data.

10. (1) Pursuant to section 40 of the Act, a data subject may request a data controller or data processor to rectify their personal data, which is untrue, inaccurate, outdated, incomplete or misleading.

(2) A request for rectification may be made in Form DPG 3 set out in the First Schedule.

(3) An application for rectification of personal data may be supported by such documents as may be relevant to the rectification sought.

(4) A data controller or data processor shall within fourteen days

of the request, rectify an entry of personal data in the database where the data controller or data processor is satisfied that a rectification is necessary.

(5) Where a request for rectification is declined, a data controller or data processor shall, in writing, notify a data subject of that refusal within seven days and shall provide reasons for refusal.

(6) A request for rectification shall made free of charge.

Data portability request.

11. (1) Pursuant to section 38 of the Act, a data subject may apply to port or copy their personal data from one data controller or data processor to another.

(2) A request for data portability may be made in Form DPG 4set out in the First Schedule.

(3) A data controller or data processor shall within thirty days of the request and upon payment of the prescribed fees port personal data to the data subject's choice of recipient.

(4) Where fee is charged under sub-regulation (2), the fee shall be reasonable and not exceed the cost incurred to actualize the request.

(5) A data controller or data processor who receives personal data that has been ported shall, with respect to such data, comply with the requirement of the Act and these Regulations.

(6) Where a data controller or data processor declines the portability request, a data controller or data processor shall, within seven days, notify the data subject of the decline and the reasons for such decline in writing.

(7) The exercise of the right to data portability by a data subject shall not negate the rights of a data subject provided under the Act.

Right of erasure.

12. (1) Pursuant to section 40 (1) (b) of the Act, a data subject may, request a data controller or data processor to erase or destroy personal data held by the data controller or data processor where —

(a) the personal data is no longer necessary for the purpose which it was collected;

(b) the data subject withdraws their consent that was the lawful basis for retaining the personal data;

(c) the data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing;

(d) the processing of personal data is for direct marketing purposes and the individual objects to that processing;

(e) the processing of personal data is unlawful including in breach of the lawfulness requirement; or

(f) the erasure is necessary to comply with a legal obligation.

(2) A data subject may request for erasure of their personal data held by a data controller or data processor in Form DPG5 set out in the

First Schedule.

(3) A data controller or data processor shall respond to a request for erasure under sub-regulation (2) within fourteen days of the request.

(4) A right of erasure does not apply if processing is necessary for one of the following reasons—

(a) to exercise the right of freedom of expression and information;

(b) to comply with a legal obligation;

(c) for the performance of a task carried out in the public interest or in the exercise of official authority;

(d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

(e) for the establishment, exercise or defence of a legal claim.

(5) A request for erasure shall be free of charge.

Exercise of rights by others.

13. (1) Subject to section 27 of the Act, where a person duly authorised by a data subject seeks to exercise the rights on their behalf, the data controller or data processor shall act in the best interests of the data subject.

(2) Where the data subject is a child, a data controller or data processor shall ensure that—

(a) a person exercising the right is appropriately identified;

(b) profiling of a child that is related to direct marketing is prohibited; and

(c) the parent or guardian is informed of the inherent risks in processing and the safeguards put in place.

(3) Where a data controller or a data processor is uncertain as to the existence of a relationship between the duly authorised person and the data subject, the data controller or data processor may restrict the request of exercising a right on behalf of the data subject until evidence to the contrary is adduced.

PART III—RESTRICTIONS ON THE COMMERCIAL USE OF PERSONAL DATA

Interpretation of commercial purposes.

14. (1) For the purposes of section 37 (1) of the Act, a data controller or data processor shall be considered to use personal data for commercial purposes where personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(2) A data controller or data processor is considered to use personal data to advance commercial interests where personal data is

used for direct marketing through—

(a) sending a catalogue through any medium addressed to a data subject;

(b) displaying an advertisement on an online media site where a data subject is logged on using their personal data; or

(c) sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

(3) Marketing is not direct where personal data is not used or disclosed to identify or target particular recipients.

Permitted commercial use of personal data.

15. (1) A data controller or data processor may use personal data, other than sensitive personal data, concerning a data subject for the purpose of direct marketing where—

(a) the data controller or data processor has collected the personal data from the data subject;

(b) a data subject is notified that direct marketing is one of the purposes for which personal data is collected;

(c) the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

(d) the data controller or data processor provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or

(e) the data subject has not made an opt out request.

(2) A data controller or data processor shall not transmit, for the purposes of direct marketing, messages by any means unless the data controller or data processor indicates particulars to which a data subject may send a request to restrict such communications without incurring charges.

(3) A person shall neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail—

(a) where the identity of the person on whose behalf the communication has been sent has been disguised or concealed;

(b) where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided; or

(c) where there is use of automated calling systems without human intervention.

(4) A data controller or data processor who uses personal data for commercial purposes without the consent of the data subject commits an offence and is liable, on conviction, to a fine not exceeding twenty thousand shillings or to a term of imprisonment not exceeding six months, or to both fine and imprisonment.

Features of an opt out message.

16. (1) An opt out mechanism contemplated under regulation 15(1)(d) shall—

(a) have a visible, clear and easily understood explanation of how to opt out;

(b) include a process for opting out that requires minimal time and effort;

(c) provide a direct and accessible communication channel;

(d) be free of charge or where necessary involve a nominal cost to a data subject; and

(e) be accessible to persons with a disability.

(2) Where a data subject has opted out, a data controller or data processor shall not use or disclose their personal data for the purpose of direct marketing, in accordance with the data subject's request.

Mechanisms to comply with opt out requirement.

17. (1) In communicating with a data subject on direct marketing, a data controller or data processor shall include a statement which is prominently displayed, or otherwise draws the attention of the data subject to the fact that the data subject may make an opt out request.

(2) A data controller or data processor may, in complying with an opt out requirement—

(a) clearly indicate, in each direct marketing message, that a data subject may opt out of receiving future messages by replying with a single word instruction in the subject line;

(b) ensure that a link is prominently located in the email, which takes a data subject to a subscription control centre;

(c) clearly indicate that a data subject may opt out of future direct marketing by replying to a direct marketing text message with a single word instruction;

(d) inform the recipient of a direct marketing phone call that they can verbally opt out from any future calls; and

(e) include instructions on how to opt out from future direct marketing, in each message.

(3) A data controller or a data processor may use an opt out mechanism that provides a data subject with the opportunity to indicate their direct marketing communication preferences, including the extent to which they wish to opt out.

(4) Despite sub-regulation (3), a data controller or data processor shall provide a data subject with an option to opt out of all future direct marketing communications as one of outlined preferences.

Request for restriction of further direct marketing.

18. (1) A data subject may request a data controller or data processor to restrict use or disclosure of their personal data, to a third party, for the purpose of facilitating direct marketing.

(2) No fee shall be charged to a data subject for making or giving

effect to a request under this Part.

(3) A data controller or data processor shall restrict use or disclosure of personal data for the purpose of facilitating direct marketing by a third party within seven days of the request.

PART IV—OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

Retention of personal data.

19. (1) Pursuant to section 39 of the Act, a data controller or data processor shall retain personal data processed for a lawful purpose, for as long as may be reasonably necessary for the purpose for which the personal data is processed.

(2) A data controller or data processor shall—

(a) establish personal data retention schedule with appropriate time limits for the periodic review of the need for the continued storage of personal data that is no longer necessary or where the retention period is reached; and

(b) erase, delete anonymise or pseudonymise personal data upon the lapse of the purpose for which the personal data was collected.

(3) A personal data retention schedule established under paragraph (2)(a) shall outline the —

(a) purpose for retention;

(b) the retention period;

(c) provision for periodic audit of the personal data retained; and

(d) actions to be taken after the audit of the personal data retained.

(4) An audit of the retained data under paragraph (3)(c), shall seek to—

(a) review records with a view of identifying personal data that no longer requires to be retained and permanently delete the personal data;

(b) ensure the retained data is accurate and up-to-date;

(c) specify the purpose for retention of personal data;

(d) ensure that the personal data security measures are adequate; and

(e) identify the best cause of action where personal data retention period lapses.

(5) A data controller or data processor shall establish appropriate time limits for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

(6) The personal data storage limitation period and data retention schedule outlined under paragraph (2)(a) may be included as part of the policy envisaged in regulation 23.

Requests to deal anonymously or pseudonymously.

20. (1) A data subject may request a data controller or data processor to process their personal data anonymously or pseudonymously where the data subject wishes—

(a) not to be identified;

(b) to avoid subsequent contact such as direct marketing from an entity or third parties;

(c) to enhance their privacy on the whereabouts of a data subject;

(d) to access services such as counselling or health services without it becoming known to others;

(e) to express views in a public arena without being personally identified; or

(f) to minimise the risk of identity fraud.

(3) A data controller or data processor may accede to the request where satisfied that the request is based on any of the reasons specified under sub-regulation (1) and where the request is in the best interests of the data subject.

Sharing of personal data.

21. (1) Subject to section 25 of the Act, a data controller or data processor may share or exchange personal data collected, upon request, by another data controller, data processor, third party or a data subject.

(2) A data controller or data processor shall determine the purpose and means of sharing personal data from one data controller or data processor to another.

(3) Data sharing outlined under this regulation may include—

(a) providing personal data to a third party by whatever means by the data controller or data processor;

(b) receiving personal data from a data controller or data processor as joint participant in a data sharing arrangement;

(c) exchanging or transmission of personal data;

(d) providing third party with access to personal data on the data controller's information systems;

(e) separate or joint initiatives by data controllers or data processors to pool personal data making the data available to each other or a third-party subject to entering into an agreement, as may be applicable; or

(f) routine data sharing between data controllers on a regular or pre-planned basis.

(4) In carrying out any routine data sharing as contemplated under paragraph (3)(f), a data controller shall enter into agreements prior to data sharing.

(5) For the avoidance of doubt, the sharing of data within the organizational structures of a data controller or data processor is not

considered as a data sharing.

(6) A request for sharing personal data under this regulation shall be in writing, and shall specify—

(a) the purpose for which personal data is required;

(b) the duration for which personal data shall be retained; and

(c) proof of the safeguards put in place to secure personal data from unlawful disclosure.

Automated individual decision making.

22. (1) In this regulation—

"an automated individual decision-making" means a decision made by automated means without any human involvement.

(2) Pursuant to section 35 of the Act, a data controller or data processor shall—

(a) inform a data subject when engaging in processing based on automated individual decision making;

(b) provide meaningful information about the logic involved;

(c) ensure—

(i) specific transparency and fairness requirements are in place;

(ii) rights for a data subject to oppose profiling and specifically profiling for marketing are present; and

(iii) where conditions specified under section 31 of the Act arise, a data protection impact assessment is carried out;

(d) explain the significance and envisaged consequences of the processing;

(e) ensure the prevention of errors;

(f) use appropriate mathematical or statistical procedures;

(g) put appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors;

(h) process personal data in a way that eliminates discriminatory effects and bias; and

(i) ensure that a data subject can obtain human intervention and express their point of view.

Data protection policy.

23. (1) A data controller or data processor shall develop, publish and regularly update a policy reflecting their personal data handling practices.

(2) A policy under sub-regulation (1) may include—

(a) the nature of personal data collected and held;

(b) how a data subject may access their personal data and

exercise their rights in respect to that personal data;

(c) complaints handling mechanisms;

(d) lawful purpose for processing personal data;

(e) obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;

(f) the retention period and schedule contemplated under regulation 19; and

(g) the collection of personal data from children, and the criteria to be applied.

Contract between data controller and data processor.

24. (1) Subject to section 42(2)(b) of the Act, a data controller shall engage a data processor, through a written contract.

(2) The contract envisaged under sub-regulation (1) shall include the following particulars—

(a) processing details including—

(i) the subject matter of the processing;

(ii) the duration of the processing;

(iii) the nature and purpose of the processing;

(iv) the type of personal data being processed;

(v) the categories of data subjects; and

(vi) the obligations and rights of the data controller;

(b) instructions of the data controller;

(c) duty on the data processors to obtain a commitment of confidentiality from any person or entity that the data processors allows to process the personal data;

(d) security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure;

(e) provision stipulating that all personal data must be permanently deleted or returned on termination or lapse of the agreement, as decided by the data controller; and

(f) auditing and inspection provisions by the data controller.

Obligations of a data processor.

25. (1) A data processor shall not engage the services of a third party without the prior authorisation of the data controller.

(2) Where authorisation is given, the data processor shall enter into a contract with the third party.

(3) The contract contemplated under sub-regulation (1) shall include such particulars as provided for under sub-regulation 24(2).

(4) A data processor shall remain liable to the data controller for the compliance of any third party that they engage.

Requirement for specified processing to be done in Kenya.

26. (1) Pursuant to section 50 of the Act, a data controller or data processor who processes personal data for the purposeof strategic interest of the state outlined under sub-regulation (2) shall —

(a) process such personal data through a server and data centre located in Kenya; or

(b) store at least one serving copy of the concerned personal datain a data centre located in Kenya.

(2) The purpose contemplated under sub-regulation (1) includes the processing of personal data for the purpose of—

(a) administering of the civil registration and legal identity management systems;

(b) facilitating the conduct of elections for the representation of the people under the Constitution;

(c) overseeing any system for administering public finances by any state organ;

(d) running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018; No.5 of 2018.

(e) offering any form of early childhood education and basic education under the Basic Education Act, 2013; or No.14 of 2013.

(f) provision of primary or secondary health care for a data subject in the country.

(3) Despite (2), the Cabinet Secretary may require a data controller who processes personal data outside Kenya to comply with sub-regulation (1), where the data controller—

(a) has been notified that personal data outside Kenya has been breached or its services have been used to violate the Act and has not taken measures to stop or handle the violation; and

(b) resists, obstructs or fails to comply with requests of the Data Commissioner or any other relevant authority in—

(i) cooperating to investigate and handle such violations; or

(ii) neutralising and disabling the effect of cyber security protection measures.

PART V—ELEMENTS TO IMPLEMENT DATA PROTECTION BY DESIGN OR BY DEFAULT

Data protection by design or default.

27. A data controller or data processor shall in processing of personal data —

(a) establish the data protection mechanisms set out under the Act and these Regulations are embedded in the processing;

and

(b) design technical and organisational measures to safeguard and implement the data protection principles.

Elements of data protection by design or default

28. The elements for the protection of personal data by design or by default that are necessary to implement the data protection principles outlined under section 25 of the Act are as set out in this Part.

Elements for principle of lawfulness.

29. The elements necessary to implement the principle of lawfulness include—

(a) appropriate legal basis or legitimate interests clearly connected to the specific purpose of processing;

(b) processing that is necessary for the purpose;

(c) the data subject being granted the highest degree of autonomy possible with respect to control over their personal data;

(d) a data subject knowing what they consented to and a simplified means to withdraw consent; and

(e) restriction of processing where the legal basis or legitimate interests ceases to apply.

Elements for principle of transparency.

30. The elements necessary to implement the principle of transparency include—

(a) the use of clear, simple and plain language to communicate with a data subject to enable a data subject to make decisions on the processing of their personal data;

(b) making the information on the processing easily accessible to the data subject;

(c) providing the information on the processing to the data subject at the relevant time and in the appropriate form;

(d) the use of machine-readable language to facilitate and automate readability and clarity;

(e) providing a fair understanding of the expectation with regards to the processing particularly for children or other vulnerable groups; and

(f) providing details of the use and disclosure of the personal data of a data subject.

Elements for principle of purpose limitation.

31. The elements necessary to implement the principle of purpose limitation include—

(a) specifying the purpose for each processing of personal data;

(b) determining the legitimate purposes for the processing of personal data before designing organisational measures and safeguards;

(c) the purpose for the processing being the determinant for

personal data collected;

(d) ensuring a new purpose is compatible with the original purpose for which the data was collected;

(e) regularly reviewing whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation; and

(f) the use of technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.

Elements for principle of integrity, confidentiality and availability.

32. The elements necessary to implement the principle of integrity, confidentiality and availability include—

(a) having an operative means of managing policies and procedures for information security;

(b) assessing the risks against the security of personal data and putting in place measures to counter identified risks;

(c) processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;

(d) ensuring only authorised personnel have access to the data necessary for their processing tasks;

(e) securing transfers shall be secured against unauthorised access and changes;

(f) securing data storage from use, unauthorised access and alterations;

(g) keeping back-ups and logs to the extent necessary for information security;

(h) using audit trails and event monitoring as a routine security control;

(i) protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;

(j) having in place routines and procedures to detect, handle, report, and learn from data breaches; and

(k) regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

Elements for principle of data minimization.

33. The elements necessary to implement the principle of data minimization include—

(a) avoiding the processing of personal data altogether when this is possible for the relevant purpose;

(b) limiting the amount of personal data collected to what is necessary for the purpose;

(c) ability to demonstrate the relevance of the data to the processing in question;

(d) pseudonymising personal data as soon as the data is no longer necessary to have directly identifiable personal data, and storing identification keys separately;

(e) anonymizing or deleting personal data where the data is no longer necessary for the purpose;

(f) making data flows efficient to avoid the creation of more copies or entry points for data collection than is necessary; and

(g) the application of available and suitable technologies for data avoidance and minimization.

Elements for principle of accuracy.

34. The elements necessary to implement the principle of accuracy include—

(a) ensuring data sources are reliable in terms of data accuracy;

(b) having personal data particulars being accurate as necessary for the specified purposes;

(c) verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation to how often it may change;

(d) erasing or rectifying inaccurate data without delay;

(e) mitigating the effect of an accumulated error in the processing chain;

(f) giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed;

(g) having personal data accurate at all stages of the processing and carrying out tests for accuracy at critical steps;

(h) updating personal data as necessary for the purpose; and

(i) the use of technological and organisational design features to decrease inaccuracy.

Elements for principle of storage limitation.

35. The elements necessary to implement the principle of storage limitation include—

(a) having clear internal procedures for deletion and destruction;

(b) determining what data and length of storage of personal data that is necessary for the purpose;

(c) formulating internal retention statements of implementing them;

(d) ensuring that it is not possible to re-identify anonymised data or recover deleted data and testing whether this is possible;

(e) the ability to justify why the period of storage is necessary for the purpose, and disclosing the rationale behind the retention period; and

(f) determining which personal data and length of storage is necessary for back-ups and logs.

Elements for principle of fairness.

36. The elements necessary to implement the principle of fairness include—

(a) granting the data subjects the highest degree of autonomy with respect to control over their personal data;

(b) enabling a data subject to communicate and exercise their rights;

(c) elimination of any discrimination against a data subject;

(d) guarding against the exploitation of the needs or vulnerabilities of a data subject; and

(e) incorporating human intervention to minimize biases that automated decision-making processes may create.

PART VI—NOTIFICATION OF PERSONAL DATA BREACHES

Categories of notifiable data breach.

37. (1) For the purpose of section 43 of the Act, a data breach is taken to result in real risk of harm to a data subject if that data breach relates to —

(a) the data subject's full name or identification number and any of the personal data or classes of personal data relating to the data subject set out in the Second Schedule; or

(b) the following personal data relating to a data subject's account with a data controller or data processor—

(i) the data subject's account identifier, such as an account name or number; and

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

(2) A breach of any personal data envisaged under sub-regulation (1) amounts to notifiable data breach under section 43 of the Act.

(3) The personal data or classes of personal data set out in the Second Schedule excludes —

(a) any personal data that is publicly available; or

(b) any personal data that is disclosed to the extent that is required or permitted under any written law.

(4) The personal data referred to in sub-paragraph (3) (a) shall not be publicly available solely because of any data breach.

Notification to Data Commissioner.

38. (1) A notification by data controller to the Data Commissioner of a notifiable data breach under section 43 of the Act shall include—

(a) the date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;

(b) a chronological account of the steps taken by the data

controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;

(c) details on how the notifiable data breach occurred, where applicable;

(d) the number of data subjects or other persons affected by the notifiable data breach;

(e) the personal data or classes of personal data affected by the notifiable data breach;

(f) the potential harm to the affected data subjects as a result of the notifiable data breach;

(g) information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissioner of the occurrence of the notifiable data breach to—

(i) eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or

(ii) address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

(h) the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach; or

(i) contact information of an authorized representative of the data controller or data processor.

(2) Where the data controller intends not to communicate a notifiable data breach to a data subject affected by such breach, under the conditions set out in section 43(1) (b) of the Act, the notification to the Data Commissioner under sub-regulation (1) shall additionally specify the grounds for not notifying the affected data subject.

PART VII—TRANSFER OF PERSONAL DATA OUTSIDE KENYA

Interpretation of the Part VII.

39. In this Part, unless the context otherwise requires —

(a) "data in transit" means personal data transferred through Kenya in the course of onward transportation to a country or territory outside Kenya, without the personal data being accessed or used by, or disclosed to, any entity while in Kenya, except for the purpose of such transportation;

(b) "recipient" means an entity that receives in a country or

territory outside Kenya the personal data transferred to the recipient by or on behalf of the transferring entity, but does not include an entity that receives the personal data solely as a network service provider or carrier;

(c) "transferring entity" means an entity that transfers personal data from Kenya to a country or a territory outside Kenya but does not include an entity dealing with data in transit; and

(d) "relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes.

General principles for transfers of personal data out of the country.

40. A data controller or data processor who is a transferring entity shall before transferring personal data out of Kenya ascertain that the transfer is based on—

(a) appropriate data protection safeguards;

(b) an adequacy decision made by the Data Commissioner;

(c) transfer as a necessity; or

(d) consent of the data subject.

Transfers on the basis of appropriate safeguards.

41. (1) A transfer of personal data to a another country or a relevant international organisation is based on the existence of appropriate safeguards where—

(a) a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations; or

(b) the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.

(2) Where a transfer of data takes place in reliance on sub-regulation (1)—

(a) the transfer shall be documented;

(b) the documentation shall be provided to the Commissioner on request; and

(c) the documentation shall include—

(i) the date and time of the transfer;

(ii) the name of the recipient;

(iii) the justification for the transfer; and

(iv) a description of the personal data transferred.

Deeming of appropriate safeguards.

42. For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49 (1) of the Act and these Regulations, any country or a territory is taken to have such

safeguards if that country or territory has—

(a) ratified the African Union Convention on Cyber Security and Personal Data Protection;

(b) a reciprocal data protection agreement with Kenya; or

(c) a contractual binding corporate rules among a concerned group of undertakings or enterprises.

Binding corporate rules.

43. (1) The contractual binding corporate rules contemplated under regulation 41 shall be valid if they—

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in sub-regulation (2).

(2) The binding corporate rules referred to in sub-regulation (1) shall specify—

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of another country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles;

(e) the rights of data subjects in regard to processing and the means to exercise those rights;

(f) the complaint procedures; and

(g) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules.

Transfers on the basis of an adequacy decision.

44. (1) A transfer of personal data to another country or a relevant international organization is based on an adequacy decision where the Data Commissioner makes a decision that—

(a) the other country or a territory or one or more specified sectors within that other country, or

(b) the international organization, ensures an adequate level of protection of personal data.

(2) The Data Commissioner may publish on its website a list of the countries, territories and specified sectors within that other country

and relevant international organisation for which the Data Commissioner has made a decision that an adequate level of protection is ensured.

Transfers on the basis of necessity.

45. (1) Personal data may be transferred to another country or territory on the basis of necessity is such a transfer is necessary for any of the purpose outlined under section 48 (c) of the Act.

(2) Prior to making a transfer under sub-regulation (1), a transferring entity shall ascertain that—

(a) that the transfer is strictly necessary in a specific case outlined under section 48(c) of the Act;

(b) there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.

(3) This section does not affect the operation of any international agreement in force between Kenya and other countries in the field of judicial co-operation in criminal matters and police co-operation.

Transfer on basis of consent.

46. (1) In accordance with section 25 (g) of the Act, in the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity, a transfer or a set of transfers of personal data to another country shall take place only on the condition that the data subject—

(a) has explicitly consented to the proposed transfer; and

(b) has been informed of the possible risks of such transfers.

(2) Without limiting the generality of sub-regulation (1), a data controller or processor must seek consent from a data subject for the transfer of sensitive personal data, in accordance with section 49 of the Act.

Subsequent transfers.

47. (1) Where personal data is transferred in accordance with this Part, the entity effecting the transfer shall make it a condition of the transfer, that the data is not to be further transferred to another country or territory without the authorisation of the transferring entity or another competent authority.

(2) A competent authority may give an authorisation under sub-regulation (1) only where the further transfer is necessary for a law enforcement purpose.

Provisions for the agreement to cross boarder transfer.

48. A transferring entity may enter into a written agreement with the recipient of personal data, which shall contain provisions relating to—

(a) unlimited access by the transferring entity to ascertain the existence of a robust information system of the recipient for storing the personal data; and

(b) the countries and territories to which the personal data may be transferred under the contract.

PART VIII—DATA PROTECTION IMPACT ASSESSMENT

Processing activities requiring data protection impact assessment.

49. (1) For the purpose of section 31 (1) of the Act, processing operations considered to result in high risks to the rights and freedoms of a data subject include —

(a) automated decision making with legal or similar significant effect that includes the use of profiling or algorithmic means or use of sensitive personal data as an element to determine access to services or that results in legal or similarly significant effects;

(b) use of personal data on a large-scale for a purpose other than that for which the data was initially collected;

(c) processing biometric or genetic data;

(d) where there is a change in any aspect of the processing that may result in higher risk to data subjects;

(e) processing sensitive personal data or data relating to children or vulnerable groups;

(f) combining, linking or cross-referencing separate datasets where the data sets are combined from different sources and where processing is carried out for different purposes;

(g) large scale processing of personal data;

(h) a systematic monitoring of a publicly accessible area on a large scale;

(i) innovative use or application of new technological or organizational solutions; or

(j) where the processing prevents a data subject from exercising a right.

(2) A data processor or data controller shall, prior to processing data under sub-regulation (1) conduct a data protection impact assessment.

Conduct of data protection impact assessment.

50. (1) Where a data protection impact assessment is required, a data controller or data processor may conduct the assessment through a template set out in the Third Schedule.

(2) Despite sub-regulation (1), a format of the data protection impact assessment may be varied by the Data Commissioner through guidance notes as may be issued from time to time.

Prior consultation.

51. (1) In accordance with section 31 (3) of the Act, where a data controller or a data processor is required to consult the Data Commissioner on the data protection impact assessment prior to processing, such consultations shall be done within sixty days from the date of the receipt of the impact statement report.

(2) In making a request under sub-regulation (1), the data controller or data processor shall provide—

(a) the data protection impact assessment prepared under section 31(1) of the Act; and

(b) where applicable, the respective responsibilities of the data controller or data processors involved in the processing.

(3) Where the Data Commissioner considers that the intended processing is likely to infringe on the Act or these Regulations, the Data Commissioner may issue such advice to the data controller or the data processor, in writing.

Consideration of the data protection impact assessment report.

52. (1) In conducting a data protection impact assessment, a data controller or a data processor may consult the Office for advice on whether risks identified and mitigation measures suggested are viable in the outlined circumstances.

(2) In reviewing the data protection impact assessment report, the Data Commissioner may make any recommendations to be incorporated prior to commencing the processing operations.

(3) Where a data controller or data processor, upon submitting the data protection impact assessment report to the Data Commissioner, does not receive any communication within sixty days of submission, may commence processing operations and the assessment report shall be taken to have been approved.

(4) A data controller or data processor may publish on its website the data protection impact assessment Report.

Audit of compliance with Assessment Report.

53. Pursuant to section 23 of the Act, the Data Commissioner may carry out periodic audits to monitor compliance with the Assessment Report and any recommendations that may have been provided by the Data Commissioner.

PART IX— PROVISIONS ON EXEMPTIONS UNDER THE ACT

Exemption for national security.

54. (1) For the purposes of section 51(2) (b) of the Act, the processing of personal data by a national security organ referred to in Article 239 (1) of the Constitution in furtherance of their mandate constitutes a processing for national security.

(2) Despite sub-regulation (1), a data controller or data processor who processes personal data for national security and wishes to be exempt on that ground shall apply to the Cabinet Secretary for an exemption.

(3) The Cabinet Secretary shall, upon being satisfied that the grounds supporting the application are sufficient, issue a certificate of exemption.

(4) The Cabinet Secretary may revoke a certificate of exemption issued, at any time, where the grounds on which the certificate was issued no longer apply.

Exemptions for public interest.

55. For the purposes of section 51(2) (b) of the Act, the processing of personal data is exempted from the Act on the grounds of public interest where such processing exists as a—

(a) permitted general situation; or

(b) permitted health situation.

Permitted general situation.

56. A permitted general situation referred to under regulation 55 (a)relates to the collection, use or disclosure by a data controller or data processor of personal data about data subject including for—

(a) lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health or safety;

(b) taking appropriate action in relation to suspected unlawful activity or serious misconduct;

(c) locating a person reported as missing;

(d) asserting a legal or equitable claim;

(e) conducting an alternative dispute resolution process; or

(f) performing diplomatic or consular duties.

Permitted health situation.

57. (1) A permitted health situation referred to under regulation 55 (b) relates to the collection, use or disclosure by a data controller or data processor of personal data about a data subject, including for—

(a) the collection of health information to provide a health service;

(b) the collection, use, or disclosure of health data is for health research and related purposes;

(c) the use or disclosure of genetic information where necessary and obtained in course of providing a health service;

(d) the disclosure of health information for a secondary purpose to a responsible person for a data subject.

(2) A permitted health situation under sub-regulation (1) applies where a data controller or data processor discloses health data about a data subject, and—

(a) they provide a health service to the data subject;

(b) the recipient of the personal data is a responsible person for the data subject;

(c) a data subject is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure;

(d) the disclosure is necessary to provide appropriate care or treatment of a data subject, or the disclosure is made for compassionate reasons;

(e) the disclosure is not contrary to any wish expressed by the data subject before the data subject became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware; and

(f) the disclosure is limited to the extent reasonable and necessary to provide appropriate care or treatment of the individual or to fulfil the purpose of making a disclosure for compassionate reasons.

PART X —GENERAL PROVISIONS

Complaints against data controller and data processor.

58. A person aggrieved by a decision of a data controller or a data processor under this Regulation or non-compliance with any provision may lodge a complaint with the Data Commissioner in accordance with the Act and regulations on complaints handling made thereunder.

FIRST SCHEDULE

FORM DPG 1 (r. 7 (2) & (r.8 (2))

REQUEST FOR RESTRICTION OR OBJECTION
TO THE PROCESSING OF PERSONAL DATA

Note

(i) A documentary evidence in support of the objection may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure

A. NATURE OF REQUEST

Mark the appropriate box with an "x". Request for:

RESTRICTION ☐ OBJECTION ☐

B. DETAILS OF THE DATA SUBJECT

Name: .....

Identity Number: .....

Phone number:.....

E-mail address: .....

(Your details below where initiating the request for a minor or a person who has no capacity)

Name .....

Relationship with the Data Subject

Contact Information:

C. REASONS FOR THE REQUEST

(*Please provide detailed reasons for the restriction or objection)*

D. DECLARATION

I certify that the information given in this application is true

Signature ☐ Date ☐

DPG 2 (r. 9(2))

REQUEST FOR ACCESS TO PERSONAL DATA

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

*(iii) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*: ☐

Identity Number*: [ ]

Phone number*: [ ]

e-mail address: [ ]

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name*

Relationship with the Data Subject* [ ]

Contact Information* [ ]

B. DETAILS OF THE PERSONAL DATA REQUESTED

(Describe the personal data requested)

[ ]

MODE OF ACCESS

I would like to: *(check all that apply)*

[ ] Inspect the record

[ ] Listen to the record

[ ] Have a copy of the record made available to me in the following format:

[ ] photocopy *(Please note that copying costs will apply)*

number of copies required: .....

[ ] electronic

[ ] transcript *(Please note that transcription charges may apply)*

[ ] Other *(specify)* .....

C. Delivery Method

[ ] collection in person

[ ] by mail (provide address where different / in addition to details provided above)

Town/City: .....

[ ] by e-mail (provide email address where different / in addition to details provided above): .....

DECLARATION

Note any attempt to access personal data through misrepresentation may result in prosecution.

☐ I certify that the information given in this application is true.

Signature

Da

FORM DPG 3 (r.10 (2))

REQUEST FOR RECTIFICATION

Fill as appropriate

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

*(iii) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*:

Identity Number*:

Phone number*:

e-mail address:

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name*

Relationship with the Data Subject*

Contact Information*

Signature Date

PROPOSED CHANGE (S)

	Personal data to be corrected e.g. name, residential status, and mobile number, email address.	*Proposed change*	*Reason for the proposed change*
1.			
2.			
3.			
4.			
5.			

B. DECLARATION

Note any attempt to rectify personal data through misrepresentation may result in prosecution.

☐ I confirm that I have read and understood the terms of this request form and certify that the information given in this application is true.

Signature _____ Date _____

FORM DPG 4 (r. 11 (2))

REQUEST FOR DATA PORTABILITY

Note:

(iv) Documentary evidence in support of this request may be required.

(v) Where the space provided for in this Form is inadequate, submit information as an annexure

*(vi) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*:

Identity Number*:

Phone number*:

e-mail address:

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name*

Relationship with the Data Subject*

Contact Information*

B. DETAILS OF THE REQUEST

Please transfer a copy of my personal data to *

By either:

- Emailing a copy to them at
- Mailing to:
- Others (*Please specify)*

DECLARATION

Note, any attempt to port personal data through misrepresentation may result in prosecution.

☐ I certify that the information given in this application is accurate to the best of my knowledge

Signature _____ Date _____

FORM DPG 5 (r.12(2))

REQUEST FOR ERASURE OF PERSONAL DATA

Fill as appropriate

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

*(iii) All fields marked as * are mandatory*

i. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*: .....

Identity Number*: .....

Phone number*: .....

e-mail address: .....

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name* .....

Relationship with the Data Subject* .....

Contact Information* .....

ii. REASON FOR ERASURE REQUEST

(Tick the appropriate box)

(a) Your personal data is no longer necessary for the purpose for which it was originally collected;	☐
(b) You have withdrawn consent that was the lawful basis for retaining the personal data;	☐
(c) You object to the processing of your personal data and there is no overriding legitimate interest to continue the processing;	☐
(d) the processing of your personal data has been unlawful	☐
(e) Required to comply with a legal obligation.	☐

PERSONAL DATA TO BE ERASED

Describe the personal data you wish to have erased.

iii. *Declaration*

Note any attempt to erase personal data through misrepresentation may result in prosecution.

☐ I confirm that I have read and understood the terms of this request form and certify that the information given in this application is true.

Signature Date

SECOND SCHEDULE (r.37 (1)& (3))

The following personal data or circumstances amount to a notifiable data breach—

1. The amount of any wages, salary, fee, commission, bonus, gratuity, allowance or other remuneration paid or payable to the data subject by any person, whether under a contract of service or a contract for services.

2. The income of the data subject from the sale of any goods or property.

3. The number of any credit card, charge card or debit card issued to or in the name of the data subject.

4. The number assigned to any account the data subject has with any entity that is a bank or finance company.

5. Any information that identifies, or is likely to lead to the identification of, the data subject who is a child in conflict with the law or in need of care and protection.

6. Any private key of or relating to a data subject that is used or may be used —

(a) to create a secure electronic record or secure electronic signature;

(b) to verify the integrity of a secure electronic record; or

(c) to verify the authenticity or integrity of a secure electronic signature as provided under the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010 or any other related law.

7. The net worth or creditworthiness of a data subject.

8. The deposit or withdraw of monies by a data subject with any entity.

9. The withdrawal by the individual of moneys deposited with any entity or a payment system.

10. The granting by a person of advances, loans and other facilities by which the data subject, being a customer of the entity, has access to funds or financial guarantees.

11. The existence, and amount due or outstanding, of any debt —

(a) owed by the data subject to an entity; or

(b) owed by an entity to the data subject.

12. The incurring by the entity of any liabilities on behalf of the data subject.

13. The payment of any moneys, or transfer of any property, by any person to the individual, including the amount of the moneys paid or the value of the property transferred, as the case may be.

14. The data subject's investment in any capital markets products.

15. Any term and condition, premium or benefits payable, or any detail relating to the condition of health, from an accident, health, or life policy of which the data subject is the policy owner or a beneficiary.

16. The assessment, diagnosis, treatment, prevention or alleviation by a health professional of any of the following affecting the data subject—

(a) any sexually-transmitted diseases;

(b) Human Immunodeficiency Virus Infection;

(c) mental disorder;

(d) substance abuse and addiction.

17. The provision of treatment to the individual for or in respect of —

(a) the donation or receipt of a human egg or human sperm; or

(b) any contraceptive operation or procedure or abortion;

18. Any of the following—

(a) the donation and removal of any organ from the body of the deceased individual for the purpose of its transplantation into the body of another individual;

(b) the donation and removal of any specified organ from the individual, being a living organ donor, for the purpose of its transplantation into the body of another individual;

(c) the transplantation of any organ mentioned in paragraph (a) or (b) into the body of the individual.

19. The suicide or attempted suicide of the individual.

20. Domestic abuse, child abuse or sexual abuse involving or alleged to involve the data subject.

21. Any of the following—

(a) information that the individual is or had been adopted pursuant to an adoption order made under the Children Act No 8 of 2001, or is or had been the subject of an application for an adoption order;

(b) the identity of the natural father or mother of the data subject;

(c) the identity of the adoptive father or mother of the subject;

(d) the identity of any applicant for an adoption order;

(e) the identity of any person whose consent is necessary under that Act for an adoption order to be made, whether or not the court has dispensed with the consent of that person in accordance with that Act.

THIRD SCHEDULE (r.50 (1))

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

Part 1: Description of the processing operations

Name of Data Controller/ Data Processors: .....
Postal Address: .....
Email Address: .....
Telephone Number: .....
1. Project Name
2. Assess the need for Data Impact Assessment
(Assess whether there is need for DPIA by determining if project involves personal data that is likely to result in high risk, specify risk where appropriate)
3. Project Outline:
(Explain broadly what the project aims to achieve and what type of processing it involves)
4. Personal data
(e.g type of personal data data being processed.)
5. Describe the Information Flow.
Describe the collection, use and deletion of personal data here, including; where you are getting the data from; how is the data being collected; where the data will be stored; how long will the data be stored; where data could be transferred to; and, how many individuals are likely to be affected by the project.
6. Describe how the data processing flow complies with the data protection principles-

Part 2: An assessment of the necessity and proportionality of the processing operations in relation to the purpose.

Require the assessment and provide the parameters of the assessment.

Describe compliance and proportionality, measures, in particular:	
The lawful basis for processing	
Methods of obtaining of consent.	
Whether processing personal data is key to achieving your purpose?	
Is there another way to achieve the same outcome without processing personal data?	
Data quality and data minimization	
Notification of the data subjects on the processing activity	
Exercising of the rights of the data subjects	
The parties are involved in the processing and their specific roles	
Measures to ensure compliance by the parties involved, if any	
Processing safeguard of the personal data	
Safeguard prior to and Cross border transfers, if any	

Part 3: The measures envisaged for addressing the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act

Risk Assessment - Identifying Privacy Risks and Evaluating Privacy Solutions							
Risk Identity and Description	*Consequence*	*Risk Owner*	*Current internal CONTROLS (provide details of how you will manage the risk)*	*Assessment of Risk*			*Describe what further ACTIONS you will take to reduce the Impact/Likelihood and mitigate the risk. State who is the risk owner for each action*
				Impact (1,2,3,4,5)	Likelihood (1,2,3,4,5)	=Score(impact + likelihood)	

Part 5: Sign Off and Record Outcomes

ITEM DESCRIPTION	NOTES/INSTRUCTIONS
Consultation with Office of the Data Protection Commissioner (where applicable)	
This DPIA will be kept under review by:	

Made on the 7th December, 2021.

JOE MUCHERU,
Cabinet Secretary, Ministry of Information, Communication, Technology, Innovation and Youth Affairs.

LEGAL NOTICE NO. 264

THE DATA PROTECTION ACT

(No. 24 *of* 2019*)*

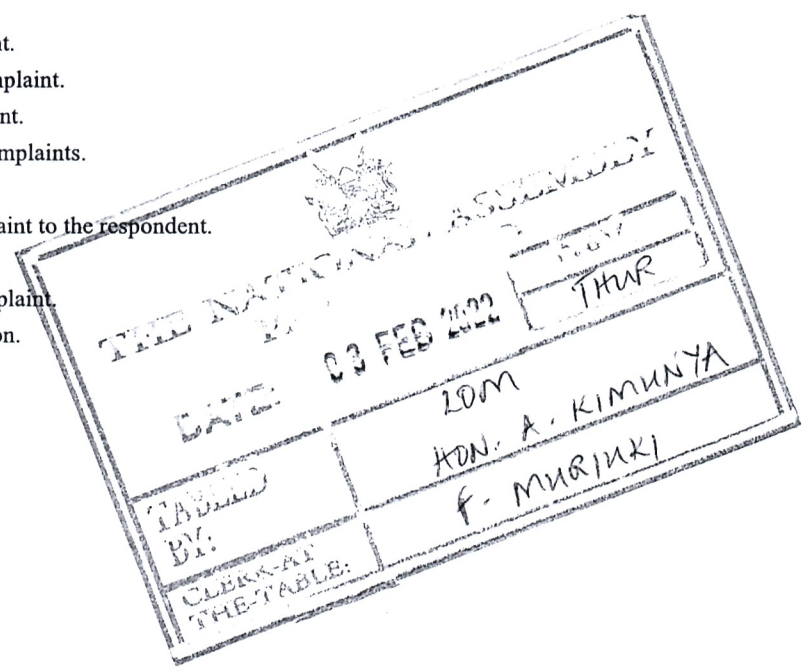
THE DATA PROTECTION (COMPLAINTS HANDLING AND ENFORCEMENT PROCEDURES) REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation

PART I–PRELIMINARY

PART II— PROCEDURE FOR LODGING, ADMISSION AND RESPONSE TO COMPLAINTS



THE DATA PROTECTION ACT, 2019

(No. 24 of 2019)

IN EXERCISE of the powers conferred by section 71 of Data Protection Act, 2019, the Cabinet Secretary for Information, Communications, Technology, Innovation and Youth Affairs makes the following Regulations—

THE DATA PROTECTION (COMPLAINTS HANDLING PROCEDURE AND ENFORCEMENT) REGULATIONS, 2021

PART I—PRELIMINARY

Citation.

1. These Regulations may be cited as the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.

Interpretation.

2. In these Regulations, unless the context otherwise requires —

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

"complainant" means a data subject or a person who has lodged a complaint pursuant to regulation 4;

"Data Commissioner" means the person appointed under section 6 of the Act;

"Office" means the office of the Data Protection Commissioner;

"enforcement notice" means a notice issued by the Data Commissioner under regulation 16;

"penalty" means a penalty imposed by a penalty notice;

"penalty notice" means a notice issued by the Data Commissioner under regulation 20;

"respondent" means a person against whom a complaint is lodged; and

"summons" means an order of the Data Commissioner, in writing, directing a person to appear before the Office.

Object and purpose of the Regulations.

3. The object and purpose of these Regulations is to—

(a) facilitate a fair, impartial, just, expeditious, proportionate and affordable determination of complaints lodged with the Data Commissioner in accordance with the Act and these Regulations, without undue regard to technicalities of procedure;

(b) provide for issuance of enforcement notices as contemplated under section 58 of the Act;

(c) provide for issuance of issuance of penalty notices as contemplated under section 62 of the Act;

(d) provide for the procedure for hearing and determining of complaints; and

(e) provide for the resolution of complaints lodged with the Data Commissioner by means of alternative dispute resolution mechanisms as specified under section 9(1) (c) of the Act.

PART II—PROCEDURE FOR LODGING, ADMISSION AND RESPONSE TO COMPLAINTS

Lodging of a complaint.

4. (1) Pursuant to section 56 of the Act, a data subject or any person aggrieved on any matter under the Act may lodge a complaint with the Data Commissioner.

(2) A complaint lodged under sub-regulation (1) may be lodged in Form DPC 1 set out in the Schedule—

(a) orally, subject to section 56(3) of the Act;

(b) through electronic means, including email, web posting, complaint management information system; or

(c) by any other appropriate means.

(3) A complaint under sub-regulation (1) may be lodged—

(a) by the complainant in person;

(b) by a person acting on behalf of the complainant;

(c) by any other person authorized by law to act on behalf of a data subject; or

(d) anonymously.

(4) The Data Commissioner shall acknowledge receipt of the complaint within seven days of receipt of the complaint under sub-regulation (1).

(5) The complaint under sub-regulation (1) shall be lodged free of charge.

Register of complaints.

5. (1) The Data Commissioner shall keep and maintain an up to date Register of Complaints.

(2) An entry into the register of complaints shall state the particulars of the complainant and the complaint filed with the Data Commissioner.

(3) The Data Commissioner shall protect the identity of the complainant where the request to protect the identity is sought by the complainant.

Admission of complaint.

6. (1) The Data Commissioner shall undertake a preliminary review of a complaint, upon receipt of the complaint by the Office.

(2) The Data Commissioner may, upon undertaking a preliminary review of the complaint—

(a) admit the complaint;

(b) where applicable, advise the complainant in writing that the matter is not within the mandate of the Data Commissioner; or

(c) advise the complainant that the matter lies for determination by another body or institution and refer the complainant to that body or institution.

(3) Despite sub-regulation (2), the Data Commissioner may

decline to admit a complaint where the complaint does not raise any issue under the Act.

(4) Upon admission of a complaint, the Data Commissioner may—

(a) conduct an inquiry into the complaint;

(b) conduct investigations;

(c) facilitate mediation, conciliation or negotiation in accordance with the Act and these Regulations; or

(d) use any other mechanisms to resolve the complaint.

(5) Where a complaint is declined for admission under sub-regulation (3), the complaint may be re-admitted within six months from the date of decline, where the complaint raises new issues for determination under the Act.

(6) A complaint under sub-regulation (5) shall be lodged in accordance with regulation 4.

Discontinuation of a complaint.

7. (1) The Data Commissioner may discontinue an existing complaint in Form DPC 2 set out in the Schedule, where—

(a) a complaint does not merit further consideration; or

(b) a complainant refuses, fails or neglects to communicate without justifiable cause.

(2) The Data Commissioner shall provide the reasons for discontinuation on any of the grounds specified under sub-regulation (1) (a) or (b) and shall, in writing, notify the complainant and respondent within fourteen days from the date the decision to discontinue a complaint is made.

(3) A complainant may, where a complaint has been discontinued pursuant to these Regulations, re-institute a complaint upon providing grounds for the restitution to the Data Commissioner.

Withdrawal of a complaint.

8. (1) A complaint may be withdrawn at any stage during its consideration but before a determination is made.

(2) A complainant may, at any time during the consideration of a complaint lodged pursuant to regulation 4 and before its determination, withdraw the complaint.

(3) An application for a withdrawal under sub-regulation (1) shall be in Form DPC 2 set out in the Schedule.

(4) A withdrawn complaint under sub-regulation (1) may be re-lodged, within six months from the date of withdrawal of such complaint.

(5) A complaint re-lodged under this regulation shall be processed in accordance with the provisions of this Part.

Joint consideration of complaints.

9. (1) Where two or more complaints are lodged in which similar issues are raised against a respondent, the Data Commissioner may with the consent of the complainants—

(a) consolidate the complaints and make a determination; or

(b) treat one complaint as a test complaint and stay further action on the other complaints pending resolution of the test complaint.

(2)The Data Commissioner shall, with necessary modifications, apply the decision of a test complaint to all the complaints stayed under sub-regulation (1)(b).

(3) The Data Commissioner shall, in writing, communicate to the complainants and all the parties the decision made under this regulation.

(4) Where complaints are consolidated in accordance with this regulation, the complaint shall be treated as a single complaint and shall be determined in accordance with the provisions of these Regulations.

Language.

10. (1) Proceedings before the Office shall be conducted in Kiswahili, English or Kenyan Sign Language.

(2) The Office may ensure that a party who cannot speak, hear or understand the language of proceedings receives the services of an interpreter provided for by the Office.

Notification of a complaint to the respondent.

11. (1) Upon admission of a complaint, the Data Commissioner shall notify the respondent of the complaint lodged against him, in Form DPC 3 set out in the Schedule and shall require the respondent to within twenty-one days —

(a) make representations and provide any relevant material or evidence in support of its representations;

(b) review the complaint with a view of summarily resolving the complaint to the satisfaction of the complainant; or

(c) provide a response with the required information.

(2) Where a respondent does not take any action as contemplated under sub-regulation (1), the Data Commissioner shall proceed to determine the complaint in accordance with the Act and these Regulations.

(3) The notice referred to under sub-regulation (1) shall specify options available to resolve a complaint including determining the complaint through alternative dispute resolution mechanisms specified in the Act and these Regulations.

Joinder of parties.

12. (1) Where it appears to the Data Commissioner, or by an application by either the complainant or the respondent, that it is necessary that a person becomes a party to a complaint, the Data Commissioner may order that person to be enjoined as a party.

(2) A person who has sufficient interest in the outcome of a complaint may apply to the Office for leave to be enjoined in the proceedings prior to the hearing of the complaint.

(3) An application under sub-regulation (1) shall include —

(a) the names of the parties to which that application relates;

(b) the name and address for service of the person wishing to be enjoined;

(c) the grounds the applicant relies on to be enjoined;

(d) a copy of any relevant document in support of the application; and

(e) the relief sought.

Investigations of a complaint.

13. (1) In investigating a complaint, the Data Commissioner may, subject to section 57 of the Act—

(a) issue summons in Form DPC 4 set out in the Schedule requiring the attendance of any person at a specified date, time and place for examination;

(b) examine any person in relation to a complaint;

(c) administer an oath or affirmation on any person during the proceedings;

(d) require any person to produce any document or information from a person or institution; and

(e) on obtaining warrants from the court, enter into any establishment or premises and conduct a search and may seize any material relevant to the investigation.

(2) Upon completion of the investigation, the Data Commissioner shall prepare an investigation report.

(3) In conducting investigations under this regulation, the Data Commissioner shall be guided by the provisions of the Fair Administrative Action Act, 2015.

No. 4 of 2015.

Outcome of investigation.

14. (1) The Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations.

(2) A determination under sub-regulation (1) shall be in writing and shall state—

(a) the nature of the complaint;

(b) a summary of the relevant facts and evidence adduced;

(c) the decision and the reasons for the decision;

(d) the remedy to which the complainant is entitled; and

(e) any other relevant matter.

(3) The remedies contemplated under sub-regulation (2) (d) may include—

(a) issuance of an enforcement notice to the respondent in accordance with the Act and these Regulations;

(b) issuance of a penalty notice imposing an administrative fine

where a respondent fails to comply with the enforcement notice;

(c) dismissal of the complaint where it lacks merit;

(d) recommendation for prosecution; or

(e) an order for compensation to the data subject by the respondent.

(4) The Data Commissioner shall within seven days from the date of such determination, communicate the decision under sub-regulation (3) to the parties, in writing.

(5) The decision of the Data Commissioner made under these Regulations shall be—

(a) binding on the parties; and

(b) shall be enforced as an order of the Court.

Negotiation, mediation or conciliation.

15. (1) Where the complaint is to be determined through negotiations, mediation or conciliation, the provisions of these Regulations shall apply.

(2)Where parties to a complaint agree to negotiation, mediation or conciliation, the Data Commissioner may in consultation with the parties facilitate the process.

(3) During the negotiations, mediation or conciliation, the Data Commissioner may apply such procedures as may, in the interest of the parties, deem appropriate in the circumstances.

(4) At the conclusion of the negotiations, mediation or conciliation process, the parties shall sign a negotiation, mediation or conciliation agreement in the manner specified in Form DPC 5 set out in the Schedule.

(5) A negotiation, mediation or conciliation agreement entered into under this regulation shall be deemed to be a determination of the Data Commissioner, and shall be enforceable as such.

(6) Despite this regulation, a party to dispute who is subject to a negotiation, mediation or conciliation may withdraw from the proceedings at any stage and shall notify the Data Commissioner and other parties of such withdrawal within seven days from the date of making such a decision.

(7) Parties to a dispute shall take all reasonable measures to amicably determine a dispute and act in good faith.

(8) Where the complaint is not determined through negotiation, mediation or conciliation, the Data Commissioner shall proceed to determine the complaint as provided for in the Act and these Regulations.

PART III—ENFORCEMENT PROVISIONS

Issuance of enforcement notice.

16. (1) The Data Commissioner may pursuant these Regulations or section 58 of the Act issue an enforcement notice.

(2) An enforcement notice shall specify the consequences of failure to comply with the notice including issuance of a penalty notice as provided under section 62 (1) of the Act.

Service of an enforcement notice.

17. (1) An enforcement notice shall be deemed to have been duly served on the concerned person where—

(a) an electronic copy of enforcement notice is sent to the concerned person's last used email address; or

(b) the enforcement notice is posted or physically delivered to the registered offices of the concerned person, in the absence of an electronic address.

(2) The enforcement notice shall take effect from the date of service specified under sub-regulation (1).

Review of enforcement notice.

18. (1) A person to whom an enforcement notice is given may apply in Form DPC 6 set out in the Schedule to the Data Commissioner for a review of the enforcement notice.

(2) An application under sub-regulation (1) may be made —

(a) before the end of the period specified in the enforcement notice; and

(b) on the ground that—

(i) a change of circumstances or new facts have arisen; or

(ii) one or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.

Appeals against enforcement notice.

19. Subject to sections 58 (2) (d) and 64 of the Act, a person may before the lapse of thirty days from the date of service of the enforcement notice, appeal to the High Court against a decision arising out of the enforcement of the notice.

Issuance of penalty notice.

20. (1) The Data Commissioner shall, where any of the circumstances specified under section 62 of the Act and these Regulations arises, issue a penalty notice for each breach identified in the enforcement notice.

(2) A penalty notice shall contain—

(a) the name and address of the concerned person, to whom it is addressed;

(b) the reasons why the Data Commissioner proposes to impose the penalty and the amount thereof;

(c) an administrative fine imposed as contemplated under section 63 of the Act;

(d) details of how the penalty is to be paid; and

(e) details of the rights of appeal under section 64 of the Act.

(3) The administrative fine levied under sub-regulation (2)(c) shall consider each individual case and have due regard to factors or reasons outlined under section 62 (2) of the Act.

(4) A penalty notice may impose a daily fine of not more than ten thousand shillings for each breach identified until the breach is rectified.

(5) The daily fine imposed under sub regulation (4) shall be managed in accordance with section 67 of the Act and the Public Finance Management Act, 2012.

Enforcement of penalty notice.

21. The Data Commissioner shall enforce or take action to recover a penalty—

(a) upon the lapse of the period specified in the penalty notice for payment of the penalty;

(b) on the final determination of any appeal against the penalty notice; or

(c) on the lapse of the period given to appeal against the penalty.

SCHEDULE

FORM DPC 1 (r. 4 (2)(a))

COMPLAINT SUBMISSION FORM

A. PARTICULARS OF THE COMPLAINANT/ REPRESENTATIVE	
Full Names	
National Identification Card Number/ Passport Number	
Contact information (Phone number/ email address)	
B. PARTICULARS OF THE COMPLAINT	
Describe your complaint;	
Indicate to whom the complaint is against;	
When did you become aware of the alleged breach	
C. REMEDY SOUGHT	
Explain the remedy you are seeking for the alleged breach;	
D. Which other steps have you already taken in relation to the Complaint, if any	
State any other institution contacted over the complaint, if any.	

Signature	Date

Note

** If the space provided for in this Form is inadequate, submit information as an annex.*

** If you have supporting documents to substantiate your claim, please annex copies to this Form.*

** The information submitted will be treated with the upmost confidentiality.*

FORM DPC 2 (r. 7(1) & r.8(3))

REQUEST TO DISCONTINUE OR WITHDRAW A COMPLIANT

A. NATURE OF REQUEST	
Mark the appropriate the box with an "x". Request for: DISCONTINUATION ☐ WITHDRAWAL ☐	
B. PARTICULARS OF THE COMPLAINANT/ REPRESENTATIVE	
Full names	
National Identification Card Number/ Passport Number	
Contact Information (Phone Number/ Email Address)	
C. NATURE OF THE COMPLAINT	
Complaint Number/Reference Number	
D. STATE REASON FOR WITHDRAWAL/DISCONTINUATION OF COMPLAINT	

Signature Date

Note:

**If the space provided for in this Form is inadequate, submit information as an Annexure to this form*

**If you have supporting documents to substantiate your claim, please annex copies to this Form.*

**The information submitted will be treated with the upmost confidentiality.*

FORM DPC (r.11 (1))

Notification of a complaint to the Respondent

Details of the Respondent	
Full names	
Complaints Register entry number	
Email address	
Details of the Complainant	
Full Names	
National Identification Card Number/ Passport Number	
Contact information	
Particulars of the Complaint	
Representations to be made to the Data Commissioner by:	

Signature Date

FORM DPC 4 (r.13 (1) (a))

Summons to Enter Appearance

OFFICE OF THE DATA PROTECTION COMMISSIONER

COMPLAINT NO..... OF .....

_____ } Complainant

AGAINST

_____ } Respondent

TO: _____

_____ *Person required to attend*

_____

WHEREAS the above-named Complainant has instituted a Complaint against you, the Respondent particulars of which are set out in the copy of Complaint annexed herewith.

YOU ARE HEREBY REQUIRED to attend to the Office of the Data Commissioner on _____(Date), _____
_____(*Venue)* At _____
_____(*Time)* (am/pm)

Should you fail to attend to the above mentioned summons, you may be liable to an offence under section 57 of the Data Protection Act, 2019.

Dated..... day of ..... 20.....

.....

Data Commissioner

Form DPC 5 (r. 15 (4))

ALTERNATIVE DISPUTE RESOLUTION SETTLEMENT AGREEMENT

The undersigned parties, on this _____ day of _____,_ , have agreed to the following settlement of their dispute concerning _____ _____ _____,and hereby memorialize such agreement according to the following terms:

_____ _____ _____,_____

The Settlement Agreement is binding on the parties and is admissible in court for enforcement purposes.

In order to facilitate the above-specified terms of settlement, the parties further agree that on or before the _____day of _____, 20_, they will Complainant:_____ _____ _____ _____ _____

Respondent:

_____ _____

Complainant:

Signature Date

_____ _____

Respondent:

Signature Date

_____ _____

Form DPC 6 (r. 18 (1))

REVIEW OF ENFORCEMENT NOTICE

A. PARTICULARS OF THE PERSON ISSUED WITH THE ENFORCEMENT NOTICE	
Full Names	
Registration Number/ Identification Number	
Contact information (Phone number/ email address)	
B. REFERENCE NUMBER OF THE ENFORCEMENT NOTICE	
C. GROUNDS FOR REVIEW OF THE ENFORCEMENT NOTICE *(tick as appropriate)*	
(i) Change of circumstances or new facts have arisen; or	
(ii) One or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.	

Note:

**If the space provided for in this Form is inadequate, submit information as an Annex to this Form*

**If you have supporting documents to substantiate your claim, please annex copies to this Form.*

**The information submitted will be treated with the upmost confidentiality.*

Made on the 7th December, 2021.

JOE MUCHERU,
Cabinet Secretary, Ministry of Information, Communications, Technology, Innovation and Youth Affairs.

LEGAL NOTICE NO. 265

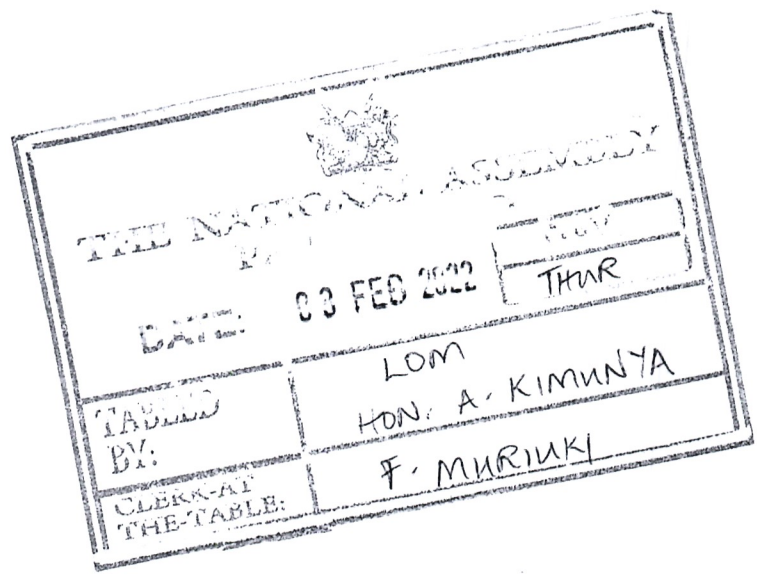
THE DATA PROTECTION ACT

(*No.* 24 *of* 2019)

THE DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation



THE DATA PROTECTION ACT

(No. 24 of 2019)

IN EXERCISE of the powers conferred by section 71 of the Data Protection Act, 2019, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs, makes the following Regulations—

THE DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATIONS, 2021

Citation and commencement.

1. (1) These Regulations may be cited as the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

(2) The provisions of these Regulations shall come into effect six months from the date of publication.

Interpretation No. 24 of 2019.

2. In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection Act, 2019;

"Data Commissioner" means the person appointed under section 6 of the Act;

"data controller" has the meaning assigned to it under the Act;

"data processor" has the meaning assigned to it under the Act;

"register" has the meaning assigned to it under the Act;

"Office" has the meaning assigned to it under the Act;

"establishment documents" include—

(a) a Statute, Charter or statutory instrument in which a body is established;

(b) registration certificate;

(c) trust deeds in which a trust has been established; and

(d) other instruments by which a body is established including its governing and administrative structure.

Scope of Regulations.

3. (1) These Regulations provide for the procedure for registration of data controllers and data processors as provided under section 18 of the Act.

(2) These Regulations shall not apply to civil registration entities specified under the Data Protection (Civil Registration) Regulations, 2020.

L.N. No. 100 of 2020.

Requirements for registration.

4. (1) Subject to regulation 13 (1), every data controller and data processor shall be required to register in accordance with the provisions of the Act and these Regulations.

(2) For purposes of registration, a person shall register as a—

(a) data controller, where the person determines the purpose and means for processing personal data; or

(b) data processor, where the person processes personal data on behalf of the data controller but excludes employees of the data controller and has—

(i) a contractual relationship with the data controller; and

(ii) no decision making power on the purpose and means of processing personal data.

(3) Despite sub-regulation (2) (a), a data controller may apply for registration as both a data controller and a data processor with regards to any processing operations and shall be required to pay the requisite fees applicable for both a data controller and a data processor thereto.

(4) Despite sub-regulation (2) (b), where a data processor processes personal data other than as instructed by the data controller, thedata processor shall be considered to be a data controller in respect of that processing activity, for purposes of assessing liability.

Application for registration.

5. (1) An application for registration of a data controller or data processor shall—

(a) be in Form DPR1 set out in the First Schedule; and

(b) be accompanied by the registration fees specified in the Second Schedule.

(2) An application for registration under sub-regulation (1) shall be accompanied by—

(a) a copy of the establishment documents;

(b) particulars of the data controllers or data processors including name and contact details;

(c) a description of the purpose for which personal data is processed; and

(d) a description of categories of personal data being processed.

Payment of registration fees by specified public bodies.

6. (1) A state department or county department shall register and pay the fees on behalf of their respective entities.

(2) The entities referred to under sub-regulation (1) shall be the public entities at national or county government which—

(a) operates within a state department or county department;

(b) is wholly funded from the Consolidated Fund; and

(c) provides a public service.

(3) The fees paid by the state department or county department under sub-regulation (1) shall cater for the specified entities registered under the concerned state department or county department.

(4) Despite this regulation, a State Corporation or a County Corporation shall be required to register as a data controller or a data processor in respect of their processing activity, in the manner specified under these Regulations.

Processing ofan application for registration.

7. The Data Commissioner shall undertake a verification process of the details provided in the application for registration.

Approval and issuance of certificate of registration.

8. Where the Data Commissioner is satisfied that the applicant fulfills the requirements for registration under these Regulations, the Data Commissioner shall, within fourteen days—

(a) issue the applicant with a certificate of registration for the duration specified under regulation 9; and

(b) enter the particulars of the successful applicant in the register.

Duration of certificate of registration.

9. A certificate of registration issued under regulation 8 (a) shall be valid for a period of twenty-four months from the date of issuance.

Refusal of registration.

10. (1) Where the Data Commissioner declines to approve an application for registration, the Data Commissioner shall within twenty-one days from the date of such decision—

(a) notify, in writing, the applicant of the refusal; and

(b) provide reasons for such refusal.

(2) The Data Commissioner may decline to grant an application for registration, where the—

(a) particulars provided for inclusion in an entry in the register are insufficient;

(b) appropriate safeguards for the protection of the privacy of the data subject have not been provided by the data controller or a data processor; or

(c) the data controller or data processor is in violation of any provisions of the Act and these Regulations.

(3) A data controller or data processor whose application for registration has been declined under these Regulations may make a fresh application upon complying with the requirements specified in the refusal notice.

(4) An application under sub-regulation (3) shall be processed as any other application and in the manner specified under these Regulations.

Renewal of registration.

11. (1) Pursuant to section 20 of the Act, a registered data controller or data processor shall apply for a renewal of registration as a data controller or data processor, after the expiry of the certificate of registration.

(2) An application for renewal of a certificate of registration shall be—

(a) made in Form PR 2 set out in the First Schedule; and

(b) accompanied by the appropriate renewal fee specified in the Second Schedule.

(3) The Data Commissioner shall, upon receipt of the application,

and where satisfied that the applicant complies with the requirements for registration, renew the certificate of registration.

(4) Despite sub-regulation (2), where renewal is for a distinct purpose or categories of data other than that for which the data controller or data processor had been registered for, the Data Commissioner shall undertake a verification process in the manner provided under regulation 7.

Refusal of renewal.

12. (1) Where the Data Commissioner declines to renew an application for registration, the Data Commissioner shall within twenty-one days from the date of such decision—

(a) notify, in writing, the applicant of the refusal; and

(b) provide reasons for such refusal.

(2) The provisions of regulation 10 shall, with necessary modifications, apply where refusal to renew notice is to be or has been issued.

Exemption from mandatory registration.

13. (1) For purposes of this regulation—

"revenue" means the total income of profit-making data controllers or data processors for the year immediately preceding the year of registration;

"turnover" means the utilized annual budget of non-profit making data controllers or data processors for the year immediately preceding the year of registration;

"non-profit making data controller or data processors" means an entity whose core mandate excludes the generation of profit and includes non-governmental organizations, charitable and religious institutions, multi-lateral agencies or civil society organizations.

(2) A data controller or data processor is exempt from mandatory registration under these Regulations where the data controller or data processor—

(a) has an annual turnover of below five million shillings or annual revenue of below five million shillings; and

(b) has less than ten employees.

(3) Despite the provisions of sub-regulation (2), the data controller and data processor exempt under sub-regulation (2) shall be required to comply with the provisions of the Part IV and Part VI of the Act.

(4) The exemption provided under sub-regulation (1) shall not apply to a data controller or data processor whose annual turnover is below five million shillings and processes personal data for the purposes specified under the Third Schedule.

(5) The data controllers and data processors contemplated under sub-regulation (2), shall be required to undertake mandatory registration in accordance with Part III of the Act and these Regulations.

Register.

14. (1) Subject to section 21 of the Act, the Data Commissioner shall keep and maintain an up to date register which shall contain—

(a) the names and particulars of registered data controllers and data processors;

(b) categories of personal data being processed by the data controllers and data processors;

(c) the address of the principal places of business of the data controllers and data processors;

(d) where applicable, details of data protection officers; and

(e) any other relevant particular.

(2) The Office shall, once every thirty days, publish on the official website a list of registered data controllers or data processors.

Change of particulars.

15. (1) Subject to section 19(2) of the Act, a data controller or data processor shall, within fourteen days of the occurrence of any changes in the particulars of a data controller or a data processor, notify the Data Commissioner in writing.

(2) The Data Commissioner shall, on receiving the notification make the necessary changes on the register, where necessary.

(3) The Data Commissioner may prior to making any change on the register, request for any necessary documents or proof thereof.

(4) A data controller or data processor who contravenes this regulation commits an offence and shall, on conviction, be liable to the penalty specified under section 73 of the Act.

Cancellation or variation of registration.

16. (1) Subject to section 22 of the Act, the Data Commissioner may cancel a certificate of registration or vary the conditions for registration, where –

(a) the data controller or data processor applies for cancellation or variation;

(b) the Data Commissioner establishes that the data controller or data processor provided false or misleading information in relation to any registration particulars; or

(c) the data controller or data processor willfully or negligently, fails to comply with provisions of the Act and any Regulations made thereunder.

(2) The Data Commissioner shall, before cancelling or varying the conditions of registration, be guided by the provisions of the Fair Administrative Actions Act, 2015. No. 4 of 2015.

Electronic registration.

17. An application made under these Regulations shall be submitted through electronic means provided for on the Office website.

Offences.

18. A data controller or a data processor who—

(a) processes personal data without registering in accordance with these Regulations;

(b) provides false or misleading information for the purpose of registration; or

(c) fails to renew a certificate of registration and continues to process personal data after the expiry of the certificate,

commits an offence and shall, upon conviction, be liable to penalty specified under section 73 of the Act.

FIRST SCHEDULE

FORM DPR 1 (r. 5(1(a))

REGISTRATION FORM FOR DATA CONTROLLERS AND DATA PROCESSORS

SECTION 1 – BASIC DETAILS	
Indicate if you are registering as a Data Controller ☐ Data Processor ☐	
Name:	
Postal Address:	
Telephone Number:	
Email Address:	
County:	
Countr:	
Sector:	
Legal establishment:	
For public body: (Specify the state department or county department)	

SECTION 2 – PERSONAL DATA		
Provided the details of the various subsets of personal data being processed and the purpose of processing.		
CATEGORY OF DATA SUBJECTS (E.g. employee, client, students, supplier, shareholder, etc.)	DESCRIPTION OF PERSONAL DATA TO BE PROCESSED (E.g. name, address, Identification number etc.)	PURPOSE OF PROCESSING (E.g. for payroll, invoicing, Know Your Customer (KYC), registration, etc.)

SECTION 3 – SENSITIVE PERSONAL DATA

Applicable ( ) Not Applicable ( )

If applicable, please fill in the below details, otherwise please proceed to section 4

Please select the type(s) of sensitive categories of personal data you process	Specify purpose(s) for processing sensitive personal data:
Racial or ethnic origin	
Political opinion or adherence	
Religious or philosophical beliefs	
Marital status and family details	
Physical or mental health or condition	
Sexual orientation, practices or preferences	
biometric data	

SECTION 4 – TRANSFER OF DATA OUTSIDE KENYA

Applicable ( ) Not Applicable ( )

If applicable, please fill in the below details, otherwise please proceed to section 5.

List the country/(ies):

SECTION 5 – MEASURES FOR PROTECTION OF PERSONAL DATA

No.	Identify risks to personal data (E.g. unauthorized access/disclosure, theft, etc.)	Safeguards, security measures and mechanisms implemented to protect personal data (E.g. Access control, visitors' logbook, privacy policy, information security policy, etc.)
1		
2		
3		
4		
5		

SECTION 6: NUMBER OF EMPLOYEES (INDICATE BY TICKING)

Organization with 1-9 employees	
Organization with 10-49 employees	
Organization with 50-99 employees	
Organization with more than 99 employees	

SECTION 7: PREVIOUS YEAR ANNUAL TURNOVER (INDICATE BY TICKING)

Organization has less than KES 2,000,000 annual turnover	
Organization has KES 2,000,000-5,000,000 annual turnover	
Organization has KES 5,000,000-10,000,000 annual turnover	
Organization has KES 10,000,000-50,000,000 annual turnover	
Organization with more than KES 50,000,000 annual turnover	

I certify that the particulars provided are correct and complete and hereby apply to be registered as Data Controller or a data Processor.

Signature: _____

Date: _____

Name: _____

FORMDPR 2 (r. 11 (2)(a))

RENEWAL FORM FOR DATA CONTROLLERS AND DATA PROCESSORS

Indicate if you are registering as a—

Data Controller ☐ Data Processor ☐

SECTION 1 – BASIC DETAILS	
Name:	
Postal Address:	
Telephone Number:	
Email Address:	
Country:	
Sector:	
Legal Establishment	
For public body: (Specify the state department or county department)	
SECTION 2: DISTINCT PURPOSE	
Specify whether renewal is for a distinct purpose or categories of data other than that for which the data controller or data processor had been registered for, respectively-	

SECOND SCHEDULE

Fees charged by office(r. 5(2)(b)

Category	*Description*	*Registration fee in Kshs. per Data Controller/Processor) (payable Once)*	*Renewal fee in Kshs. per Data Controller/Processor) (after every 2 years)*
Micro and Small Data Controllers /Processors	A data controller/ processor with between 1 and 50 employees and an annual turnover/revenue of a maximum of Kshs 5Million	4,000	2,000
Medium Data Controllers /Processors	A data controller/ processor with between 51 and 99 employees and an annual turnover/revenue of between Kshs 5,000,001 and maximum of Kshs 50,000,000	16,000	9,000
Large Data Controllers /Processors	Data controller/processor with more than 99 employees and an annual turnover/revenue of more than Kshs 50Million	40,000	25,000

Public entities	Data controller/processor offering government functions (Regardless of number of employees or revenue/turnover)	4,000	2,000
Charities and Religious entities	Data controller or Data processor offering charity or religious functions (Regardless or revenue/turnover)	4,000	2,000

THIRD SCHEDULE

THRESHOLDS FOR MANDATORY REGISTRATION *(r. 13(3))*

A data controller or data processor processing personal data for the following purposes shall register as a data controller or a data processor as provided for under these Regulations—

1. Canvassing political support among the electorate.
2. Crime prevention and prosecution of offenders (including operating security CCTV systems).
3. Gambling.
4. Operating an educational institution.
5. Health administration and provision of patient care.
6. Hospitality industry firms but excludes tour guides.
7. Property management including the selling of land.
8. Provision of financial services.
9. Telecommunications network or service providers.
10. Businesses that are wholly or mainly in direct marketing.
11. Transport services firms (including online passenger hailing applications)
12. Businesses that process genetic data.

Made on the 7th December, 2021.

JOE MUCHERU,
Cabinet Secretary, Ministry of Information, Communication, Technology, Innovation and Youth Affairs.

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

ANNEX 3

THE REPUBLIC OF KENYA

LAWS OF KENYA

DATA PROTECTION ACT

NO. 24 OF 2019

Published by the National Council for Law Reporting
with the Authority of the Attorney-General

www.kenyalaw.org

NO. 24 OF 2019

DATA PROTECTION ACT

ARRANGEMENT OF SECTIONS

PART I – PRELIMINARY

Sections

PART XI — MISCELLANEOUS PROVISIONS

NO. 24 OF 2019

DATA PROTECTION ACT

[*Date of assent: 8th November, 2019.*]

[*Date of commencement: 25th November, 2019.*]

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; 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; and for connected purposes

[Act No. 24 of 2019.]

PART I — PRELIMINARY

1. Short title

This Act may be cited as the Data Protection Act, 2019.

2. Interpretation

In this Act, unless the context otherwise requires—

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

"biometric data" means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

"Cabinet Secretary" means the Cabinet Secretary responsible for matters relating to information, communication and technology;

"consent" means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject;

"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 paragraphs (a), (b) or (c), forms part of an accessible record; or

(e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

"Data Commissioner" means the person appointed under section 6;

"data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;

"data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"data subject" means an identified or identifiable natural person who is the subject of personal data;

"encryption" means the process of converting the content of any readable data using technical means into coded form;

"filing system" means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"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;

"identifiable natural person" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

"national security organs" has the meaning assigned to it under Article 239 of the Constitution;

"Office" means the office of the Data Protection Commissioner;

"person" has the meaning assigned to it under Article 260 of the Constitution;

"personal data" means any information relating to an identified or identifiable natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

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

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects 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 or movements;

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

"register" means the register kept and maintained by the Data Commissioner under section 21;

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject; and

"third Party" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

3. Object and purpose of this Act

The object and purpose of this Act is —

(a) to regulate the processing of personal data;

(b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25;

(c) to protect the privacy of individuals;

(d) to establish the legal and institutional mechanism to protect personal data; and

(e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

4. Application

This Act applies to the processing of personal data—

(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means:

Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;

(b) by a data controller or data processor who—

(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or

(ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.

PART II — ESTABLISHMENT OF THE OFFICE OF DATA PROTECTION COMMISSIONER

5. Establishment of the Office

(1) There is established the office of the Data Protection Commissioner which shall be a body corporate with perpetual succession and a common seal and shall in its corporate name, be capable of—

(a) suing and being sued;

(b) taking, purchasing or otherwise acquiring, holding, charging or disposing of movable and immovable property;

(c) entering into contracts; and

(d) doing such other legal acts necessary for the proper performance of the functions of the Office.

(2) The Office is designated as a State Office in accordance with Article 260 (q) of the Constitution.

(3) The Office shall comprise the Data Commissioner as its head and accounting officer, and other staff appointed by the Data Commissioner.

(4) The Office shall ensure reasonable access to its services in all parts of the Republic.

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

6. Appointment of the Data Commissioner

(1) The Public Service Commission shall, whenever a vacancy arises in the position of the Data Commissioner, initiate the recruitment process.

(2) The Public Service Commission shall, within seven days of being notified of a vacancy under subsection (1), invite applications from persons who qualify for nomination and appointment for the position of the Data Commissioner.

(3) The Public Service Commission shall within twenty-one days of receipt of applications under subsection (2)—

(a) consider the applications received to determine their compliance with this Act;

(b) shortlist qualified applicants;

(c) publish and publicise the names of the applicants and the shortlisted applicants;

(d) conduct interviews of the shortlisted persons in an open and transparent process;

(e) nominate three qualified applicants in the order of merit for the position of Data Commissioner; and

(f) submit the names of the persons nominated under paragraph (e) to the President.

(4) The President shall nominate and, with approval of the National Assembly, appoint the Data Commissioner.

7. Qualifications of Data Commissioner

(1) A person shall be qualified for appointment as the Data Commissioner if that person—

(a) holds a degree from a university recognized in Kenya in—
  (i) data science;
  (ii) law;
  (iii) information technology; or
  (iv) any other related field;
(b) has knowledge and relevant experience of not less than ten years;
(c) meets the requirements of Chapter Six of the Constitution; and
(d) holds a master's degree.

(2) The Data Commissioner shall be appointed for a single term of six years and shall not be eligible for a reappointment.

8. Functions of the Office

(1) The Office shall—
(a) oversee the implementation of and be responsible for the enforcement of this Act;
(b) establish and maintain a register of data controllers and data processors;
(c) exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;
(d) promote self-regulation among data controllers and data processors;
(e) conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;
(f) receive and investigate any complaint by any person on infringements of the rights under this Act;
(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;
(h) carry out inspections of public and private entities with a view to evaluating the processing of personal data;
(i) promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;
(j) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals; and
(k) perform such other functions as may be prescribed by any other law or as necessary for the promotion of object of this Act.

(2) The Office of the Data Commissioner may, in the performance of its functions collaborate with the national security organs.

(3) The Data Commissioner shall act independently in exercise of powers and carrying out of functions under this Act.

9. Powers of the Office

(1) The Data Commissioner shall have power to—

(a) conduct investigations on own initiative, or on the basis of a complaint made by a data subject or a third party;

(b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate;

(c) facilitate conciliation, mediation and negotiation on disputes arising from this Act;

(d) issue summons to a witness for the purposes of investigation;

(e) require any person that is subject to this Act to provide explanations, information and assistance in person and in writing;

(f) impose administrative fines for failures to comply with this Act;

(g) undertake any activity necessary for the fulfilment of any of the functions of the Office; and

(h) exercise any powers prescribed by any other legislation.

(2) The Data Commissioner may enter into association with other bodies or organisations within and outside Kenya as appropriate in furtherance of the object of this Act.

10. Delegation by the Data Commissioner

The Data Commissioner may, subject to such conditions as the Data Commissioner may impose, delegate any power conferred under this Act or any other written law to a regulator established through an Act of Parliament.

11. Vacancy in the Office of the Data Commissioner

The Office of the Data Commissioner shall become vacant, if the Data Commissioner—

(a) dies;

(b) resigns from office by notice in writing addressed to the President;

(c) is convicted of an offence and sentenced to imprisonment for a term exceeding six months without the option of a fine;

(d) is removed from office on the grounds of—

(i) inability to perform the functions of office arising from mental or physical infirmity;

(ii) non-compliance with Chapter Six of the Constitution;

(iii) bankruptcy;

(iv) incompetence; or

(v) gross misconduct.

12. Removal of the Data Commissioner

(1) A person desiring the removal of Data Commissioner on any ground specified under section 11(d) may present a complaint to the Public Service Commission setting out the alleged facts constituting that ground.

(2) Subject to Article 47 of the Constitution, the Public Service Commission shall consider the complaint and, if satisfied that the complaint discloses a ground under section 11(d), shall—

(a) investigate the matter expeditiously;

(b) report on the facts; and

(c) make a recommendation to the Cabinet Secretary.

(3) Prior to any action under sub-section (2), the Data Commissioner shall be—

(a) informed, in writing, of the reasons for the intended removal; and

(b) offered an opportunity to put in a defence against any such allegations.

13. Staff of the Office

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.

14. Remuneration of the Data Commissioner and staff

The Data Commissioner and staff of the Office shall be paid such remuneration or allowances as the Salaries and Remuneration Commission may advise.

15. Oath of office

The Data Commissioner shall take the oath set out in the First Schedule on appointment.

16. Confidentiality agreement

The Data Commissioner, or any staff of the Office, shall not, unless with lawful authority, disclose any information obtained for the purposes of this Act.

17. Protection from personal liability

The Data Commissioner or any staff of the Office shall not be held liable for having performed any of their functions in good faith and in accordance with this Act.

PART III — REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

18. Registration of data controllers and data processors

(1) Subject to sub-section (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner.

(2) The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider—

(a) the nature of industry;

(b) the volumes of data processed;

(c) whether sensitive personal data is being processed; and

(d) any other criteria the Data Commissioner may specify.

19. Application for registration

(1) A data controller or data processor required to register under section 18 shall apply to the Data Commissioner.

(2) An application under sub-section (1) shall provide the following particulars—

(a) a description of the personal data to be processed by the data controller or data processor;

(b) a description of the purpose for which the personal data is to be processed;

(c) the category of data subjects, to which the personal data relates;

(d) contact details of the data controller or data processor;

(e) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data;

(f) any measures to indemnify the data subject from unlawful use of data by the data processor or data controller; and

(g) any other details as may be prescribed by the Data Commissioner.

(3) A data controller or data processor who knowingly supplies any false or misleading detail under sub-section (1) commits an offence.

(4) The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.

(5) A data controller or data processor shall notify the Data Commissioner of a change in any particular outlined under subsection (2).

(6) On receipt of a notification under sub-section (5), the Data Commissioner shall amend the respective entry in the Register.

(7) A data controller or data processor who fails to comply with the provisions of this section commits an offence.

20. Duration of the registration certificate

A registration certificate issued under section 19 shall be valid for a period determined at the time of the application after taking into account the need for the certificate, and the holder may apply for a renewal of the certificate after expiry of the certificate.

21. Register of data controllers and data processors

(1) The Data Commissioner shall keep and maintain a register of the registered data controllers and data processors.

(2) The Data Commissioner may, at the request of a data controller or data processor, remove any entry in the register which has ceased to be applicable.

(3) The register shall be a public document and available for inspection by any person.

(4) A person may request the Data Commissioner for a certified copy of any entry in the register.

22. Cancellation or variation of the certificate

The Data Commissioner may, on issuance of a notice to show cause, vary terms and conditions of the certificate of registration or cancel the registration where—

(a) any information given by the applicant is false or misleading; or

(b) the holder of the registration certificate, without lawful excuse, fails to comply with any requirement of this Act.

23. Compliance and audit

The Data Commissioner may carry out periodical audits of the processes and systems of the data controllers or data processors to ensure compliance with this Act.

24. Designation of the Data Protection Officer

(1) A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where—

(a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;

(b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects; or

(c) the core activities of the data controller or the data processor consist of processing of sensitive categories of personal data.

(2) A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.

(3) A group of entities may appoint a single data protection officer provided that such officer is accessible by each entity.

(4) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures.

(5) A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

(6) A data controller or data processor shall publish the contact details of the data protection officer on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

(7) A data protection officer shall—

(a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;

(b) ensure on behalf of the data controller or data processor that this Act is complied with;

(c) facilitate capacity building of staff involved in data processing operations;

(d) provide advice on data protection impact assessment; and

(e) co-operate with the Data Commissioner and any other authority on matters relating to data protection.

PART IV — PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

25. Principles of data protection

Every data controller or data processor shall ensure that personal data is—

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

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

(f) 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;

(g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

(h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

26. Rights of a data subject

A data subject has a right—

(a) to be informed of the use to which their personal data is to be put;

(b) to access their personal data in custody of data controller or data processor;

(c) to object to the processing of all or part of their personal data;

(d) to correction of false or misleading data; and

(e) to deletion of false or misleading data about them.

27. Exercise of rights of data subjects

A right conferred on a data subject may be exercised—

(a) where the data subject is a minor, by a person who has parental authority or by a guardian;

(b) where the data subject has a mental or other disability, by a person duly authorised to act as their guardian or administrator; or

(c) in any other case, by a person duly authorised by the data subject.

28. Collection of personal data

(1) A data controller or data processor shall collect personal data directly from the data subject.

(2) Despite sub-section (1), personal data may be collected indirectly where—

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public;

(c) the data subject has consented to the collection from another source;

(d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source;

(e) the collection from another source would not prejudice the interests of the data subject;

(f) collection of data from another source is necessary—

(i) for the prevention, detection, investigation, prosecution and punishment of crime;

(ii) for the enforcement of a law which imposes a pecuniary penalty; or

(iii) for the protection of the interests of the data subject or another person.

(3) A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.

29. Duty to notify

A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of—

(a) the rights of data subject specified under section 26;

(b) the fact that personal data is being collected;

(c) the purpose for which the personal data is being collected;

(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;

(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;

(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and

(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

30. Lawful processing of personal data

(1) A data controller or data processor shall not process personal data, unless—

(a) the data subject consents to the processing for one or more specified purposes; or

(b) the processing is necessary—

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(ii) for compliance with any legal obligation to which the controller is subject;

(iii) in order to protect the vital interests of the data subject or another natural person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public authority;

(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

(2) Further processing of personal data shall be in accordance with the purpose of collection.

(3) A data controller who contravenes the provisions of sub-section (1) commits an offence.

31. Data protection impact assessment

(1) Where a processing 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.

(2) A data protection impact assessment shall include the following—

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects;

(d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

(3) The data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.

(4) For the purposes of this section, a "data protection impact assessment" means an assessment of the impact of the envisaged processing operations on the protection of personal data.

(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.

32. Conditions of consent

(1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) The withdrawal of consent under sub-section (2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

33. Processing of personal data relating to a child

(1) Every data controller or data processor shall not process personal data relating to a child unless—

(a) consent is given by the child's parent or guardian; and

(b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.

(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of—

(a) available technology;

(b) volume of personal data processed;

(c) proportion of such personal data likely to be that of a child;

(d) possibility of harm to a child arising out of processing of personal data; and

(e) such other factors as may be specified by the Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).

34. Restrictions on processing

(1) A data controller or data processor shall, at the request of a data subject, restrict the processing of personal data where—

(a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;

(b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defence of a legal claim;

(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(d) data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

(2) Where processing of personal data is restricted under this section—

(a) the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) the data controller shall inform the data subject before withdrawing the restriction on processing of the personal data.

(3) The data controller or data processor shall implement mechanisms to ensure that time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, is observed.

35. Automated individual decision making

(1) Every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.

(2) Sub-section (1) shall not apply where the decision is—

(a) necessary for entering into, or performing, a contract between the data subject and a data controller;

(b) authorised by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) based on the data subject's consent.

(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—

(a) the data controller or data processor must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and

(b) the data subject may, after a reasonable period of receipt of the notification, request the data controller or data processor to—

(i) reconsider the decision; or

(ii) take a new decision that is not based solely on automated processing.

(4) A data controller or data processor, upon receipt of a request under sub-section (3), shall within a reasonable period of time —

(a) consider the request, including any information provided by the data subject that is relevant to it;

(b) comply with the request; and

(c) by notice in writing inform the data subject of—

(i) the steps taken to comply with the request; and

(ii) the outcome of complying with the request.

(5) The Cabinet Secretary may by Regulations make such further provision to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of decisions based solely on automated processing.

36. Objecting to processing

A data subject has a 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.

37. Commercial use of data

(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.

38. Right to data portability

(1) A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit the data obtained under sub-section (1), to another data controller or data processor without any hindrance.

(3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.

(4) Where data controller or data processor declines to comply with a request under sub-section (3), the Data Commissioner may make a determination on the technical capacity of the data controller or data processor.

(5) The right under this section shall not apply in circumstances where—

(a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or

(b) it may adversely affect the rights and freedoms of others.

(6) A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of thirty days.

(7) Where the portability request is complex or numerous, the period under sub-section (6) may be extended for a further period as may be determined in consultation with the Data Commissioner.

39. Limitation to retention of personal data

(1) A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is—

(a) required or authorised by law;

(b) reasonably necessary for a lawful purpose;

(c) authorised or consented by the data subject; or

(d) for historical, statistical, journalistic literature and art or research purposes.

(2) A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section (1) in a manner as may be specified at the expiry of the retention period.

40. Right of rectification and erasure

(1) A data subject may request a data controller or data processor—

(a) to rectify without undue delay personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading; or

(b) to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(2) Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested—

(a) the rectification of such personal data in their possession or under their control that is inaccurate, out-dated, incomplete or misleading; or

(b) the erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(3) 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.

41. Data protection by design or by default

(1) Every data controller or data processor shall implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner; and

(b) to integrate necessary safeguards for that purpose into the processing.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing.

(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration—

(a) the amount of personal data collected;

(b) the extent of its processing;

(c) the period of its storage;

(d) its accessibility; and

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

(4) To give effect to this section, the data controller or data processor shall consider measures such as—

(a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;

(b) to establish and maintain appropriate safeguards against the identified risks;

(c) to the pseudonymisation and encryption of personal data;

(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) to verify that the safeguards are effectively implemented; and

(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.

42. Particulars of determining organisational measures

(1) In determining the appropriate measures referred to in section 41, in particular, where the processing involves the transmission of data over an

information and communication network, a data controller shall have regard to—

(a) the state of technological development available;

(b) the cost of implementing any of the security measures;

(c) the special risks that exist in the processing of the data; and

(d) the nature of the data being processed.

(2) Where a data controller is using the services of a data processor —

(a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of organisational measures for the purpose of complying with section 41(1); and

(b) the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

(3) Where a data processor processes personal data other than as instructed by the data controller, the data processor shall be deemed to be a data controller in respect of that processing.

(4) A data controller or data processor shall take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor, complies with the relevant security measures.

43. Notification and communication of breach

(1) Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall—

(a) notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and

(b) subject to subsection (3), communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.

(2) Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.

(3) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach.

(4) The data controller may delay or restrict communication referred to under subsection (1)(b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

(5) The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including—

(a) description of the nature of the data breach;

(b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;

(c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and

(e) the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.

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

(7) Where and to the extent that it is not possible to provide all the information mentioned in subsection (5) at the same time, the information may be provided in phases without undue delay.

(8) The data controller shall record the following information in relation to a personal data breach—

(a) the facts relating to the breach;

(b) its effects; and

(c) the remedial action taken.

PART V— GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

44. Processing of sensitive personal data

No category of sensitive personal data shall be processed unless section 25 applies to that processing.

45. Permitted grounds for processing sensitive personal data

Without prejudice to section 44, sensitive personal data of a data subject may be processed where—

(a) the processing is carried out in the course of 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—

(i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and

(ii) the personal data is not disclosed outside that body without the consent of the data subject.

(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 interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

46. Personal data relating to health

(1) Personal data relating to the health of a data subject may only be processed—

(a) by or under the responsibility of a health care provider; or

(b) by a person subject to the obligation of professional secrecy under any law.

(2) The condition under subsection (1) is met if the processing—

(a) is necessary for reasons of public interest in the area of public health; or

(b) is carried out by another person who in the circumstances owes a duty of confidentiality under any law.

47. Further categories of sensitive personal data

(1) The Data Commissioner may prescribe further categories of personal data which may be classified as sensitive personal data.

(2) Where categories of personal data have been specified as sensitive personal data under subsection (1), the Data Commissioner may specify any further grounds on which such specified categories may be processed, having regard—

(a) to the risk of significant harm that may be caused to a data subject by the processing of such category of personal data;

(b) to the expectation of confidentiality attached to such category of personal data;

(c) to whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and

(d) to the adequacy of protection afforded by ordinary provisions applicable to personal data.

(3) The Data Commissioner may specify other categories of personal data, which may require additional safeguards or restrictions.

PART VI —TRANSFER OF PERSONAL DATA OUTSIDE KENYA

48. Conditions for transfer out of Kenya

A data controller or data processor may transfer personal data to another country only where—

(a) 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;

(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;

(c) the transfer is necessary—

(i) for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) 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; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

49. Safeguards prior to transfer of personal data out of Kenya

(1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

(2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests.

(3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

50. Processing through a data server or data centre in Kenya

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.

PART VII — EXEMPTIONS

51. General exemptions

(1) Nothing in this Part shall exempt any data controller or data processor from complying with data protection principles relating to lawful processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data.

(2) The processing of personal data is exempt from the provisions of this Act if—

(a) it relates to processing of personal data by an individual in the course of a purely personal or household activity;

(b) if it is necessary for national security or public interest; or

(c) disclosure is required by or under any written law or by an order of the court.

52. Journalism, literature and art

(1) The principles of processing personal data shall not apply where—

(a) processing is undertaken by a person for the publication of a literary or artistic material;

(b) data controller reasonably believes that publication would be in the public interest; and

(c) data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

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

(3) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Journalism, Literature and Art.

53. Research, history and statistics

(1) The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes and the data controller or data processor shall ensure that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

(2) The data controller or data processor shall take measures to establish appropriate safeguards against the records being used for any other purposes.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if—

(a) data is processed in compliance with the relevant conditions; and

(b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

(4) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Research, History and Statistics.

54. Exemptions by the Data Commissioner

The Data Commissioner may prescribe other instances where compliance with certain provisions of this Act may be exempted.

55. Data-sharing code

(1) The Data Commissioner may issue a data sharing code which shall contain—

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation; and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) The data sharing code under subsection (1) shall specify on the lawful exchange of personal data between government departments or public sector agencies.

PART VIII — ENFORCEMENT PROVISIONS

56. Complaints to the Data Commissioner

(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 the complaint 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.

57. Investigation of complaints

(1) The Data Commissioner may, for the purpose of the investigation of a complaint, order any person to—

(a) attend at a specified time and place for the purpose of being examined orally in relation to the complaint;

(b) produce such book, document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other enactment from disclosing; or

(c) furnish a statement in writing made under oath or on affirmation setting out all information which may be required under the notice.

(2) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Data Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(3) A person who, without reasonable excuse, fails or refuses to comply with a notice, or who furnishes to the Data Commissioner any information which the person knows to be false or misleading, commits an offence.

58. Enforcement notices

(1) Where the Data Commissioner is satisfied that a person has failed, or is failing, to comply with any provision of this Act, the Data Commissioner may serve an enforcement notice on that person requiring that person to take such steps and within such period as may be specified in the notice.

(2) An enforcement notice served under subsection (1) shall—

(a) specify the provision of this Act which has been, is being or is likely to be, contravened;

(b) specify the measures that shall be taken to remedy or eliminate the situation which makes it likely that a contravention will arise;

(c) specify a period which shall not be less than twenty-one days within which those measures shall be implemented; and

(d) state any right of appeal.

(3) Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

59. Power to seek assistance

For the purpose of gathering information or for any investigation under this Act, the Data Commissioner may seek the assistance of such person or authority as they deem fit and as is reasonably necessary to assist the Data Commissioner in the discharge of their functions.

60. Power of entry and search

The Data Commissioner, upon obtaining a warrant from a Court, may enter and search any premises for the purpose of discharging any function or exercising any power under this Act.

61. Obstruction of Data Commissioner

A person who, in relation to the exercise of a power conferred by section 9 —

(a) obstructs or impedes the Data Commissioner in the exercise of their powers;

(b) fails to provide assistance or information requested by the Data Commissioner;

(c) refuses to allow the Data Commissioner to enter any premises or to take any person with them in the exercise of their functions;

(d) gives to the Data Commissioner any information which is false or misleading in any material aspect,

commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

62. Penalty notices

(1) If the Data Commissioner is satisfied that a person has failed or is failing as described in section 58, the Data Commissioner may issue a penalty notice requiring the person to pay to the Office of the Data Commissioner an amount specified in the notice.

(2) In deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Data Commissioner shall, so far as relevant, have regard—

(a) to the nature, gravity and duration of the failure;

(b) to the intentional or negligent character of the failure;

(c) to any action taken by the data controller or data processor to mitigate the damage or distress suffered by data subjects;

(d) to the degree of responsibility of the data controller or data processor, taking into account technical and organisational measures;

(e) to any relevant previous failures by the data controller or data processor;

(f) to the degree of co-operation with the Data Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) to the categories of personal data affected by the failure;

(h) to the manner in which the infringement became known to the Data Commissioner, including whether, and if so to what extent, the data controller or data processor notified the Data Commissioner of the failure;

(i) to the extent to which the data controller or data processor has complied with previous enforcement notices or penalty notices;

(j) to adherence to approved codes of conduct or certification mechanisms;

(k) to any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) to whether the penalty would be effective, proportionate and dissuasive.

63. Administrative fines

In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

64. Right of appeal

A person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court.

65. Compensation to a data subject

(1) A person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor.

(2) Subject to subsection (1) —

(a) a data controller involved in processing of personal data is liable for any damage caused by the processing; and

(b) a data processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the Act specifically directed at data processors; or

(ii) has acted outside, or contrary to, the data controller's lawful instructions.

(3) A data controller or data processor is not liable in the manner specified in subsection (2) if the data controller or data processor proves that they are not in any way responsible for the event giving rise to the damage.

(4) In this section, **"damage"** includes financial loss and damage not involving financial loss, including distress.

66. Preservation Order

The Data Commissioner may apply to a court for a preservation order for the expeditious preservation of personal data including traffic data, where there is reasonable ground to believe that the data is vulnerable to loss or modification.

PART IX — FINANCIAL PROVISIONS

67. Funds of the Office

The funds and assets of the Office shall consist of—

(a) monies allocated by the National Assembly for purposes of the Office;

(b) any grants, gifts, donations or other endowments given to the Office; and

(c) such funds as may vest in or accrue to the Office in the performance of its functions under this Act or any other written law.

68. Annual estimates

(1) At least three months before the commencement of each financial year, the Data Commissioner shall cause to be prepared estimates of the revenue and expenditure of the Office for that year.

(2) The annual estimates shall make provision for all the estimated expenditure of the Office for the financial year concerned and in particular shall provide for—

(a) the payment of salaries, allowances and other charges in respect of the staff of the Office;

(b) the payment of pensions, gratuities and other charges in respect of retirement benefits which are payable out of the finances of the Office;

(c) the acquisition, maintenance, repair and replacement of the equipment and other movable property of the Office;

(d) funding of training, research and development of activities of the Office;

(e) the creation of such reserve funds to meet future or contingent liabilities or in respect of such other matters as the Data Commissioner may deem fit; and

(f) any other expenditure for the purposes of this Act.

(3) The annual estimates shall be submitted to the Cabinet Secretary for tabling in the National Assembly.

69. Accounts and Audit

The annual accounts of the Office shall be prepared, audited and reported in accordance with the provisions of Articles 226 and 229 of the Constitution, the Public Finance Management Act, 2012 (No. 18 of 2012), or any other law relating to audit of public entities.

70. Annual reports

(1) The Data Commissioner shall, within three months after the end of each financial year, prepare and submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year.

(2) The Cabinet Secretary shall submit the annual report before the National Assembly within three months of receipt of the report under subsection (1).

(3) The annual report shall contain in respect of the year to which it relates—

(a) the financial statements and description of activities of the Office;

(b) such other statistical information as the Data Commissioner may consider appropriate relating to the Data Commissioner's functions;

(c) the impact of the exercise of any of Data Commissioner's mandate or function;

(d) any impediments to the achievements of the object and purpose of this Act or any written law; and

(e) any other information relating to its functions that the Data Commissioner may consider necessary.

PART X — PROVISIONS ON DELEGATED POWERS

71. Regulations

(1) The Cabinet Secretary may, make regulations generally for giving effect to this Act, and for prescribing anything required or necessary to be prescribed by or under this Act.

(2) Without prejudice to the generality of subsection (1), regulations made under that subsection may provide for—

(a) the requirements which are imposed on a data controller or data processor when processing personal data;

(b) mechanisms of conducting certification program;

(c) the contents which a notice or registration by a data controller or data processor should contain;

(d) information to be provided to a data subject and how such information shall be provided;

(e) the levying of fees and taking of charges;

(f) the measures to safeguard a data subject's rights, freedoms and legitimate interests;

(g) the processing of data through a data server or data centre in Kenya;

(h) issuing and approval of codes of practice and guidelines; or

(i) any other matter that the Cabinet Secretary may deem fit.

(3) For the purposes of Article 94 (6) of the Constitution—

(a) the purpose and objective of the delegation under this section is to enable the Cabinet Secretary to make regulations for better carrying into effect the provisions of this Act;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and fulfilment of the objectives specified under this section.

(4) The principles and standards applicable to the delegated power referred to under this Act are those found in—

(a) the Statutory Instruments Act, 2013 (No. 23 of 2013);

(b) the Interpretation and General Provisions Act (Cap. 2);

(c) the general rules of international law as specified under Article 2 (5) of the Constitution; and

(d) any treaty and convention ratified by Kenya under Article 2 (6) of the Constitution.

PART XI — MISCELLANEOUS PROVISIONS

72. Offences of unlawful disclosure of personal data

(1) A data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected commits an offence.

(2) A data processor who, without lawful excuse, discloses personal data processed by the data processor without the prior authority of the data controller commits an offence.

(3) Subject to subsection (4), a person who—

(a) obtains access to personal data, or obtains any information constituting such data, without prior authority of the data controller or data processor by whom the data is kept; or

(b) discloses personal data to third party, commit an offence.

(4) Subsection (3) shall not apply to a person who is an employee or agent of a data controller or data processor acting within the scope of such mandate.

(5) A person who offers to sell personal data where such personal data has been obtained in breach of subsection (1) commits an offence.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

73. General penalty

(1) A person who commits an 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 three million shillings or to an imprisonment term not exceeding ten years, or to both.

(2) In addition to any penalty referred to in subsection (1), the Court may—

(a) order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence; or

(b) order or prohibit the doing of any act to stop a continuing contravention.

74. Codes, guidelines and certification

(1) The Data Commissioner may, for the purpose of this Act —

(a) issue guidelines or codes of practice for the data controllers, data processors and data protection officers;

(b) offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with this Act;

(c) require certification or adherence to code of practice by a third party;

(d) develop sector specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education, social Protection and any other area as the Data Commissioner may determine.

(2) A certification issued under this section shall not alter the responsibility of the data controller or data processor for compliance with this Act.

75. Consequential amendments

The laws specified under the Second Schedule are amended in the manner specified.

FIRST SCHEDULE

[Section 15.]

I, ..., make oath/solemnly affirm/declare that I will faithfully and honestly fulfil my duties as the Data Commissioner in conformity with the Data Protection Act and that I shall not, without the due authority in that behalf, disclose or make known any matter or thing which comes to my knowledge by reason of discharge of my duties.

.....
Magistrate/Judge

SECOND SCHEDULE

[Section 75.]

CONSEQUENTIAL AMENDMENTS

Written Law	*Provision*	*Amendment*
Births and Deaths Act *(Cap 149)*	s. 7	Add the following new sub-section immediately after subsection (3)— (4) The Register shall be maintained in accordance with the principles of data protection set out in the Data Protection Act.
Capital Markets Act *(Cap 485A)*	s.11(3)	Insert the following new paragraph immediately after paragraph (v)— (va) ensure processing of personal data in the operations of capital markets is in accordance with principles set out under the Data Protection Act, 2019.
	Insertion of new section	Insert the following new section immediately after section 13B—
	Data protection principles	**13C.** The principles of personal data protection as set out in the Data Protection Act shall apply to the collection and processing of personal data by the Authority or any person authorized by the Authority.
	s. 18C (2)	Insert the following new paragraph immediately after paragraph (d) — (e) mechanisms of protecting personal data of the data subjects in compliance with the Data Protection Act.
Independent Electoral and Boundaries Commission Act	s. 25	Adding the following new paragraph immediately after paragraph (h) — (i) the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters under this Act.

	s.27	Adding the following new subsection immediately after subsection (5) — (6) The Commission shall ensure the management of personal data is in accordance with the principles of personal data protection as set out in the Data Protection Act.
Kenya National Examinations Council Act	s.10(2)	Insert the following new paragraph immediately after paragraph (m)— (n) to align its Regulations on the collection and processing of information which consists of personal data with the Data Protection Act.
Employment Act, 2007	s.61	Adding the following new subsection— (2) Where an employer maintains such a register, the register shall be maintained in accordance with the principles of data protection as set out in the Data Protection Act.
The Kenya Citizenship and Immigration Act, 2011	Insertion of new section	Insert the following new section immediately after section 3— Personal data of individuals 3A. Personal data of individuals obtained under this Act shall be held and maintained in accordance with the principles of data protection set out in the Data Protection Act.
Basic Education Act, 2013	s.79	Add the following new sub-section immediately after sub-section (2)— (3) The Board shall deal with any relevant personal data collected and so held in the register according to the data principles set out in the Data Protection Act.
Universities Act, 2012	s.13	Add the following new sub-section immediately after sub-section (3) —

		(3A) Any information containing personal data presented to the Commission shall be handled in accordance with data protection principles set out in the Data Protection Act.
The Central Depositories Act, 2000	s.36 (6)	Insert the following new sub-section immediately after sub-section (6) — (7) A record of depositors required by an issuer under sub-section (1) shall be issued and maintained in accordance with the principles of data protection set out in the Data Protection Act, 2019.
	s.47	Insert the following new sub-section immediately after sub-section (1)— (2) The disclosure of information under this Act shall be done according to the data principles set out in the Data Protection Act, 2019.
Anti-Money Laundering and Proceeds of Crime Act, 2009	s.40	Insert the following new sub-section immediately after sub-section (1)— (2) The sharing of information by the Centre shall be with adherence to the data principles set out in the Data Protection Act, 2019.
	s.13	Insert the following new sub-section immediately after sub-section (1)— (2) the information collected on natural persons under this section shall be dealt according to the data principles set out in the Data Protection Act, 2019.
Kenya Information and Communications Act, 1998	s.23 (2)	Insert the following new paragraph immediately after paragraph (c)— (ee) ensure processing of personal data of subscribers is in accordance with principles set out under the Data Protection Act, 2019.
	s.25 (3)	Insert the following new paragraph immediately after paragraph (c)— (cc) to ensure necessary steps are taken to secure the integrity of personal data under their possession or

control through the adoption of appropriate, reasonable, technical and organizational measures to prevent the loss of, damage to or unauthorized destruction and prevent any unlawful access to or unauthorized processing of personal data.

Insolvency Act, 2015 — s. 148 — Insert the following new section immediately after section 148-

148A. The principles of personal data protection set out in the Data protection Act, 2019 shall apply with necessary modifications to the processing and handling, by the bankruptcy trustee, of *the bankrupt's* personal data.

ANNEX 4

Public Notice on the Call for comments and the invitation to the public participation forums on the draft Data Protection Regulations

Published in My-Gov on 13th April 2021

REPUBLIC OF KENYA

MINISTY OF ICT,INNOVATION AND YOUTH AFFAIRS

OFFICE OF THE DATA PROTECTION COMMISSIONER

CALL FOR COMMENTS AND INVITATION FOR PUBLIC PARTICIPATION ON THE DRAFT DATA PROTECTION REGULATIONS, 2021.

The Ministry of ICT, Innovation and Youth Affairs through a Taskforce on the development of the Data Protection Regulations has formulated 3 sets of Regulations to actualize the Data Protection Act,2019 which seeks to safeguard the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes.

These Regulations are the:

1. **Data Protection (General) Regulations, 2021.**
   Which set out the procedures for enforcement of the rights of the data subjects as well as elaborating on the duties and obligations of the data controllers and data processors. These regulations can be accessed here ***https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/***

2. **Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.**
   The regulations defines the procedure that will be adopted by the Office of the Data Commissioner in registering data controllers and data processors as per the Data Protection Act. These regulations can be accessed here: ***https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021***

3. **Data Protection (Compliance and Enforcement) Regulations, 2021.**
   These regulations outline the compliance and enforcement provisions for Data Commissioner, Data Controllers and Data Processors. These regulations can be accessed here: ***https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/***

In accordance with the Constitution the Ministry invites interested members of the public to submit any representations that they may have on the draft regulations. The representations may be made orally or by written memoranda through:

1. Email addresses **dataprotectionregulations@odpc.go.ke** not later than **Tuesday 27th April 2021, at 12:00 noon.**
2. WhatsApp platforms on telephone numbers **0796954269 - Safaricom, 0752896867-Airtel** and **0778048164-Telkom** to be received not later than **Tuesday 27th April 2021, at 12:00 noon.**

Further the Ministry invites interested members of the public to a virtual public hearing on the draft regulations as follows:

Date: 27th April 2021
Time: 1400 Hours – 1600 Hours
Regulations: The Data protection (General) Regulations, 2021
Link for the Meeting:
https://moictke.webex.com/webappng/sites/moictke/meeting/info/ce4ff168337f4493b-7735c783136fd8e?isPopupRegisterView=true

Date: 28th April 2021
Time: 1400 Hours – 1600 Hours
Regulations: The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.
Link for the Meeting:
https://moictke.webex.com/webappng/sites/moictke/meeting/info/f3c87581bf9849e1b-299b9ac13ec5228?isPopupRegisterView=true

Date: 29th April 2021
Time: 1400 Hours – 1600 Hours
Regulations: The Data Protection (Compliance and Enforcement) Regulations, 2021
Link for the Meeting:
https://moictke.webex.com/webappng/sites/moictke/meeting/info/10610eec0078491c9c80b-69253a07ca8?isPopupRegisterView=true

Joe Mucheru, EGH
Cabinet Secretary.

ANNEX 5

Public Notice on the extension of the period on the submission of the Memoranda on the draft regulations from 27th April 2021 to 11th May 2021

Published in My-Gov on 27th April 2021

REPUBLIC OF KENYA

MINISTY OF ICT,INNOVATION AND YOUTH AFFAIRS

OFFICE OF THE DATA PROTECTION COMMISSIONER

EXTENSION OF PERIOD FOR SUBMISSION OF WRITTEN MEMORANDA ON THE DRAFT DATA PROTECTION REGULATIONS, 2021

The Cabinet Secretary, Ministry of Information, Communication Technology, Innovation and Youth Affairs, extends the period for submission of written memoranda on the Draft Data Protection Regulations, published on the 20th April, 2021 vide MyGov issue No.40/2020-2021, from Tuesday, the 27th April, 2021, mid-day to Tuesday, the 11th May, 2021, mid-day.

These Regulations are the:

1. **The Data Protection (General) Regulations, 2021.**
   Which set out the procedures for enforcement of the rights of the data subjects as well as elaborating on the duties and obligations of the data controllers and data processors.
   Download: https://bit.ly/3uRec1e

2. **Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.**
   These Regulations define the procedure that will be adopted by the Office of the Data Commissioner in registering data controllers and data processors as per the Data Protection Act, 2019.
   Download: https://bit.ly/3e8v9h0

3. **Data Protection (Compliance and Enforcement) Regulations, 2021.**
   These Regulations outline the enforcement provisions.
   Download: https://bit.ly/3uReDso

Written memorandum can be sent to:

1. Email address: **dataprotectionregulations@odpc.go.ke** to be received not later than **Tuesday, the 11th May, 2021 at 12:00 noon.**
2. WhatsApp platforms on the telephone numbers 0796954269-Safaricom, 0752896867-Airtel and 0778048164-Telkom to be received not later than **Tuesday, the 11th May, 2021, at 12:00 noon.**

The Ministry further invites interested Members of the Public to Virtual Public Hearings on the draft regulations as follows:

1. **Date: Tuesday April 27th, 2021**
   Time: 1400 Hours – 1600 Hours
   Regulations: ***The Data protection (General) Regulations, 2021***
   Link for the Meeting: https://bit.ly/3tFoHV8
2. **Date: Wednesday April 28th, 2021**
   Time: 1400 Hours – 1600 Hours
   Regulations: ***The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.***
   Link for the Meeting: https://bit.ly/3xoZu3E
3. **Date: Thursday April 29th, 2021**
   Time: 1400 Hours – 1600 Hours
   Regulations: ***The Data Protection (Compliance and Enforcement) Regulations, 2021***
   Link for the Meeting: https://bit.ly/2QHJLvy

Joe Mucheru, EGH
Cabinet Secretary.

ANNEX 6

SPECIAL ISSUE

THE KENYA GAZETTE

Published by Authority of the Republic of Kenya

(Registered as a Newspaper at the G.P.O.)

Vol. CXXII—No. 105 **NAIROBI, 13th May, 2021** **Price Sh. 60**

GAZETTE NOTICE NO. 4695

THE CONSTITUTION OF KENYA

THE SENATE STANDING ORDERS

SPECIAL SITTING OF THE SENATE

NOTICE is given to all Senators that pursuant to standing order 30(1) of the Senate Standing Orders, on the request of the Senate Majority Leader and with the support of the requisite number of Senators, I have appointed Monday, 17th May, 2021 as a day for a special sitting of the Senate. The special sitting shall be held in the Senate Chamber, Main Parliament Buildings, Nairobi, commencing at 2.30 p.m.

The business to be transacted at the sitting shall be the consideration of the Report of the Special Committee on the Proposed Removal from the Office of the Governor of Wajir County.

In accordance with standing order 30(5) of the Senate Standing Orders, the business specified in this notice shall be the only business before the Senate during the special sitting, following which the Senate shall stand adjourned until Tuesday, 18th May, 2021, at 10.00 a.m., in accordance with the Senate Calendar.

Dated the 12th May, 2021.

KENNETH LUSAKA,
Speaker of the Senate.

GAZETTE NOTICE NO. 4696

THE NATIONAL YOUTH COUNCIL ACT

(No. 10 *of* 2009*)*

YOUTH ADVISORY BOARD

APPOINTMENT

IN EXERCISE of the powers conferred by section 16(2) of the National Youth Council Act, 2009, the Cabinet Secretary for Information, Communication and Technology, Innovation and Youth Affairs appoints—

Under paragraph (d) (i)—

Kevin Mogeni Machogu (Dr.)

Under paragraph (d) (ii)—

Njekele Ashura Michael

Under paragraph (d) (iii)—

Job Njau Njenga

Under paragraph (d) (v)—

Esha Mohamed Abdalla

Under paragraph (e)—

Angel Mbuthia

Alex Ali Kuuni

to be members of the Youth Advisory Board, for a period of three (3) years.

Dated the12th May, 2021.

JOE MUCHERU,
Cabinet Secretary for Information,Communication and Technology, Innovation and Youth Affairs.

GAZETTE NOTICE NO. 4697

THE STATUTORY INSTRUMENTS ACT

(No. 23 *of* 2013*)*

REGULATORY IMPACT STATEMENT

PURSUANT to section 8 of the Statutory Instruments Act, 2013, the Cabinet Secretary for ICT, Innovation and Youth Affairs notifies the general public that a Regulatory Impact Statement on the proposed Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 has been prepared to assess the impact of the Regulations on the community and businesses.

The main objective of the proposed regulations is to facilitate the registration of data controllers and data processors pursuant to Part III of the Data Protection Act, 2019 ('the Act'). Specifically, the Regulations seek to provide for—

(a) the procedure for registration of data controllers and data processors;

(b) the procedure for renewal of registration;

(c) the charging of regulatory fees by the Data Commissioner;

(d) the creation of offences for breaches under the Regulations; and

(e) the imposition of fines by the Data Commissioner.

This is therefore to request all persons likely to be affected by the proposed Regulations to submit written memorandum to reach the undersigned within fourteen (14) days from the date of publication of this notice to the email address dataprotectionregulations@odpc.go.ke.

The draft Regulatory Impact Statement and the proposed Regulations are available on *www.odpc.go.ke*.

Dated the 4th May, 2021.

JOE MUCHERU,
Cabinet Secretary for ICT, Innovation and Youth Affairs.

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

REPUBLIC OF KENYA

MINISTRY OF ICT, INNOVATION AND YOUTH AFFAIRS

REGULATORY IMPACT STATEMENT

ON

THE DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATIONS, 2021

This Regulatory Impact Assessment (RIA) has been prepared by the Office of the Data Protection Commissioner pursuant to Section 6 and 7 of the Statutory Instruments Act (No. 23 of 2013)

May, 2021.

Table of Contents

1. BACKGROUND

1.1. The right to privacy is enshrined under Article 31 of the Constitution of Kenya 2010. The Data Protection Act No. 24 of 2019, enacted on 24th September 2019, gives effect to some aspects of the right to privacy. More particularly, the Act seeks to regulate the processing of personal data, protect the privacy of individuals as well as to establishing the legal and institutional mechanisms to protect the processing of personal data.

1.2. The enactment of this Act was a big milestone in appreciating the need to protect personal data in the age of digital evolution. Further, there have been concerted efforts by governments all over the world to regulate the processing activities that rely on personal data purposely to ensure safeguard privacy of their citizens.

1.3. To ensure full operationalization of the Data Protection Act, on 15th January 2021, the Cabinet Secretary in the Ministry ICT, Innovation and Youth Affairs established the Taskforce on Development of the Data Protection Regulations, to among others, develop the necessary draft regulations under this Act. The Taskforce has generated the draft Regulations to implement various provisions of the Act and subjected them for public input.

2. REGULATORY IMPACT ASSESSMENT

2.1 A regulatory impact assessment (RIA) is an evaluation conducted before a new regulation is introduced. It provides a detailed and systematic appraisal of the potential impact of a new regulation in order to assess whether the regulation is likely to achieve the desired objectives. RIAs promote evidence-based policy-making as new regulations typically lead to numerous impacts that are often difficult to foresee.

2.2 The central purpose of RIA is to ensure that regulation is welfare-enhancing from the societal viewpoint, in that, the benefits will surpass costs. RIA therefore has objectives of improving understanding of the real-world impact of regulatory action, including both the benefits and the costs of action, integrating multiple policy objectives, improving transparency and consultation and enhancing governmental accountability. The conduct of RIA involves a range of methods aimed at systematically assessing the negative and positive impacts of proposed and existing regulations.

2.3 The Statutory Instruments Act, No. 23 of 2013 provides the legal framework for the conduct of RIA in Kenya. Particularly, Sections 6 and 7 of this Act require that if a proposed statutory instrument is likely to impose significant costs on the community or a part of the community, the regulation-making authority shall, prior to making the statutory instrument, prepare a regulatory impact statement about the instrument. Additionally, the Statutory Instruments Act sets out certain key elements that must be contained in the RIA. These include:

(a) a statement of the objectives of the proposed legislation and the reasons;
(b) a statement explaining the effect of the proposed legislation;
(c) a statement of other practicable means of achieving those objectives, including other regulatory as well as non-regulatory options
(d) an assessment of the costs and benefits of the proposed statutory rule and of any other practicable means of achieving the same objectives; and
(e) the reasons why the other means are not appropriate.

2.4 This Regulatory Impact Statement has been made to fulfil the requirement of section 6 of the Statutory Instruments Act, 2013.

3. THE REGULATIONS

3.1 The Act delegates rule making powers to both the Cabinet Secretary and the Data Commissioner. Pursuant to the Act, the following three draft statutory instrument have been made, namely:

(a) The Data Protection (General) Regulations 2021,

(b) The Data Protection (Registration of Data Controllers and Processors) Regulations, 2021; and

(c) The Data Protection (Compliance and Enforcement) Regulations 2021.

3.2 The draft Data Protection (General) Regulations 2020 and the Data Protection (Compliance and Enforcement) Regulations 2021 contain regulatory matters than do not impose any significant cost on the community or a part of the community and fall under the matters where regulatory impact statements may be unnecessary outlined under section 9 of the Statutory Instrument Act.

3.3 However, the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 that seeks to provide a framework for the registration of Data Controllers and Data Processors is likely to result in the imposition of a significant cost on the private and the public sector as contemplated under section 6 of the Statutory Instrument Act.

3.4 An impact assessment has been made specifically on this proposed instrument.

4. PURPOSE, OBJECTS AND OVERVIEW OF PROPOSED REGULATIONS

4.1 The draft Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 seek to provide a framework through which the registration processes will be carried out as required by the Data Protection Act.

4.2 Section 18 (2) of the Data Protection Act requires the Data Commissioner to prescribe thresholds for mandatory registration of the data controllers and data processors. This provides the rule making authority for the Data Commissioner to make these regulations.

4.3 By way of an overview, the draft Regulations provides for the procedure for registration of data controllers and data processors in compliance with section 18 of the Data Protection Act. Further, they provide the modality for the determination of data controllers and data processors required to register, the manner for lodging the application for registration, verification, renewal and cancellation of the registration by the Office of the Data Commissioner.

4.4 In addition, the Regulations provide for the fees chargeable by the Office of the Data Commissioner in executing the registration of the data controller and data processor and further make certain exemption of names sectors from mandatory registration. The Regulations require the maintaining of a register of registered data controllers and data processors.

4.5 Lastly, the draft regulations provide for the processes of applying for a certified copy of the registration certificate as well as the replacement of a lost certificate of registration. Various offences for failure of compliance with the various provisions are outlined.

5. CONSULTATIONS ON THE DRAFT INSTRUMENT.

5.1 Public consultation is required as a constitutional prerogative in making any statutory instrument. It avails all the interested or affected parties with an opportunity to present their views. This because the regulations ought to be developed in an open and transparent fashion, with appropriate procedures for effective and timely input from interested parties such as affected businesses, interest groups and other government ministries, departments and agencies.

5.2 With regard to the subsidiary legislation making process, the Statutory Instruments Act requires that the regulatory making authority shall make consultations before making statutory instruments (Regulations), and in particular, where the proposed regulations are likely to have a direct or a substantial indirect effect on business or restrict competition.

5.3 The Statutory Instrument Act further provides that in determining whether any consultation that was undertaken is appropriate, the regulation making authority shall have regard to all relevant matters, including the extent to which the consultation: drew on the knowledge of persons having expertise in fields relevant to the proposed statutory instrument; and ensured that persons likely to be affected by the proposed statutory instrument had an adequate opportunity to comment on its proposed content.

5.4 The persons to be consulted are alerted of the draft instrument either directly or by advertisement and invited to make submissions by a specified date, or be invited to participate in public hearings concerning the proposed instrument.

5.5 In line with section 5 of the Statutory Instruments Act, the Taskforce that generated the draft Regulation identified and engaged key stakeholders and members of the public for consultations. These stakeholders included professional and specialist institutions and the general public who were directly or indirectly likely to be affected by the proposed statutory instruments.

5.6 Some of the institutions consulted include Telecommunication Companies, Mobile Lending Applications, Schools and Hospitals, Civil registration entities, Insurance and Pension Management Companies, Financial Sector Players, Statutory Regulators, ICT professional, and data protection enthusiasts.

5.7 Taking into consideration the prevailing COVID-19 global pandemic, and the attendant health protocols, the following methodology was adopted for public consultations:

(a) A draft of the Regulation was published on the Ministry's website;

(b) A call for comment was published in newspapers of national circulation inviting submissions and the same was circulated through social media platforms;

(c) Direct letters and emails were written to select stakeholders inviting them to make their submissions on the draft Regulation within the outlined period;

(d) A supplement of advertisement extending the period for making submission was made and the same was circulated through other electronic media and social platforms;

(e) Extensive virtual/online meetings were held with select stakeholders and members of the public.

5.8 In this regard therefore, it is summed that the proposed Regulation has been exposed through an extensive public participation program and attains the public participation threshold as required by the Statutory Instrument Act. Annexed to this Statement is a detail public participation report including an analysis of the comments received.

6. IMPACT STATEMENT

6.1. The impact assessment considers the likely impact of the draft regulations including the general positive or negative externalities, impact on the fundamental rights of the people, the impact on the economy and the public sector, economic impact on individuals and environmental considerations. The summary of the key findings is as follows:

6.2. Impact on Fundamental Rights and Freedoms, Environment and administrative actions

(a) The draft Regulation is not expected to have a negative impact on fundamental rights of persons or institutions that are subject to it. The Regulations seeks to ensure actualization of the Bill of Rights, particularly on the right to privacy under Article 31 of the Constitution.

(b) The draft Regulation is not expected to have any possible negative impact on the environment or environmental rights of the people.

(c) The draft Regulation does not contain any provisions that are likely to impair or prejudice the right to any fair administrative action of an individual.

6.3. Economic Impact on the Private Sector

(a) The Regulation imposes additional costs on the private sector by requiring registration and the renew fees in registering as data controllers or data processors. The fees payable in this account are set out under the schedule to the draft regulation.

(b) However, despite these additional costs, it is expected the registration of data controllers and data processors would motivate the legal compliance of all entities that are processing personal data. This will consequently enhance the business management aspect of processing personal data by behooving a better management and storage of personal data, leading to better business practices.

(c) The requirement to register, which attracts this cost, would equally enhance customer security given that all persons processing personal data would register. As such, the requirement to display the registration certificate will instill faith in data subjects. This would ensure personal data of citizens is handled in accordance with the Law.

6.4. Impact on the Public Sector

(a) The Regulation imposes additional costs on the public sector by requiring entities within the public sector to register either as data controllers or data processors and this registration and the renew of registration attracts fees set out under the schedule. These costs are additional compliance costs that would be borne by the public sector.

(b) However, the anticipated benefic for the public sector gains is assurance to the general public and business community that the public sector entities have committed to handling personal data of data subjects in compliance with the Data Protection Act specifically in adherence to the principles of data protection.

(c) A positive externality will flow from this imposition to extent that it would directly create demand for more business, hence contributing to the growth of the gross domestic product (GDP). Additionally, simplified provisions of registration reduce the compliance costs.

7. OPTIONS TO REGULATIONS

7.1. This Part considers the question whether the proposed regulation is the best form of government action. The Statutory Instruments Act requires a regulator to carry out, early in the regulatory process, an informed comparison of a variety of regulatory and non-regulatory policy measures, considering relevant issues such as costs, benefits, distributional effects and administrative requirements. Thus, the regulation should be the last resort in realizing policy objectives.

7.2. Certainly, there are alternatives to these regulations. For the draft regulation is not the only means of realizing policy objectives intended in overseeing the conduct of data controllers and data processors. There alternatives that could come in handy in dealing with certain aspects of personal data protection that were considered include:

(a) Policy guidelines: In this option, the Government ensures that policies decided are communicated to the persons to apply them and ensure they are adhered to without making any regulations.

(b) Self-regulation: This is where the industry regulates itself with minimal role of Government and norms from a regulator. Various actors in the sector set the standards and the need for prescriptive legislation is lessened.

(c) Co-regulation: In this option, the Government deals with some aspects of regulating a sector while other aspects are left to be handled by players in the industry, in this case the actors in the data protection ecosystem;

(d) Procedural guidance notes: These is where guidance is issued by a government regulator to guide those tasked with making decision in the data protection ecosystem, such as those who license data processors to consider certain factors in granting or refusing permit. The need for bespoke regulation is dispensed.

8. EVALUATING THE OPTIONS

8.1 This part of the impact assessment involved evaluating the costs and benefits on implementing the regulations based on the policy options outlined above.

8.2 Generally, a policy change is a Pareto improvement if upon implementing the requirement on the registration of data controllers or data processors, they are better off and no one is worse off after the policy change. It is noted from general practice that some policy changes benefit some at the cost of others. However, an exchange could have those who benefit compensates those who suffer, and thus make everyone better off.

8.3 Secondly, a policy change is a potential Pareto improvement if an exchange could be made among data controllers or data processors that would make it a Pareto improvement, even if that exchange never occurs.

8.4 In view of this context, a policy change is considered desirable if it is a real or potential Pareto improvement. This is determined by accumulating the direct and indirect benefits and the attendant costs.

8.5 Based on this philosophical modeling, the four policy options present strengths and weaknesses on their application towards implementation of the Act on the aspects under consideration in the draft regulation.

8.6 One, issuing policy guidelines without binding regulations would certainly occasion a suboptimal result because of limited options for enforcement.

8.7 Second, the Self-regulation option would require a body that would set standards for the persons processing personal data. This option would still require some players in the sector might adopt certain regulations that would serve as a guide and to be employed for self-regulation and that. The Self-regulation option would work well in a mature sector, which is not the case with the data protection in Kenya.

8.8 Thirdly, the co-regulation option may not be effective since data protection is an emerging concept that needs clear guidelines in terms of regulations.

8.9 Lastly, providing procedural guidance note option is a practical option could be equally effective. However, these options put on a scale and considered, it is concluded that having prescriptive regulations to guide the registration of data controllers and data processors is the most effective option for the purpose of implementing section 18(2) of the Data Protection Act.

9. COST BENEFITS MODELLING

9.1 As an explanatory note, a data controller or data processor who commits an 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 three million shillings or to an imprisonment term not exceeding ten years, or to both

9.2 The regulations provide that the Data Commissioner make an order for the payment by a data controller or data processor, of a sum not exceeding two-thirds of the maximum fine that would otherwise have been imposed upon conviction;

9.3 From the above provisions of the Data Protection Act of 2019, the Penalties for violating a provision of the Act or attendant Regulations may be up to Kshs. 3,000,000. For purposes of this analysis, this will be the benefit associated with compliance with the Data Protection Act. Similarly, the Regulations propose payable fees for registrations calculated depending on three variables.

9.4 MODEL:

Net Benefit is derived from total Cost deducted from Benefit (**Net Benefit**= Benefit-Cost)

If Benefits outweighs Costs, it is recommended to proceed for implementation (Benefits ≥ Costs = Proceed)

9.5Table 1 illustrates Benefits and Costs attached to the registration of Data Controllers and Data Processors.

Table 1: Cost-benefit Analysis

S/N	Pay Determinants	Pay(Cost) (Kshs.)	Maximum Penalty (Benefit)	Maximum Net Benefit
	Number of Employees			
	for organization with 1-9 employees	2,000	3,000,000	2,998,000
	for organization with 10-49 employees	6,000	3,000,000	2,994,000
	or organization with 50-99 employee	10,000	3,000,000	2,990,000
	for organization with more than 99 employees	15,000	3,000,000	2,985,000
	Annual Turnover			
	if organization has less than KES 2,000,000 annual turnover	2,000	3,000,000	2,998,000
	if organization has between KES 2,000,001 and 5,000,000 annual turnover	6,000	3,000,000	2,994,000
	if organization has between KES 5,000,001-10,000,000 annual turnover	10,000	3,000,000	2,990,000

S/N	Pay Determinants	Pay(Cost) (Kshs.)	Maximum Penalty (Benefit)	Maximum Net Benefit
	if organization has between KES 10,000,001-50,000,000 annual turnover	15,000	3,000,000	2,985,000
	KES 25,000 for organization with more than KES 50,000,000 annual turnover	20,000	3,000,000	2,980,000
	Risk of Exposure			
	Personal Data intensive sectors	25,000	3,000,000	2,975,000

9.6 The analysis further indicates that small enterprises stand to gain a lot from the draft regulations. The regulations exempt data controllers and data processors with less than 10 employees and a turnover/revenue less than KES 5 Million from registration. This is expected to create a positive impact in terms of providing incentives to the small enterprises.

9.7 It is also expected that the net benefit will further increase even when data controllers and data processors are making renewal of their registrations. The cost of renewal is lower than the cost of registration. In addition, there are other numerous non-monetary benefits that registered data controllers and processors stand to gain including improving their reputation and trust with clients and funders.

9.8 It is noted that the Benefits as presented by (Maximum Penalty) which is the benefit that Data Controllers and Data Processors will realize by ensuring compliance with the Data Protection Regulations is Positive (greater than Kshs. 2,900,000 Payable Costs determined by the 3 categories). The Policy in this case, the Data Protection Registration of Data

Controllers and Data Processors Regulations will positively impact on Data Controllers or Processors directly or indirectly.

9.9 Overall, it is expected that newer industries in the data protection ecosystem will be created thus creating jobs and improving the growth of Kenyan economy. Finally, the regulations are expected to boost the international trade because trading partners are expecting countries to adopt data protection measures.

10 CONCLUSION

10.1 A conclusion is made that the proposed Regulations are necessary in the operationalization of the Data Protection Act, 2019 and is therefore the preferred option.

10.2 Although it is not capable of providing monetary cost of the other options, it is clear that the benefits and impact of developing these Regulations by far outweigh any estimated cost of its implementation. The other two options have little or no impact in addressing the problem.

10.3 It also apparent that the draft regulations are made in accordance with the Data Protection Act and there have been compliance with the provisions of the Statutory Instrument's Act in making of the draft regulation.

10.4 The proposed Data Protection (Registration of Data Controllers and Data Processors) Regulation, 2021, facilitates the implementation of the Data Protection Act, 2019 and is the most viable regulatory option.

11 RECOMMENDATION

It is recommended that the proposed Statutory Instrument, namely the draft Data Protection (Registration of Data Controllers and Data Processors) Regulation, 2021 be adopted as proposed and published.

MAY 2021

ANNEX 7

Public Notice on the Regulatory Impact Assessment

Published in My-Gov on 18th May 2021

REPUBLIC OF KENYA

MINISTY OF ICT,INNOVATION AND YOUTH AFFAIRS

OFFICE OF THE DATA PROTECTION COMMISSIONER

THE STATUTORY INSTRUMENTS ACT
(No. 23 of 2013)

NOTIFICATION OF REGULATORY IMPACT STATEMENT

PURSUANT to section 8 of the Statutory Instruments Act, 2013, the Cabinet Secretary for ICT, Innovation and Youth Affairs notifies the general public that a Regulatory Impact Statement on the proposed Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 has been prepared to assess the impact of the regulations on the community and businesses

The main objective of the proposed regulations is to facilitate the registration of data controllers and data processors pursuant to Part III of the Data Protection Act 2019 ('the Act'). Specifically, the Regulations seek to provide for –

a. **The Procedure for registration of Data Controllers and Data Processors**
b. **The Procedure for renewal of registration**
c. **The Charging of regulatory fees by the Data Commissioner**
d. **The creation of offences for breaches under the Regulations; and**
e. **The imposition of fines by the Data Commissioner.**

In line with the Gazette Notice No. 4697, dated 13th May 2021, this is to request all persons likely to be affected by the proposed Regulations to submit written memorandum to reach the undersigned within fourteen (14) days from the date of the above-mentioned Gazette Notice to the email address **dataprotectionregulations@odpc.go.ke**

The Regulatory Impact Statement and the proposed Regulations are available on **https://www.odpc.go.ke/regulatory-impact-assessment/**

JOE MUCHERU,
Cabinet Secretary for ICT, Innovation and Youth Affairs

ANNEX 8

Scheduled of Memoranda received from the call of comments

No.	Name of the Organization	Date Received	Memorandum
1.	Mack Kigada CEO Digulab Ltd. M +254 711 405 589	14th April 2021	Hi Under the threshold for mandatory registration you have omitted huge controllers of data. These are the large retailers such as Naivas, Quickmart, Carrefour etc. They operate large loyalty programs and I strongly feel they need to be included in the mandatory registration. They also do a lot of direct marketing.
2.	Daisy Nyanganyi daisyn@kabarak.ac.ke	19th April 2021	Mobile applications collect a lot of personal data and at some point it is shared with third parties (advertising agencies).In my opinion they should as well register The US for instance has the **4th Amendment** that is there to protect her citizens against government intrusion. Is there such a provision in the regulation? We have had so many issues touching on data protection that we seem not to win in the war on cyber security and privacy. This is so because most of the legal representatives lack the knowledge to argue such cases in court. How is the commission going to ensure that this is well taken care of because there is a very big gap? Thank you. Regards Registration of data controllers Mobile applications collect a lot of personal data and at some point it is shared with third parties (advertising agencies).In my opinion they should as well register The US for instance has the 10th Amendment that is there to protect her citizens against government intrusion. Is there such a provision in the regulation? We have had so many issues touching on data protection that we seem not to win in the war on cyber security and privacy. This is so because most of the legal representatives lack the knowledge to argue such cases in court. How is the commission going to ensure that this is well taken care of because there is a very big gap? Thank you.

3.	Doris Matu.	19th April 2021	In view of the call for public participation of the recently published regulations, I have a question for your consideration: In Regulation 50(1)(a), the General Regulations state that the Data Commissioner may compound an offence under sections 58(8) and 74 of the Act. However, section 58(8) does not exist and section 74 speaks about the Commissioner providing Guidelines, Codes etc. Is this an error in the Act? Thank you!
4.	Mack CEO Digulab Ltd. Data Privacy Practitioner M +254 711 405 589 mack@digulab.com	19th April 2021	I am suggesting that the ***ODPC Data Protection Impact Assessment document*** found here https://www.odpc.go.ke/documents/ it should be converted to a fillable PDF document. Currently it is impossible to edit those fields. One is left to recreate the document when it could easily be a fillable PDF. Kindly take that into consideration.
5.	Pathways International Limited Gideon Aswani Managing Partner & Africa CEO Mobile: +254 722 721 519 Office: +254 771 616 839 Email: gaswani@pathwaysinternational.com	26th April 2021	Memorandum.
6.	British American Tobacco Doris Otiato Corporate Governance & Compliance Counsel British American Tobacco Kenya plc. Direct Line: +254 711 062504 Switchboard: +254 711 062000	26th April 2021	Memorandum
7.	Competition Authority of Kenya Ninette K. Mwarania Manager, Planning, Policy & Research, Competition Authority of Kenya, Nairobi, Kenya.	26th April 2021	Memorandum

	Pilot Line: +254 202628233 Direct Line: +254 202779114		
8.	Chrispine Bosire Associate Commercial Department Simba & Simba Advocates	26th April 2021.	Memorandum
9.	Vivian Onyino, Advisor, Legal & Regulatory: Rest of Africa Regions. Trans-union	26th April 2021	Memorandum.
10.	Samantha Oswago | Legal Officer East African Centre for Human Rights (EACHRights) Kilimani Area| Timau Road| Cedar Court| House No. 4| P.O Box 19494-00100 WEBSITE: www.eachrights.or.ke| EMAIL: info@eachrights.or.ke TWITTER: @EACHRights| FACEBOOK: EACHRights| OFFICE:+254701670090 EMAIL: Samantha @eachrights.or.ke | SKYPE: Samantha. O	26th April 2021	Memorandum
11.	Benard Sompoika PA TO THE COMMISSION SECRETARY/CEO NATIONAL GENDER AND EQUALITY COMMISSION	27th April 2021.	Memorandum
12.	James Mbugua Njenga Group Data Protection Officer Direct Line: +254 (20) 322 2402 | Board: +254 (20) 322 1000 I&M Bank Tower | 6th Floor | Kenyatta Avenue P. O. Box 30238 – 00100 | Nairobi | Kenya	27Tth April 2021	Memorandum – 3
13.	Cyber-Security Technologies & Research Systems.	27th April 2021	Memorandum
14.	Shikuku	27th April 2021	Dear all.

			My comments on the Data Protection Act 2019 are as follows: Clause 24(3) of the Data protection act 2019 allows a group of entities to appoint a single data protection officer provided that such officer is accessible by each entity. However Clause 24(5) on designation or appointment of data protection officer does not specify whether the data protection officer must be located in Kenya. it is not clear whether data controllers or data processors operating in Kenya can appoint a data protection officer located in a foreign country or appoint a foreign(non kenyan) data protection officer provided that he/she is accessible to each entity. Regards Shikuku
15.	Central Bank of Kenya	27th April 2021	Memorandum
16.	Multi-choice Kenya Mwendwa Maundu General Manager: Regulatory - East Africa MGH – Northern Region 1st Floor, 90 JGO, James Gichuru Road, NAIROBI Telephone:+254(0)709980113 |Mobile: +254 (0)722977893 Email: Mwendwa.Maundu@ke.multichoice.com	27th April, 2021	Memorandum
17.	COULSON HARNEY LLP 5th Floor, West Wing, ICEA Lion Centre Riverside Park, Chiromo Road, Nairobi PO Box 10643-00100, Nairobi, Kenya www.bowmanslaw.com	27th April 2021	Memorandum
18.	Elsy Sainna Ag. Executive Director The Kenyan Section of the International Commission of Jurists ICJ Kenya House, Off Silanga Road, Karen P.O. Box 59743-00200, Nairobi, Kenya Tel: +254-20-2084836/8 | +254 720 491549	27th April 2021	Memorandum
19.	UAP Old Mutual Insurance. CYNTHIA KAGIRI	27th April 2021	Memorandum

	LEGAL ADVISOR | LEGAL & COMPANY SECRETARIAT T. +254 (0)711 065 674 6th Floor, UAP Old Mutual Tower, Upper Hill Road, Nairobi ckagiri@uapoldmutual.com I www.uapoldmutual.com		
20.	Moses Otsieno Cyber Policy Centre	27th April 2021	Memorandum
21 .	Tamara Cook FSD Kenya	27th April 2021	Memorandum
22.	Sophie Kaibiria Senior Programme Officer, Women, and Governance Federation of Women Lawyers(FIDA-Kenya) Amboseli Road,Off Gitanga Road P.O Box 46324-00100,NAIROBI, Tel: 0722509760/0710607241 Email: sophie @fidakenya.org	27th April 2021	Memorandum
23.	Dismas Ong'ondi, MSc Cybersecurity (Warwick), CISPP, CISM, CISA)	27th April 2021	Memorandum
24.	Inline image Nixon Mageka about.me/mageka	27th April 2021	Dear madam, Firstly congratulations on your appointment and facilitating the data protection regulation. I am worried of all private information in the hands of private companies like safaricom, Airtel and Telkom Kenya. They know where we go every night, who we send money to and good night messages. Right to privacy is a constitutional right and cannot be waived by what this companies referred as Terms and Conditions signed by users. That is not true at all. Not all contracts are enforceable especially when they are against public rights and morality. The issue of consent, informed and prior is not clear How would we enforce this on the regulations?

25	Esther Kung'u AIG Legal Counsel AIG Kenya Insurance Company Limited Eden Square,Chiromo Road P.O Box 49460-00100 Nairobi, Kenya T +254 (0)20 3676000 | M +254 (0)713 812051 Esther.Kungu@aig.com | www.aig.com/ke	27th April 2021	Memorandum
26.	Kenya Bankers Association Kennedy Mutisya Chief Finance Officer|Kenya Bankers Association International House, 13th Floor|Mama Ngina Street, Nairobi Phone: +254-20-2221704/2224014| Mobile:+254 733 601549 Email: kmutisya@kba.co.ke	27th April 2021	Memoranda
27.	monicaengola@gmail.com Monica Engola	27th April 2021	Dear Sir/Madam, What qualifies as transfering personal data outside Kenya? Kindly explain in detail so that the issue of transfer is clear. Kind regards, Monica Dear Sir/Madam, I trust this email finds you well.

			I have reviewed the draft general regulations and note that there is no timeframe prescribed within which a data controller or data processor should comply with a data subject access request under regulation 8. Kindly confirm if my observation is correct or advise on what timeline is applicable.
28.	Josiah.Munene Josiah.Munene@absa.africa	27th April 2021	Hi, Questions as below; 1) Any date when Kenya is expected to ratify the African Union Convention on Cyber Security and Personal Data. Meanwhile will this hamper operations when regulations are in force? 2) Will the ODPC issue a list of permitted countries where Data Controllers and Data Processors can transfer and process data 3) How will the ODPC collaborate with other regulators who also provide approvals on hosting and security of data to have timeous decisions. e.g. CBK - prudential consent. 4) Any guidance on how DCs and DPs should handle data subjects acquired before the Act came into force when it comes to obtaining consent? 5) Will there be localization requirements for private entities?
29.	Kaplan&Stratton Hope Miring'u | Associate Williamson House, 4th Ngong Avenue P.O. Box 40111 – 00100, Nairobi, Kenya tel +254 20 2841000 www.kaplanstratton.com	27th April 2021	Memorandum
30.	Jamii Telecommunications Limited	27th April 2021	Memorandum
31.	Chrispin Bosire. ADVOCATE OF THE HIGH COURT OF KENYA. LL. B (Hons) Moi University; P.GD (Law) - Kenya School of Law; Certified Professional Mediator – Mediation Institute (A); Alumnus – Young African Leaders Initiative (YALI) - East Africa.	28th April 2021	Memorandum

32.	Britam Jackson, Kiboi Head of Legal | Life Legal | Head Office	29th April 2021	Memorandum
33.	Keziah Kinuthia Data Scientist Nation Media Group	29th April 2021	*What is a data breach under the DPA?* *2. What are the penalties for not complying with the DPA?* *3. What lawful bases for processing should we use, and do we always need consent?* *4. Do organizations need to register under the DPA?* *5. What is the difference between personal data and sensitive data under the DPA?* *6. In the 100 days, have the office of the data Protection Commissioner (ODPC) received any complaints regarding data privacy infringement? Have there been any fines levied?* *7. Have you identified notorious companies/ institutions highly likely to infringe Kenyan's data privacy rights?* *8. How many technical experts have you hired to investigate shady practices of data trackers?* *9. What's your strategy in monitoring compliance?* *10. What strategy have you put in place to ensure Kenyans are aware of their data privacy rights?* *11. Can Kenyans tell the information companies hold about them?* *12. How many data controllers and processors registered so far?* *13. What challenges have you faced so far?*
34.	Prof. Stephen Kimani ICT Director Jomo Kenyatta University of Agriculture and Technology (JKUAT) PO Box 62000 00200 Nairobi Kenya	29th April 2021	Thank you very much for the great work in order to improve regulation of data. After going through the Data Protection Act 2019, and the sets of the Draft Data Protection Regulations, I for now have three comments: 1. According to PART IV 25 of the Data Protection Act 2019, every data controller or data processor shall ensure that personal data is (among other things) "(h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject" This does not seem to align well with PART VI 48 of the same Act. In the current form of the Act, there appear to be mismatches such as the following: From PART IV

			25 (h) one can interpret that satisfying either "consent from the data subject" or "proof of adequate data protection safeguards" is enough (in order to transfer personal data out of Kenya). On the other hand, PART VI 48 does not mention obtaining consent from the data subject as one of the conditions for transfer of personal data outside Kenya. Part VII of the Draft Data Protection (General) Regulations 2021 still does not give clarity to the foregoing transfer matters. The Draft Data Protection (General) Regulations 2021 could be revised so as to give clarity and guidance on the foregoing matters. 2. The Draft Data Protection (General) Regulations 2021 could be revised in order to make it more explicit what transfer of data outside Kenya really entails. For instance: it is important to know if the transfer restricts: i) Emailing/e-submission of applications for funding (e.g. grant proposals, etc) outside the country. ii) Publishing of books outside the country. iii) Emailing/e-submission of conference papers and journal articles, where the conferences and journals are based outside Kenya. iv) Publishing of research work, where the conferences and journals are based outside Kenya. 3. Part III 13 (c) of the Draft Data Protection (General) Regulations 2021 should probably not limit itself to only "electronic message". It could refer to (or include) any medium. Office of the Data Protection Commissioner, Thank you for the awesome work that you are doing. I have the following one more comment: PART VI 48 of the Data Protection Act 2019 has three items, namely a), b) and c). From the articulation, it is not clear if it is a requirement to satisfy all the three items, or if satisfying any one of them is sufficient. The Draft Data Protection (General) Regulations 2021 could be revised to give clarity to this matter. Office of the Data Protection Commissioner,

			Thank you for the good work Here are two comments: 1. In the SECOND SCHEDULE (a) Registration and Renewal Fee Stage 2 does not cover organizations with annual turnover of exactly KES 2,000,000. Only for those with "less than KES 2,000,000" and KES 2,000,0001 upwards (Page 15). 2. If necessary, how would ODPC verify the annual turnover of the applying organization (since the establishment documents might not have the information)? Otherwise the ODPC would have to rely on other sources e.g. audit and background checks. Regards. Stephen Kimani
35.	Ombo Malumbe, Partner Ong'anya Ombo Advocates Windsor House, 4th Floor, Muindi Mbingu Street/ University Way P O. Box 15598 - 00400 Nairobi, Kenya. m: +254 724 026 355 w: https://onganyaombo.com	3rd May 2021	Memorandum
36.	Annabel Monthe Muema	3rd May 2021	On the same on the standard qualifications of data protection officers, I would suggest a cross cutting sensitization and training through ODPC of these officers. On Thursday, April 29, 2021, novelty ventures < venturesnovelty@gmail.com > wrote: In regards to hiring data protection officers by data processors or controllers, is there a particular guideline of skills and certification that this regulation can provide on the same? On Thursday, April 29, 2021, novelty ventures <

			venturesnovelty@gmail.com > wrote: Dear ODPC, Thank you for the opportunity and aApologies that I wasn't unmuted to get this question. Under the data protection (registration of data controllers and data processors) regulations,2021 Does this regulation make a provision for institutional sharing of data? If yes,is there a structure to get these institutions organized to facilitate accountability in the case that personal data of a data subject is breached? Thank you once more. Best regards, Annabel Monthe On Tuesday, April 27, 2021, novelty ventures < venturesnovelty@gmail.com > wrote: In line with GDPR laws and cloud storage,to ensure security by the data controllers stipulates that personal data stored on the cloud is encrypted so if there is a breach,the information will be useless to those who may have stolen or acquired.This can be added In the regulations In part 4, section 23 d Security measures subjecting the data processor to the same requirements as the data controller in relation to keeping personal data secure, encryption should also be part of this so that it cyber criminals breach cloud systems..the information can become useless. On Tuesday, April 27, 2021, novelty ventures <

			venturesnovelty@gmail.com > wrote: A question in regards to the option of opting out.There are organizations which give wrong steps intentionally to opt out from subscriptions but in real sense it is not an opt out procedure but an activation code.What consequences are there for such persons who give the public misleading information in regards to opt out steps? On Monday, April 26, 2021, novelty ventures < venturesnovelty@gmail.com > wrote: Dear ODPC, Kindly find below suggestions towards the data protection (General) regulations,2021 arrangement of regulations. Part II (4) A data subject may prior to the processing of their personal data give consent either orally or in writing, and may include a handwritten signature, an oral statement, or use of an electronic or other medium to signify agreement. Suggestions: 1.Provided the data subject has not been forced to give their information where it poses no security harm or information required for intelligence purposes. 2.The electronic signature processing is secured from Cyber criminals. Example of cyber criminal offences of stealing electronic signatures through text message prompts. A text message received on 6th April 2021 from SMS code 836 Do you like your friend's signature? Reply '1' to copy your friend's signature, dial *836*1# for more info. Reply stop to stop receiving these messages.

			5.2.) 2) Subject to section 28 (2) of the Act, a data controller or data processor shall have regard to the following during data collection— (a) collect personal data which it is permitted to collect by the data subject (b) undertake steps to ensure the quality of personal data; (c) undertake processes to secure personal data; and (d) subject to section 45 (b) of the Act, only collect sensitive personal data directly from a data subject. Suggestion: a) collect personal data which it is permitted to collect by the data subject provided the data being processed is in accordance to the regular or normal standards of the processing agency. Example: If the standard of an institution only requires a national Identification number and no other additional informational,that to be adhered to strictly and the data subject to be made aware /sensitized what information they are required to give so that they don't end up giving additional information to the wrong people. What is happening is cyber criminals are hidding under Institutions to Syphon additional information,a data subject may not be aware that they are giving additional information than what is required.
37.	John Benard Owegi National Coordinator CSRG Secretariat P.O. Box 37485 – 00100, Nairobi, Kenya Ufungamano House, Room 10-11, Mamlaka Road, off Statehouse Road, Nairobi, Website: www.civilsocietyrg.org Email: jowegi@civilsocietyrg.org ; info@civilsocietyrg.org	3rd May 2021	Memorandum

	Cell: +254728 303 864/782 924 775 Office Line: +254 772 342 310		
38.	Annabel Monthe venturesnovelty@gmail.com	5th May 2021	Kindly find below suggestions towards the data protection (General) regulations,2021 arrangement of regulations. Part II (4) A data subject may prior to the processing of their personal data give consent either orally or in writing, and may include a handwritten signature, an oral statement, or use of an electronic or other medium to signify agreement. Suggestions: 1.Provided the data subject has not been forced to give their information where it poses no security harm or information required for intelligence purposes. 2.The electronic signature processing is secured from Cyber criminals. Example of cyber criminal offences of stealing electronic signatures through text message prompts. A text message received on 6th April 2021 from SMS code 836 Do you like your friend's signature? Reply '1' to copy your friend's signature, dial *836*1# for more info. Reply stop to stop receiving these messages. 5.2.) 2) Subject to section 28 (2) of the Act, a data controller or data processor shall have regard to the following during data collection— (a) collect personal data which it is permitted to collect by the data subject (b) undertake steps to ensure the quality of personal data; (c) undertake processes to secure personal data; and (d) subject to section 45 (b) of the Act, only collect sensitive personal data directly from a data subject. Suggestion: a) collect personal data which it is permitted to collect by the data subject provided the data being processed is in accordance to the regular or normal standards of the processing agency.

			Example: If the standard of an institution only requires a national Identification number and no other additional informational, that to be adhered to strictly and the data subject to be made aware /sensitized what information they are required to give so that they don't end up giving additional information to the wrong people. What is happening is cyber criminals are hidding under Institutions to Syphon additional information, a data subject may not be aware that they are giving additional information than what is required. A question in regards to the option of opting out. There are organizations which give wrong steps intentionally to opt out from subscriptions but in real sense it is not an opt out procedure but an activation code. What consequences are there for such persons who give the public misleading information in regards to opt out steps? In line with GDPR laws and cloud storage,to ensure security by the data controllers stipulates that personal data stored on the cloud is encrypted so if there is a breach,the information will be useless to those who may have stolen or acquired.This can be added In the regulations In part 4, section 23 d Security measures subjecting the data processor to the same requirements as the data controller in relation to keeping personal data secure, encryption should also be part of this so that it cyber criminals breach cloud systems..the information can become useless Thank you for the opportunity and aApologies that I wasn't unmuted to get this question. Under the data protection (registration of data controllers and data processors) regulations,2021 Does this regulation make a provision for institutional sharing of data? If yes,is there a structure to get these institutions organized to facilitate accountability in the case that personal data of a data subject is breached?

			Thank you once more. In regards to hiring data protection officers by data processors or controllers,is there a particular guideline of skills and certification that this regulation can provide on the same? On the same on the standard qualifications of data protection officers, I would suggest a cross cutting sensitization and training through ODPC of these officers. Another gap in form of criminal activity that has been happening in regards to handling of the forms by data protection officers would be to safe guard the forms entrusted to the data processors and controllers that are hand written by the data subjects. Criminals are accessing these forms to implicate innocent Kenyans to illegal activities through forensics like accessing their finger prints and not only just their data.
39.	Peter Kimpian Data Protection Unit Human Rights and Rule of Law CONSEIL DE L'EUROPE - COUNCIL OF EUROPE tel : + 33(0) 3 90 21 58 51	6th May 2021	Comments on the Regulations/ Memorandum.
40.	Leah Muchiri Senior Associate J.K. Kibicho & Co. Advocates ACK Garden House 1st Ngong Avenue P.O. Box 73137 - 00200 Nairobi, Kenya Tel: 020-2737100 / 2712929 Cell: 0717297146	6th May 2021	Memorandum on the 3 sets of regulations.
41.	Paul Mombo	7th May 2021	Comments

	paulmombo@gmail.com		
42.	Thuku wa Thuku Kenya Country Manager Smile Identity Inc Kenya	10th May 2021	Memorandum
43.	KE. Digital LLP P.O. Box 64717 00620 Nairobi +254 742 012 599 +49 171 282 0526 Kenya	10th May 2021	Comments-
44.	State Department of Vocational & Technical Training.	10th May 2021	Memorandum
45.	Mutie Advocates Anne M Mutie Partner	10th May 2021	Memorandum
46.	Amazon Web Services Narrimane Benakcha Data Policy and Regulated Industries, Middle East & Africa narriman@amazon.ae Mobile: +971 52 776 1159	10th May 2021	Memorandum
47.	Centre for Intellectual Property & Information Technology Law Direct Line: +254 (0) 703 034 612 Ext: 2612 Enquiries: +254 (0) 703-034000/200/300 OR +254 (0) 730-734000/200/300	10th May 2021	Memorandum
48.	Dr.Amritpal Kalsi	10th May 2021	Memorandum
49.	Florence Kwamboka Independent Electoral and Boundaries Commission Tel 0722841900	11th May 2021	Memorandum
50	ATC Kenya	11th May 2021	Memorandum
51.	International Committee of the Red Cross.	11th May 2021	Memorandum

	Hillary Muchiri Kiboro Legal Officer Denis Pritt Road, P.O Box 73226-00200, NAIROBI T: +254 20 2723963: Mobile : +254 706 110 126		
52.	Victor Lee Legal	11th May 2021	Memorandum
53.	Microsoft Corporation Serge Ntamack Corporate, External and Legal Affairs Mobile: +237 695 95 54 75 Office: +237 233 42 71 89	11th May 2021	Memorandum
54.	Sendy Mercy Mwaniki Senior Legal Associate M: +254 721 532 400	11th May 2021	Memorandum
55.	American Chamber Of Commerce, Kenya Maxwell Okello Maxwell@amcham.co.ke Chief Executive Officer +254 733 787 416 +254 709 207 000 The Address, 10th Floor Muthangari Drive, off Waiyaki Way P. O. Box 26390 – 00603 Nairobi, Kenya	11th May 2021	Memorandum
56.	U.S. Embassy Nairobi, Kenya Diane Jones Commercial Counselor +254 705154592 Diane.Jones@trade.gov	11th May 2021	Memorandum
57.	Evans Kibet evanskibet@yandex.com		Comments
58.	KICTANet portals Grace Githaiga		Memorandum

	KICTANet Convenor		
59.	Secunets Technologies Ltd Grace Ngugi *(Technical support)*		Memorandum
60.	Katiba Institute Ray Odanga		Memorandum
61.	Lawyers Hub Ms. Catherine Muya| Tech Policy Fellow *Tech for Justice* ACK Garden House| Block D, 6th Floor |Upper Hill, Nairobi| Kenya Email: catherine.muya@lawyershub.ke		Memorandum
62.	Nyasani obiko and company advocates Rachel Nyasani.		Memorandum
63.	Airtel Telecommunications Limited Joan Mburu		Memorandum
64.	KO. Associates LLP		Memorandum
65.	GSMA Caroline Mbugua, HSC. | Senior Policy Manager, Sub-Saharan Africa |		Memorandum
66.	U.S. Embassy Nairobi Adrian J. Amen Economic Officer		Memorandum
67.	ECM CONSULTING GROUP LLP, CPA(K) Enock Nyanchoga Monari CPA		Memorandum
68.	Women in Cyber Security (WiCyS) East Africa Aprielle Oichoe President - WiCyS East Africa affiliate		Memorandum
69.	ISACA Kenya Chapter Veronica N. Rose, CISA, CDPSE Director - Advocacy		Memorandum

70.	Lanet Consulting Group Limited **Evans Ikua,** Cell: +254-722-955831		Memorandum
71	ARTICLE 19 Eastern Africa Sigi Waigumo Mwanzia, Programme Officer - Digital.		Memorandum
72	Wananchi Telecommunications Limited Zuku Amida		Memorandum
73	Kenya National Commission on Human Rights (KNCHR). Janet Kabaya 0723-818963.		Memorandum
74	Triple OK Advocates		Memorandum
75	Principal Secretary, State Department of Interior and Citizenship Services.		Memorandum
76.	Nyauchi & Company Advocates Gragory Nyauchi, +254 736 351753		Memorandum
77	KPMG		Memorandum
78.	PricewaterhouseCoopers Limited Kenya ("**PwC**")		Memorandum
79.	IEBC		Memorandum
80	FaceBook Mercy Ndegwa, Head of Public Policy, East & Horn of Africa		Memorandum – no attachment
81.	Trust Data Privacy Consultancy.		Memorandum
82.	Safaricom		Memorandum
83.	V. A. Nyamodi & Co. Advocates Bridgitte NdongHse. 7, Duplex Apartments Lowerhill Road, Upperhill		Memorandum

	P. O. Box 51431-00200 NAIROBI Tel No. + 254 20 2715542, 2715547, 0773 405 73		
84.	National Cohesion and Integration Commission Isaac Munya KMA Centre 6th Floor, Mara Rd, Upper hill P.o. Box 7055-00100 Nairobi, Kenya Tel +254 -20-2585702/3/1. Ext. 150.		Memorandum
85.	ICEA Lion Group		Memorandum
86.	Anjarwalla & Khanna LLP JADE MAKORY | Trainee Lawyer		Memorandum
87.	Kenya Revenue Authority G. Muraguri DC ICT|CSS		Memorandum
88.	Konza		Memorandum
89.	AAR Insurance Kenya (Ltd)	12th may 2021	Memorandum
90.	KEPSA		Memorandum
91.	Evotrust		
92.	Gen Africa		Memorandum
93.	Council of Governors		Memorandum
94.	Capital Markets Authority		Memorandum
95.	Department of Defence		Memorandum
96.	Kenya Association of Manufactures		Memorandum
97.	KN Law LLP		Memorandum

ANNEX 9

WEEK ONE (1): MONDAY 19TH TO FRIDAY 23RD APRIL 2021

TEAM A MEMBERS	ROLE
1. **Eng. Daniel Obam**	**Moderator**
2. Thuranira Gatuyu	Presenter 1
3. Sylvia Chelogoi	Presenter 2
4. Duncan Nyale	Presenter 3
5. Christopher Maina	Presenter 4

TEAM B MEMBERS	ROLE
1. **Rose Mosero**	**Moderator**
2. Marion Murithi	Presenter 1
3. Victor Nzomo	Presenter 2
4. Miriam Kakenya	Presenter 3
5. Dr. Humphrey Njogu	Presenter 4

	MORNING SESSION: (9am - 11am)	**WEBINAR LINKS - WEEK ONE (1)**
1.	**Academia** - Monday 19th April 2021	Taskforce on the Development the General regulations on Monday 19th April 2021 Hosted by Rittah Awuor https://moictke.webex.com/moictke/j.php?MTID=m86fae8d7e371773853787f7396055528 Monday, Apr 19, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 616 9285 Password: RimJpKE8X92
2.	**Civil Society** -Tuesday 20th April 2021 (9am - 11am)	Civil Society - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=mbcc475d844285c02dab30084679e55ff Tuesday, Apr 20, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 249 0966 Password: yUUPj4Zkk62
3.	**Regulators** - Wednesday 21st April 2021 (9am - 11am)	Regulators - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m30787eef7b3ad1c1a70778efa0bc963c Wednesday, Apr 21, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 988 7968 Password: 3zfX7KynuR9
4.	**Key Data Holders** - Thursday 22nd April 2021 (9am - 11am)	Key Data Holders - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru

	MORNING SESSION: (9am - 11am)	WEBINAR LINKS - WEEK ONE (1)
		https://moictke.webex.com/moictke/j.php?MTID=m99964790cfa079e0fefdd8ba5266855a Thursday, Apr 22, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 459 4508 Password: 7MxHPq7DeQ4
5.	**Private** - Friday 23rd April 2021 (9am - 11am)	Private - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=mabe507fed34178aec45839fb1e1be833 Friday, Apr 23, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 225 9560 Password: 33qmZVpV5NP

	AFTERNOON SESSION: (2pm - 4pm)	WEBINAR LINKS - WEEK ONE (1)
6.	**Lawyers Hub** - Monday 19th April 2021 (2pm - 4pm)	Lawyers Hub - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Paxton Musomba https://moictke.webex.com/moictke/j.php?MTID=m4af47f54d96e4563acd854801e9c3c9a Monday, Apr 19, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 576 9904 Password: n65Mwt3kFEM
7.	**Civil Society** - Tuesday 20th April 2021 (2pm - 4pm)	Civil Society - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Rittah Awuor https://moictke.webex.com/moictke/j.php?MTID=m295ce2a1d971a31ba5a151bea44e85cd Tuesday, Apr 20, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 022 2122 Password: xsEsRjuP233
8.	**Regulators** - Wednesday 21st April 2021 (2pm - 4pm)	Regulators - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Rittah Awuor https://moictke.webex.com/moictke/j.php?MTID=m93f3b3209a168b6431389f6971146752 Wednesday, Apr 21, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi

	AFTERNOON SESSION: (2pm - 4pm)	WEBINAR LINKS - WEEK ONE (1)
		Meeting number: 183 290 3688 Password: yD3sTa5gHp2
9.	**Key Data Holders -** Thursday 22nd April 2021 (2pm - 4pm)	Key Data Holders - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m02babd99b4a13d8c477b5e413edff93c Thursday, Apr 22, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 038 4446 Password: yiPETHd4c26
10.	**Private Sector Representative -** Friday 23rd April 2021 (2pm - 4pm)	Private Sector Representative - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m22cb6641a5b6ad69f7c1906c765d5d51 Friday, Apr 23, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 922 3032 Password: 3D8UmVAU4yP

MORNING SESSION (9am - 11am)				
Monday 19th April 2021 (9am - 11am)	**Tuesday 20th April 2021 (9am - 11am)**	**Wednesday 21st April 2021 (9am - 11am)**	**Thursday 22nd April 2021 (9am - 11am)**	**Friday 23rd April 2021 (9am - 11am)**
Academia Team A	**Civil Society** Team B	**Regulators** Team A	**Key Data Holders** Team B	**Private** Team A
1. The University of Nairobi 2. Strathmore University 3. Dedan Kimathi University 4. Jomo Kenyatta University of Agriculture and Technology	1. Kenya ICT Action Network (KICTAnet) 2. FIDA 3. Child Welfare Society of Kenya 4. International Commission of Jurists (Kenya)	1. Kenya Revenue Authority 2. Insurance Regulatory Authority 3. National Construction Authority 4. Kenya Ports Authority 5. Kenya Maritime Authority	1. Safaricom 2. Airtel 3. Telkom 4. Jamii Telecom	1. Kenya Private Sector Alliance (KEPSA) 2. Protective & Safety Association of Kenya (PROSAK) 3. American Chamber of Commerce (AMCHAM)

5. MultiMedia University 6. Kenya School of Government 7. Kenya School of Law 8. Artificial Intelligence Center of Excellence	5. Kenya Human Rights Commission 6. AMNESTY International 7. Article 19 EAST Africa	6. Kenya Civil Aviation Authority 7. Kenya Bureau of Standards 8. National Transport Safety Association 9. Communications Authority of Kenya (CA) 10. Kenya National Bureau of Statistics 11. Central Bank of Kenya 12. Sacco Societies Regulatory Authority 13. Capital Markets Authority		
AFTERNOON SESSION (2pm - 4pm)				
Monday 19th April 2021 (2pm - 4pm)	**Tuesday 20th April 2021 (2pm - 4pm)**	**Wednesday 21st April 2021 (2pm - 4pm)**	**Thursday 22nd April 2021 (2pm - 4pm)**	**Friday 23rd April 2021 (2pm - 4pm)**
Lawyers Hub Team B	**Civil Society** Team A	**Regulators** Team B	**Key Data Holders** Team A	**Private Sector Representative** Team B
	1. Freedom House 2. Amnesty International – Kenyan & Regional Office 3. Open Institute 4. Artificial Intelligence Center of Excellence 5. National Coalition for Human Right Defenders 6. Supreme Council Of Kenya Muslims 7. The National Council of Churches of Kenya	1. State Department for Social Protection, Department of Children Services. 2. National Population Council 3. Kenya National Archives and Documentation Services 4. National Council for Persons with Disability 5. Kenya Power and Lighting Company	1. Facebook 2. Google Kenya 3. Microsoft 4. Oracle Kenya 5. Konza Technopolis 6. Liquid Telecom	1. Kenya Association of Hotel Keepers and Caterers 2. Kenya Bankers Association 3. Kenya Hospitals Association 4. Bloggers Association of Kenya 5. Kenya Association of Manufacturers 6. GSMA 7. TESPOK 8. EvoTrust LTD

WEEK TWO (2): MONDAY 26TH TO FRIDAY 30TH APRIL 2021

TEAM A MEMBERS	ROLE
1. **Eng. Daniel Obam**	**Moderator**
2. Thuranira Gatuyu	Presenter 1
3. Sylvia Chelogoi	Presenter 2
4. Duncan Nyale	Presenter 3
5. Christopher Maina	Presenter 4

TEAM B MEMBERS	ROLE
1. **Rose Mosero**	**Moderator**
2. Marion Murithi	Presenter 1
3. Victor Nzomo	Presenter 2
4. Miriam Kakenya	Presenter 3
5. Dr.Humphrey Njogu	Presenter 4

	MORNING SESSION (9am – 11am)	WEBINAR LINKS - WEEK TWO (2)
1.	**Media -** Monday 26th April 2021 (9am – 11am)	Media - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m0f87ea54c9393d83ad954f72f8191daf Monday, Apr 26, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 248 9068 Password: 4YNyBGgEY38
2.	**Professional Bodies& Associations -** Tuesday 27th April 2021 (9am – 11am)	Professional Bodies& Associations - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=mc59f78b7ce9572e8172a429b06d898dd Tuesday, Apr 27, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 984 1996 Password: MPmvNZJE365
3.	**Independent Commissions and Key State Offices -** Wednesday 28th April 2021 (9am – 11am)	Independent Commissions and Key State Offices - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m74849c637b5fcfb018eda7fd8e9022e9 Wednesday, Apr 28, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 569 0490 Password: MMj43H92WdM

4.	**Devolved Government -** Thursday 29th April 2021 (9am – 11am)	Devolved Government - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m80b2e5a2a71d34a045f2f9fc79c14cc1 Thursday, Apr 29, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 438 9702 Password: Ek6TWPFQi82
5.	**Key Government Entities -** Friday 30th April 2021 (9am – 11am)	Key Government Entities - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m9cc1ab36db7296bbfd2c94e987375213 Friday, Apr 30, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 645 5914 Password: FBpDy3bMn35

	AFTERNOON SESSION (2pm - 4pm)	**WEBINAR LINK**
6.	Monday 26th April 2021 (2pm - 4pm)	Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m18b1ac75618ff5dae984e9806afda0c8 Monday, Apr 26, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 480 2216 Password: PcA3HbBim33
7.	**Public Participation forums** - Tuesday 27th April 2021 (2pm - 4pm)	Public Participation forums - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=mbf33e81add153a4dbc8329bd08ca749f Tuesday, Apr 27, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 401 9298 Password: uZJgjr7WU75
8.	**Public Participation forums** - Wednesday 28th April 2021 (2pm - 4pm)	Public Participation forums - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=md8fe88d3d7be6e0dbe69712463efec20

		Wednesday, Apr 28, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 836 3166 Password: ndCsqh2C8T2
9.	**Public Participation forums** - Thursday 29th April 2021 (2pm - 4pm)	Public Participation forums - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m4f81670eacb3465f54149243973eda38 Thursday, Apr 29, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 227 2098 Password: JTmWJqE2Z84
10.	**Public Participation forums** - Friday 30th April 2021 (2pm - 4pm)	Public Participation forums - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=ma1679364a01893ce829d8b188658f5ca Friday, Apr 30, 2021 2:00 pm | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 994 2492 Password: y2GX25pTNkt

MORNING SESSION (9am - 11am)				
Monday 26th April 2021 (9am - 11am)	**Tuesday 27th April 2021 (9am - 11am)**	**Wednesday 28th April 2021 (9am - 11am)**	**Thursday 29th April 2021 (9am - 11am)**	**Friday 30th April 2021 (9am - 11am)**
Media Team A	**Professional Bodies& Associations** Team B	**Independent Commissions and Key State Offices** Team A	**Devolved Government** Team B	**Key Government Entities** Team A
1. Media Council of Kenya 2. Kenya Editors Guild 3. Kenya Yearbook Editorial Board 4. Kenya Film Classification Board 5. Postal Corporation of Kenya 6. Kenya Broadcasting Corporation	1. Law Society Of Kenya 2. Kenya Medical Practitioners Pharmacists and Dentistry Union (KMPDU)/ Kenya Medical Association (KMA) 3. Engineers Board of Kenya	1. Parliamentary Service Commission 2. Commission on Revenue Allocation 3. Salaries and Remuneration Commission 4. National Police Service Commission	1. County Assembly Forum 2. County Executive	1. Integrated population registration system (IPRS) 2. ICT Authority Kenya 3. The National Education Management

7. Kenya Institute of Mass Communications 8. Kenya Film Commission 9. National Youth Council 10. Kenya Copyright Board	4. Institute of Human Resource Management 5. Kenya Association of Technical Training Institutes 6. The Marketing Society of Kenya 7. Institute of Certified Secretaries of Kenya 8. Architectural Association of Kenya 9. Association of private universities in Kenya. 10. Board of Registration of Architects and Quantity Surveyors, Kenya Chartered Institute of Arbitrators 11. Chartered Institute of Management Institution of Surveyors of Kenya 12. Kenya National Association of Agricultural Professionals 13. Kenya National Association of Private Colleges 14. Kenya Engineering Technology 15. Board of Registration of Architects and Quantity Surveyors, Kenya;	5. Registrar of political parties 6. Teachers Service Commission 7. Gender Commission 8. Public Service Commission 9. Ethics and Anti-Corruption Commission 10. Kenya National Human Rights Commission 11. National Land Commission 12. Independent Electoral and Boundaries Commission		Information System (NEMIS) 4. National Integrated Identity Management System (NIIMS) 5. National Payment Systems 6. Integrated Financial Management System. 7. Integrated Personal Payroll Management System

AFTERNOON SESSION (2pm - 4pm)				
Monday 26th April 2021 (2pm - 4pm) Team B	**Tuesday 27th April 2021** (2pm - 4pm) Team A	**Wednesday 28th April 2021** (2pm - 4pm) Team B	**Thursday 29th April 2021** (2pm - 4pm) Team A	**Friday 30th April 2021** (2pm - 4pm)
1. International Committee of the Red Cross 2. World bank 3. United Nations Development Program 4. UK High Commissioner 5. European Union 6. GIZ Kenya 7. Tony Blair Institute	Public Participation forums	Public Participation forums	Public Participation forums	

WEEK THREE (3): MONDAY 3RD MAY 2021

TEAM A MEMBERS	ROLE
1. **Eng. Daniel Obam**	**Moderator**
2. Thuranira Gatuyu	Presenter 1
3. Sylvia Chelogoi	Presenter 2
4. Duncan Nyale	Presenter 3
5. Christopher Maina	Presenter 4

TEAM B MEMBERS	ROLE
1. **Rose Mosero**	**Moderator**
2. Marion Murithi	Presenter 1
3. Victor Nzomo	Presenter 2
4. Miriam Kakenya	Presenter 3
5. Dr.Humphrey Njogu	Presenter 4

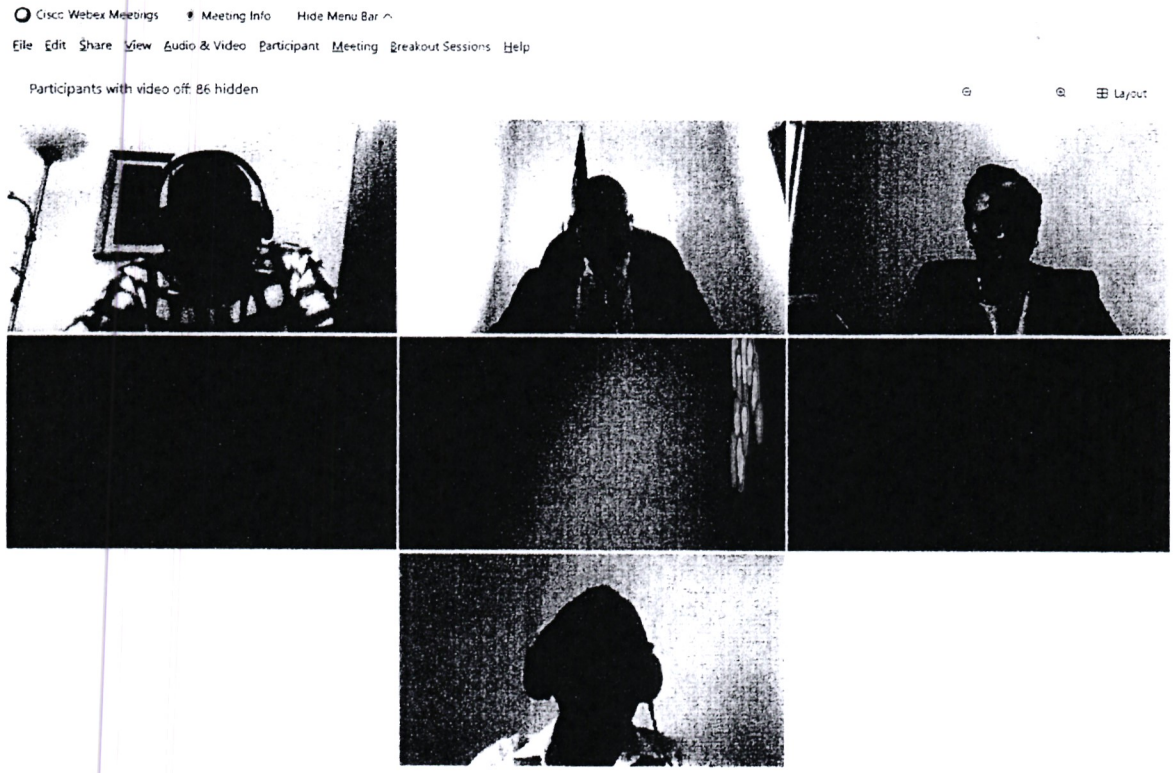
	Morning Session (9am – 11am)	**WEBINAR LINKS - WEEK THREE (3)**
1.	**Judiciary** - Monday 3rd May 2021	Taskforce Meeting With the Judiciary on 3rd May 2021 - Stakeholder consultations on the proposed data protection regulation, 2021 Hosted by Raphael Njeru https://moictke.webex.com/moictke/j.php?MTID=m763c65855ba1a3698e6b6b742713fb5f Monday, May 3, 2021 9:00 am | 2 hours | (UTC+03:00) Nairobi Meeting number: 183 772 4364 Password: yAjUWPJf353

ANNEX 10

Sno.	Meeting Name and Date Held	No of Participants
1.	Webex Screen Shots - Taskforce Meeting on the Development the General regulations on Monday 19th April 2021	50
2.	Meeting Screen Shots for Civil Society - Stakeholder consultations on the proposed Data Protection Regulation - Tuesday 20th April 2021 (2pm - 4pm)	50
3.	Wednesday 21st April 2021 Morning 9-11 Am 21st April 2021 Afternoon, 2-4pm (Was conducted by Lawyers Hub)	Meeting hosted by Lawyers Hub
4.	Attendance Key Data Holders – Thursday, 22-04-2021 9am -11am Stakeholder consultations on the proposed data protection regulation	34
5.	Attendance Key Data Holders – Thursday, 22-04-2021 2 -4 pm Stakeholder consultations on the proposed data protection regulation	41
6.	Attendance for Private – Friday, 23rd April 2021 From 9-11 Am - Stakeholder consultations on the proposed data protection regulation	47
7.	Attendance and Chat for Private – Friday, 23rd April 2021 From 2-4pm - Stakeholder consultations on the proposed data protection regulation	25
8.	Attendance and Chat with the Media – Monday, 26th April 2021 From 9-am - Stakeholder consultations on the proposed data protection regulation	35
9.	Attendance and Chat with Development Partners and International Orgs – Monday 26th April 2021 From 2-4pm - Stakeholder consultations	31
10.	Attendance and Chat with the Professional Bodies & Associations – Tuesday, 27th April 2021 From 9-am - Stakeholder consultations	38
11.	Public Participation Forum - Tuesday 27th April 2021(2pm-4pm)- Stakeholder consultations on proposed Data Protection Regulation	308 Attended 134 Absent
12.	Attendance and Chat with the Independent Commissions and Key State Offices–Wednesday, 28th April 2021 From 9-11Am - Stakeholder Consultations	40
13.	Attendance and Chat with the Public – Wednesday, 28th April 2021 From 2-4 PM - Stakeholder consultations on the proposed data protection regulation	212 Attended 70 Absent
14.	Attendance and Chat with Devolved Government –Thursday, 29th April 2021 From 9-11Am - Stakeholder Consultations	49
15.	Attendance and Chat with the Public –Thursday, 29th April 2021 From 2-4Pm - Stakeholder Consultations	348 Attended 69 Absent
16.	Attendance for the Key Government Entities – Friday, 30th April 2021 From 9-11 Am - Stakeholder consultations on the proposed data protection regulation	53
17.	Attendance With the Financial Sector – Monday, 3rd May 2021 From 2-4 Pm - Stakeholder consultations on the proposed data protection regulation	254

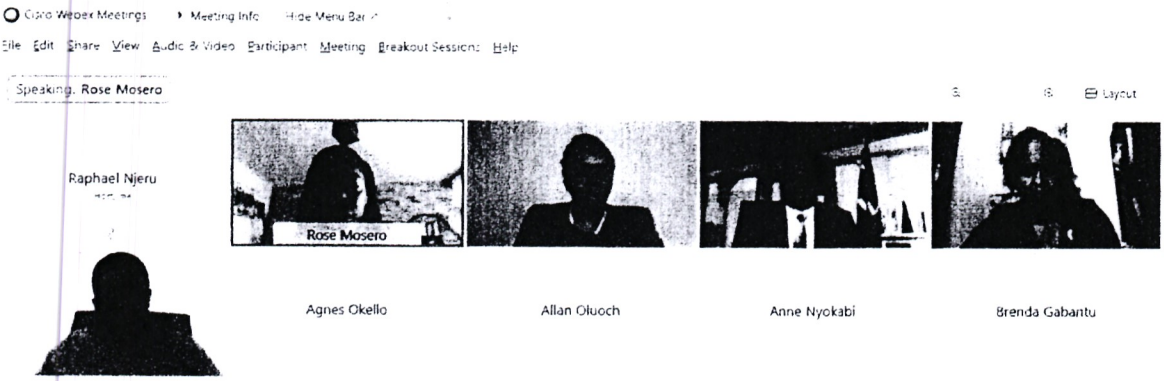
Meeting Screen Shots:

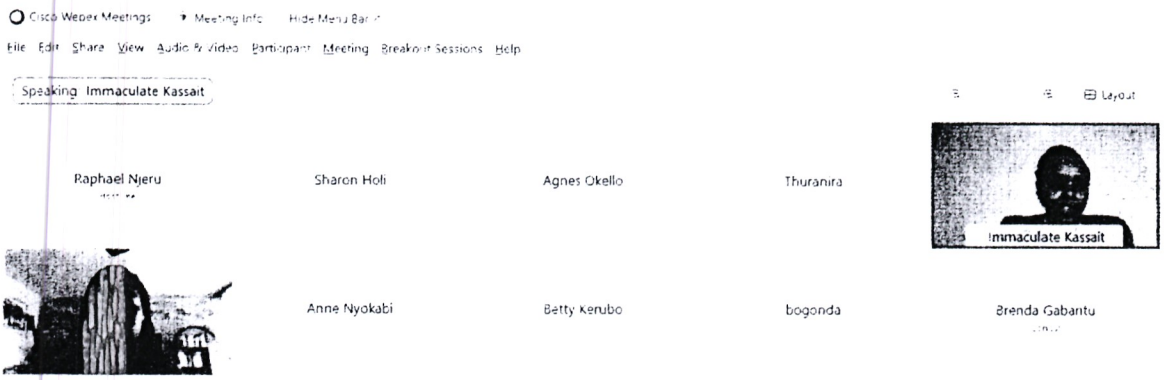
Civil Society - Stakeholder consultations on the proposed Data Protection Regulation, Tuesday 20th April 2021 (2pm - 4pm)




Rahab Jumia
EOS WEBCAM UTILITY

Attendance: Key Data Holders – Thursday, 22/04/2021 Stakeholder consultations on the proposed data protection regulation

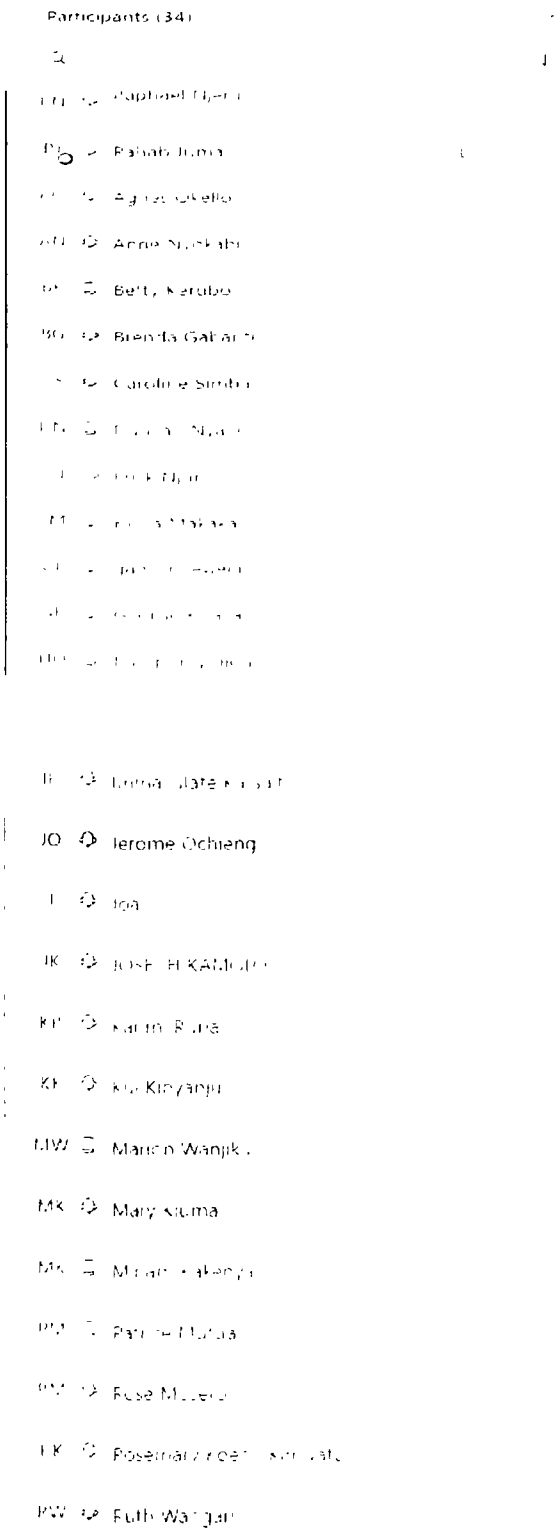




Meeting Information

Meeting Topic:	Key Data Holders - Stakeholder c...
Location:	moictke.webex.com
Meeting number:	183 459 4508
Current host:	Raphael Njeru
Current presenter:	Rahab Juma
Current user:	Raphael Njeru
Current number of particip...	34

Screen Shot of Participants



RK Rosemary Koech-Kimwatu

RW Ruth Wangari

SA said ali

 Sally Washiko

SH Sharon Holi

SO Sharone Otieno

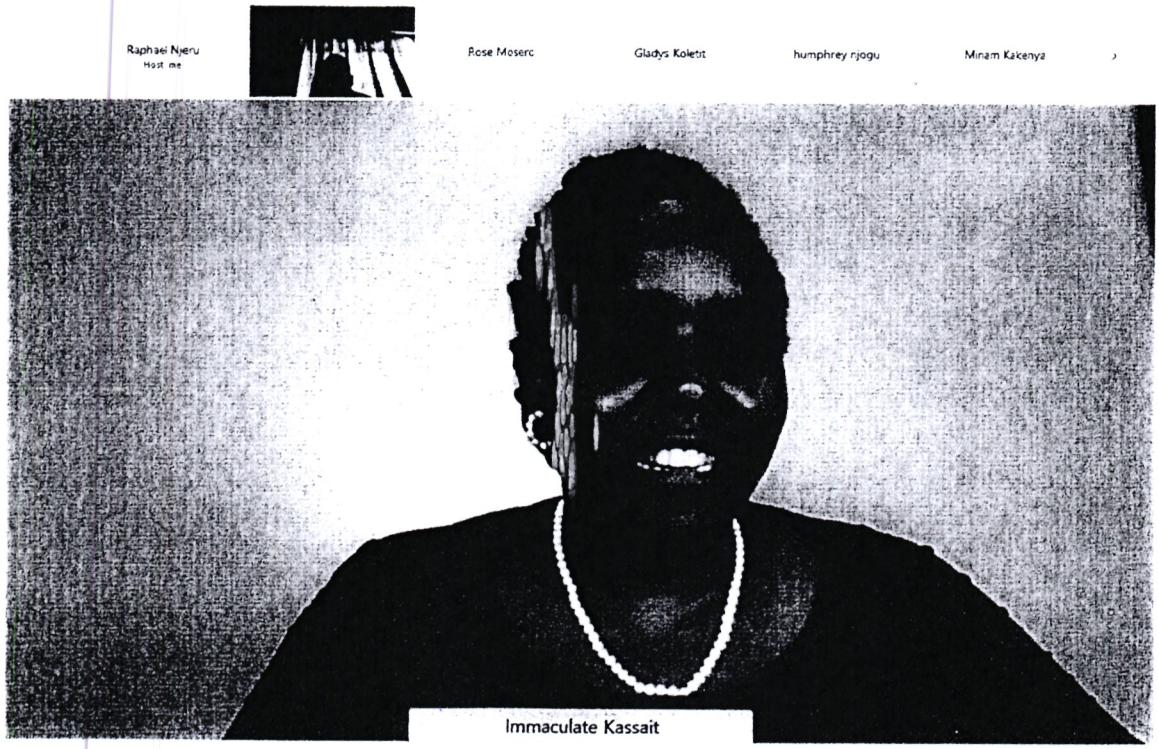
SC sylvia Chelogoi

T Thuranira

VN Victor B. Nzomo

YM Yvonne Mwendi

Attendance Key Data Holders – Thursday, 22-04-2021 2-4pm Stakeholder consultations on the proposed data protection regulation



Michael Murungi

Duncan Ndyali

George Owuor

Gladys Kolera

Humphrey Ngogu

Immaculate Kassait

Jackson Kariuki

Jane Munoru

JOSEPH KAMOLO

Lady Njeru

Mary Kiuma

Miriam Maina

Patrice Mutua

Ramab Ikoma

Augustus Munyasia

Cornelius Murgor

Duncan Ndyali

George Owuor

Michael Murungi

Mary Kiuma

Patrice Mutua

Ramab Ikoma

Anne Nyokabi

Bogonda

Michael Murungi | narrimane Guest | Otilia Phiri | Patrice Mutua | said ali

Victor B. Nzomo | Anne Nyokabi | bogonda | Brenda Gabantu

CW | Dana Osiemo | jane Munoru | Jesse Kasuku | jtanui

lynneth cheronoh | Miriam Kakenya | Miriam Maina | Rahab Juma | Thuranira

Participants (41)

Search

RN Raphael Njeru

RJ Rahab Juma

MM Michael Murungi

BG Brenda Gabantu
Conost

AL Adam Lane

AN Anne Nyokabi

AM Augustus Munywoki

A AWafula

B bogonda

CG Christopher Guest

CM Cornelius Murpus

C CW

DO Dana Osiemo

DM Dianson Mucheru

DN Duncan Ndare

GO George Ooko

GK Gladys Kolet

HS Hadia Shakombo

HN Humphrey Ngigi

IK Immaculate Kasait

JK Jackson Kalaw

JM Jane Muchoki

JK Jesse Kasuku

JK Joseph Kamau

KM Kamau

KM Kelly Mbi

LM Lucy Mwa

MM Margaret Mumbua

MK Mary Kuria

MK Miriam Kaberia

MM Mirriam Mutua

NK Nancy Kamau

OP Olivia Pkoi

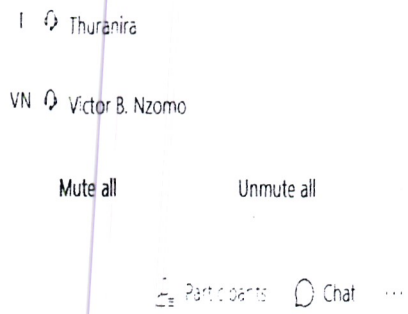
PM Patrick Mutua

PM Peter Mbeti

Sa Sayial

SA Said, Wasiwa

SC Sylvia Chelogoi


I Thuranira
VN Victor B. Nzomo
Mute all
Unmute all
Participants
Chat

Attendance for <u>Private</u> – 23rd April 2021 9-11 Am - Stakeholder consultations on the proposed data protection regulation

Speaking: Duncan Nyale

Layout

Raphael Njeru			Adam Lane	Jade Makory
Anne Nyokabi	Anthony Mwangi	Augustus Munywoki	Brenda Gabantu	Charlene Owidh
collins	Davis Waithaka	Dr Chweya	Eugene Ngumi	George Owuor
Hez Gikang'a	Humphrey Amos Lilech	Hanifa Shakombo	Immaculate Kassait	JOSEPH KAMOLO
Mary Kiuma	Maxwell Okello	Michael Maina	Miriam Kakenya	Nono Malefane
Eugene Ngumi	George Owuor	Hanifa Shakombo	Hez Gikang'a	Immaculate Kassait
JOSEPH KAMOLO	Michael Maina	Miriam Kakenya	Nono Malefane	Otilia Phiri
Patrice mutua	Phyllis Kamau	Rahab Juma	Rhodah Mwangi	Rishi Saha
Rose Mosero	Rose Mosero	Rosemary Koech-Kimwatu	said ali	
Samantha	sylvia cherotich chelogoi	Thomas Reilly	Tom OMARIBA	Victor B. Nzomo



Humphrey njogu | Adam Lane | Augustus Munywoki | Ben Roberts | Brenda Gabanu

Jade Makory | JOSEPH KAMOLO | Mary Kiuma | Maxwell Okello | Peter Shamisi

Rahab Iuma |  |  | Anne Nyokabi

Anthony Mwangi | Catherine Muiya | Charlene Owidh | colins | Dr Laweya

Mary Kiuma |  | Peter Shamisi | Rahab Kuria | Sylvia Chemutai Chelogoi

Agnes Okello | Anne Nyokabi | Catherine Muiya | Charlene Owidh | Dr Chweya

felix ochoro | Hanifa Shakombo | Humphrey Amos Lilechi | Humphrey Njogu | Jade Makory

Ken | Laura Kerubo | Lee Kachan Ali | Linda Bonyo | Michael Maina

Miriam Kakenya | Patrick mutua |  | Samantha | Tom OMARIBA

Meeting Information

Meeting Topic:	Private - Stakeholder consultatio...
Location:	moictke.webex.com
Meeting number:	183 225 9560
Current host:	Raphael Njeru
Current presenter:	Rahab Juma
Current user:	Raphael Njeru
Current number of particip...	46

Participants (47)

Search

RN Raphael Njeru (Host, me)

RJ Rahab Juma

AL Adam Lane

AN Anne Nyokabi

AM Anthony Mwangi

AM Augustus Munywoki

BR Ben Roberts

BG Brenda Gabantu

CM Catherine Muya

CO Charlene Owidh

C collins

DW Davis Waithaka

DC Dr Chweya

DN Duncan Nyale

EN Eugene Ngure

FO Felix Ochieng

GO George Owuor

HS Hanifa Shakombo

HG Hez Gikang'a

HH Humphrey Amos Heidi

HM Mungai Mwangi

IK Ismail Kassam

IM Ian Mwaura

JK JOSEPH KAMOLO

KK Kevin

LB Linda Bonyo

MK Mary Kiuma

MO Maxwell Okello

MM Michael Maina

MK Miriam Kakenya

NM Nono Malefane

OP Otilia Phiri

PM Patrice mutua

PK Peter Khamisi

PK Phyllis Kamau

RM Rhodah Mwangi

RS Rishi Saha

R Risper

RM Rose Mosero

RM Rose Mosero

RK Rosemary Koech-Kimwatu

SA said ali


Sali, Washiko

S Samantha

SC sylvia cherotich chelogoi

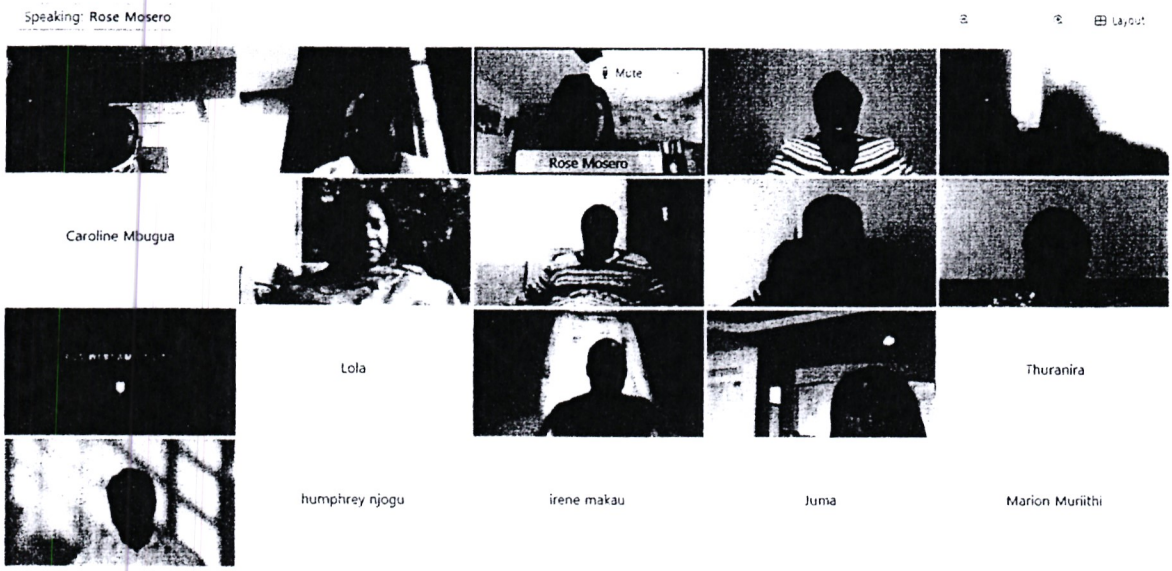
TR Thomas Reilly

TO [illegible] MARBA

VN [illegible] Nzomo

Mute all Unmute all

Attendance and Chat for Private – Friday, 23rd April 2021 From 2-4pm - Stakeholder consultations on the proposed data protection regulation



Participants (25)

RN Raphael Njeru

RJ Rahab Juma

BG Brenda Gabantu

AN Anne Nyokabi

AM Augustus Munywoki

CM Caroline Mbugua

DM Danson Mugambi

FA Fiona Asonga

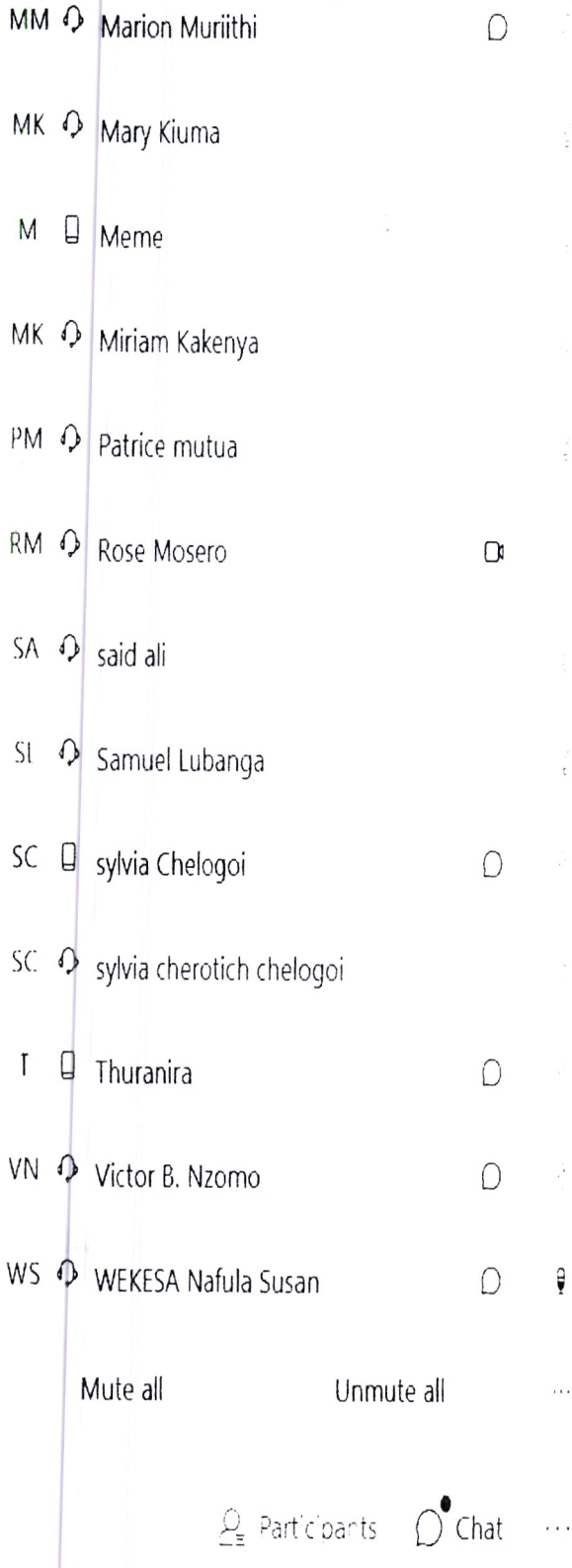
HN Humphrey njogu

IK Immaculate Kassait

JK JOSEPH KAMOLO

L Lola

MM Marion Muruli


MM Marion Muriithi
MK Mary Kiuma
M Meme
MK Miriam Kakenya
PM Patrice mutua
RM Rose Mosero
SA said ali
SI Samuel Lubanga
SC sylvia Chelogoi
SC sylvia cherotich chelogoi
T Thuranira
VN Victor B. Nzomo
WS WEKESA Nafula Susan
Mute all
Unmute all
Participants
Chat

Chat

Please enable the chat with everyone function

from Rose Mosero (privately)· 2:08 PM

you can enable then using the assign privileges function

from Rose Mosero to everyone: 2:09 PM

Welcome everyone! we will be commencing this afternoon's session shortly

from Rose Mosero to everyone: 2:23 PM

Welcome to all participants

from Rose Mosero to everyone: 2:29 PM

to those who were able to introduce themselves at the begining of the session, please do so on the chat stating your name, designation and organisation you represent.

from Rose Mosero to everyone· 2:29 PM

Welcome Samuel. Thank you for joining!

from Brenda Gabantu to everyone· 3:47 PM

https://bit ly/3xoZu3E

from Brenda Gabantu to everyone· 3:48 PM

Public Participation Forum - Tuesday 27th April 2021
https://bit.ly/3tFoHV8

Public Participation Forum-Wednesday 28th April 2021
https://bit.ly/3xoZu3E

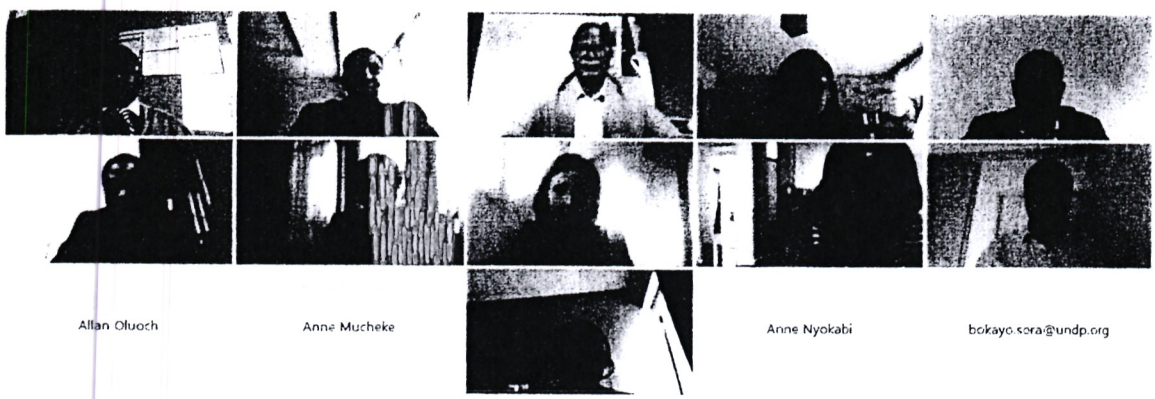
Public Participation Forum-Thursday 29th April 2021
https://bit.ly/2QHJLvy

Attendance and Chat with Development Partners and International Orgs – Monday, 26th April 2021 From 2-4 Pm - Stakeholder consultations on the proposed data protection regulation

Anne Nyokabi | bokayo.sora@undp.org | Hillary Kiboro | Charles Wesonga Juma | humphrey njogu

JOSEPH KAMOLO | Mary Kiuma | Miriam Kakenya | Olivier Dubois ICRC | Patrice Mutua

Rahab Juma | Roly Davila/UNDP | | Victor B. Nzomo | Thuranira



Charles Wesonga Juma | humphrey njogu | Mary Kiuma | Olivier Dubois ICRC | Miriam Kakenya

Patrice Mutua | Rahab Juma | Roly Davila/UNDP

Meeting Information

Meeting Topic:	Stakeholder consultations on the...
Location:	moictke.webex.com
Meeting number:	183 480 2216
Current host:	Raphael Njeru
Current presenter:	Rahab Juma
Current user:	Raphael Njeru
Current number of particip...	31

Attendance

Participants (29)

Q

PN Raphael Njeru

RJ Rahab Juma

BG Brenda Gabantu

AO Allan Oluoch

AL Anat Lewin

AM Anne Mucheke

AN Anne Nyokabi

B bokayo.sora@undp.org

CK Caroline Chepkorir Koech

C Charles Wesonga Juma

DO DANIEL OBAM

DS David Satola

DN Duncan Nyale

HK Hillary Kiboro

HN humphrey njogu

JS Jane Serwanga

JK JOSEPH KAMOLO

MK Mary Kiuma

MK Miriam Kakenya

OI Olivier Dubois ICRC

PM Patrice Mutua

RD Roly Davila/UNDP

RM Rose Mosero

SA said ali

Sally Washiko

SI Salomé Eggler

SC sylvia cherotich chelogoi

T Thuranira

VN Victor B. Nzomo

Chat with Development Partners and International Orgs – Monday, 26th April 2021
From 2-4 Pm - Stakeholder consultations on the proposed data protection regulation

from Anne Mucheke to everyone: 2:07 PM

My apologies. That appears by mistake - I'm trying to put it down. sorry

from Salomé Eggler to everyone: 2:13 PM

Good afternoon, my name is Salomé Eggler. I'm the Head of the Digital Transformation Centre of Germany's Development Agency GIZ. Unfortunately there seems to be a technical glitch with my microphone so kindly accept my introduction here in the chat. Happy to be participating in the consultation

from Salomé Eggler to everyone: 2:14 PM

Thank you!

from Rose Mosero to everyone: 2:20 PM

Welcome All!

from Brenda Gabantu to everyone: 2:21 PM

Public Participation Forum - Tuesday 27th April 2021

https://bit.ly/3tFoHV8

Public Participation Forum-Wednesday 28th April 2021

https://bit.ly/3xoZu3E

Public Participation Forum-Thursday 29th April 2021

https://bit.ly/2QHJLvy

from Rose Mosero to everyone: 2:21 PM

For those joining us after the round of introductions, please introduce yourself in the chat by stating your name, designation and organisation you represent.

from Brenda Gabantu to everyone: 2:22 PM

Please find the links for registration to the Public Webinars starting tomorrow from 2pm

from Brenda Gabantu to everyone: 2:24 PM

https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/

from Brenda Gabantu to everyone: 2:24 PM

https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021

from Rose Mosero to everyone: 2:33 PM

For those joining us after the round of introductions, please introduce yourself in the chat by stating your name, designation and organisation you represent.

from Rose Mosero to everyone: 2:38 PM

Please feel free to post your questions on the chat and we will address them after the taskforce members have made their presentations.

from Hillary Kiboro to everyone: 2:50 PM

The General Regulations provide for exemption from the Act, data collected for purposes of locating a missing a person; could you elaborate on the 'reporting' contemplated in the Regulations? does it require the report to have been made to the police/authorities (local admin)? Would it include a situation of emergency where humanitarian organizations are trying to locate missing persons, who may not necessary have been reported to authorities as missing?

from Hillary Kiboro to everyone: 3:14 PM

Are organizations that process data under the rubric of public interest exempt from the entirety of the Act, including registration?

from Olivier Dubois ICRC to everyone: 3:23 PM

Sound was unstable. specially for the second answer

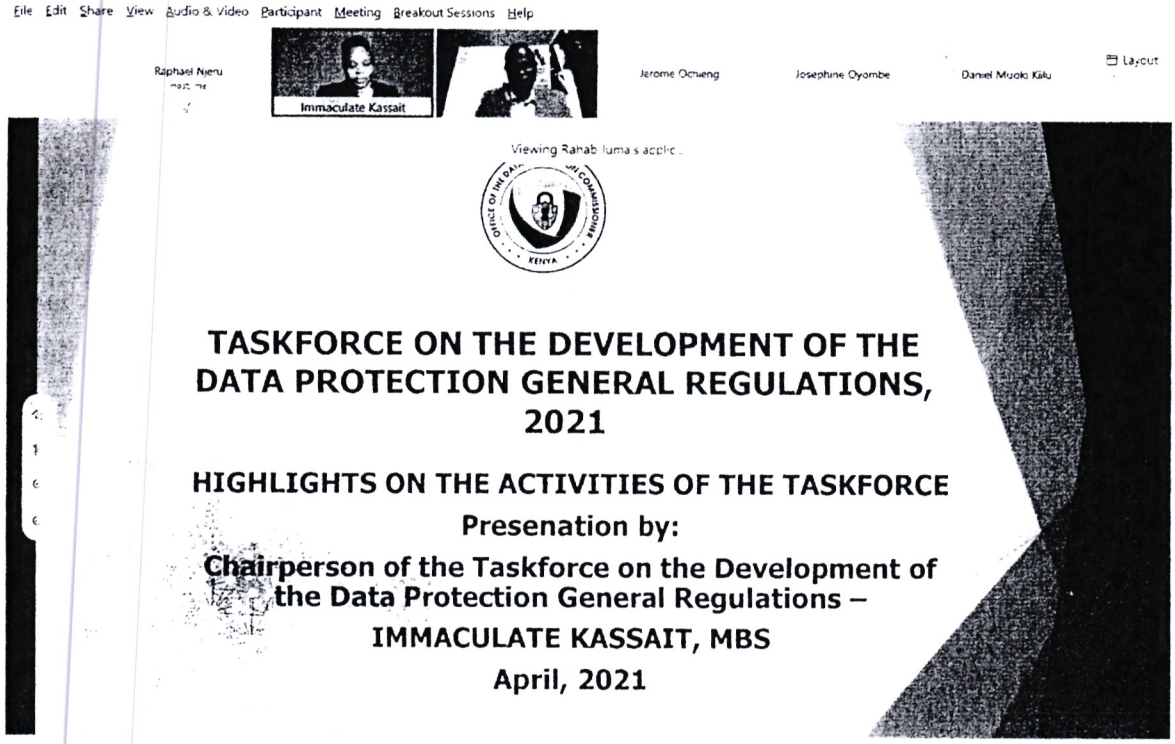
from Hillary Kiboro to everyone: 3:32 PM

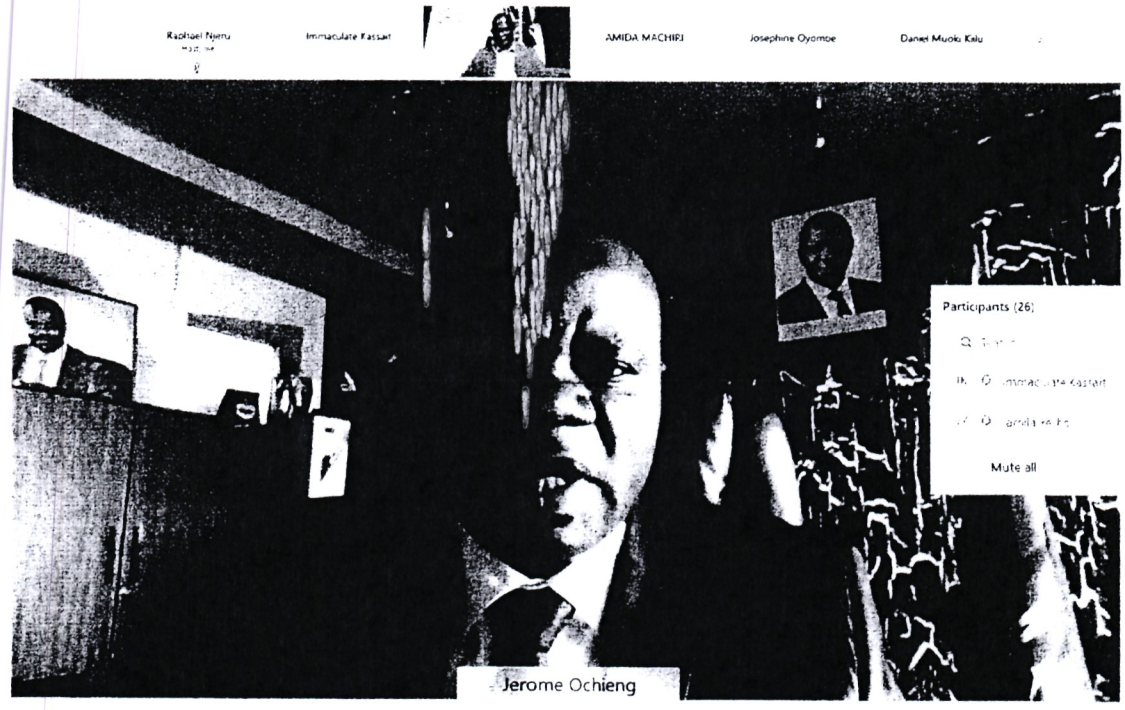
Does an organization need to apply for exemption or it's granted as a matter of course?

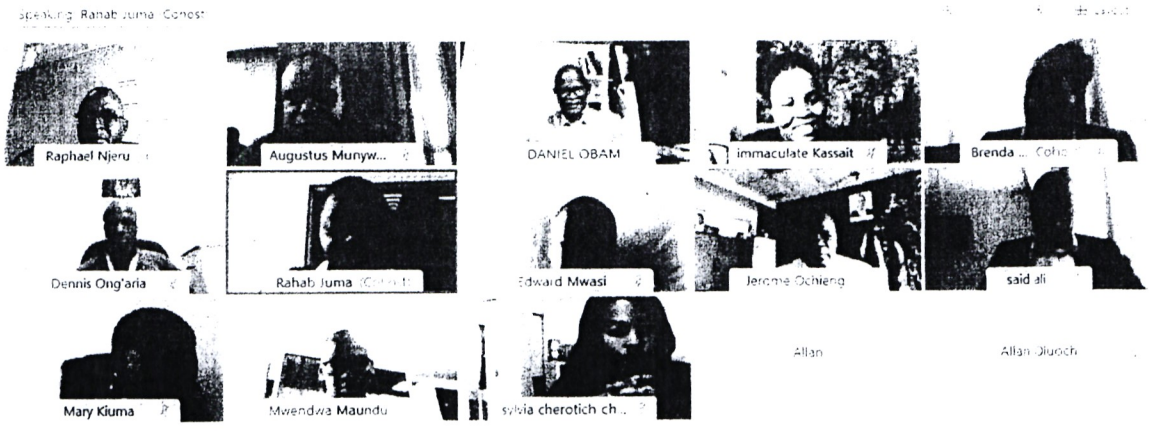
from Olivier Dubois ICRC to everyone: 3:44 PM

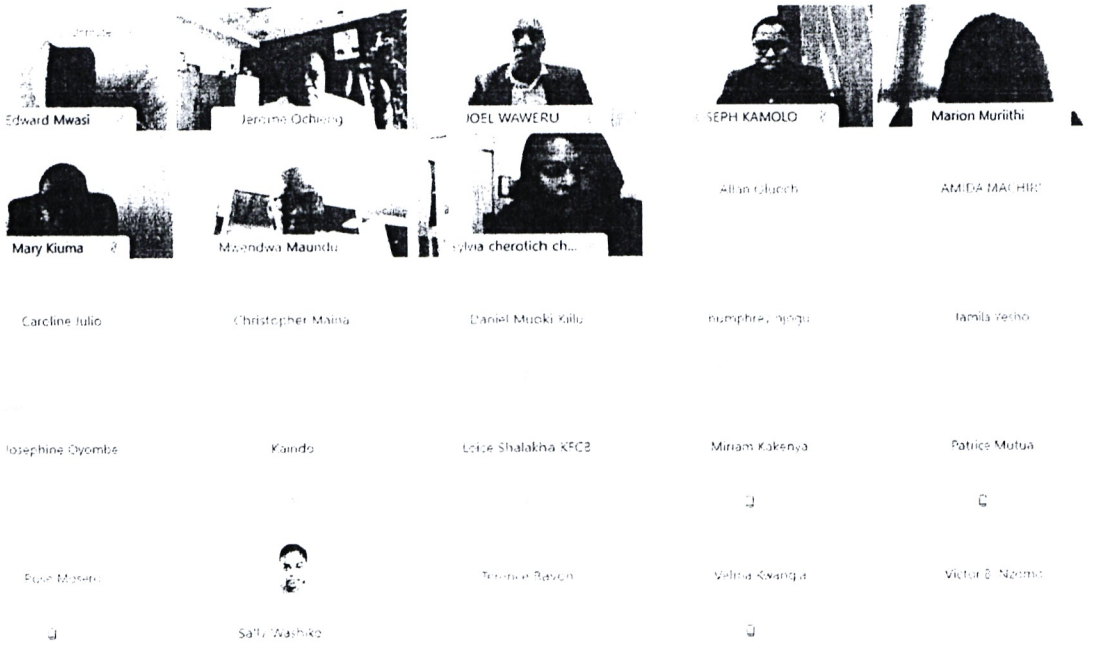
unable to open the video

Attendance and Chat with the Media – Monday, 26th April 2021 From 9-11 Am - Stakeholder consultations on the proposed data protection regulation






Raphael Njeru
Augustus Munyw...
DANIEL OBAM
immaculate Kassait
Brenda ... Cohe
Dennis Ong'aria
Rahab Juma (Ghost)
Edward Mwasi
Jerome Ochieng
said ali
Mary Kiuma
Mwendwa Maundu
sylvia cherotich ch...
Allan
Allan Oluoch
AMIDA MACHIRI
Christopher Maina
Daniel Muoki Kilu
Humphrey Ojiogu
Tamila Yecho
Josephine Oyombe
Kaindo
Leice Shalakha KECB
Miriam Kakenya
Patrice Mutua
Sally Washiko


Edward Mwasi
Jerome Ochieng
JOEL WAWERU
SEPH KAMOLO
Marion Muriithi
Mary Kiuma
Mwendwa Maundu
sylvia cherotich ch...
Allan Oluoch
AMIDA MACHIRI
Carcline Julio
Christopher Maina
Daniel Muoki Kilu
Humphrey Ojiogu
Tamila Yecho
Josephine Oyombe
Kaindo
Leice Shalakha KECB
Miriam Kakenya
Patrice Mutua
Sally Washiko

chieng

Josephine Oyombe	Daniel Muoki Kilu	AMIDA MACHIRI	Anne Nyokabi	Augustus Munywoki
Brenda Gabantu	Caroline	Duncan Nyale	Edward Mwasi	Eunice Mwanza
humohrey njogu	Jamila Yesho	JOEL WAWERU	JOSEPH KAMOLO	Loice Shalakha KFCB
Mary Kiuma	Mwendwa Maundu	Patrice Mutua	Rahab Juma	Rose Mosero
said ali	 Sali, Washiko	sylvia cherotich chelogoi	Terence Bavon	Victor B. Nzomo

Meeting Information

Meeting Topic:	Media - Stakeholder consultation...
Location:	moictke.webex.com
Meeting number:	183 248 9068
Current host:	Raphael Njeru
Current presenter:	Rahab Juma
Current user:	Raphael Njeru
Current number of particip...	35

Attendance

Participants (32)

Search

RN Raphael Njeru

Ranak Iuma

Alia Ghuge

AM AMEA MACHIP

[illegible]

[illegible]

[illegible]

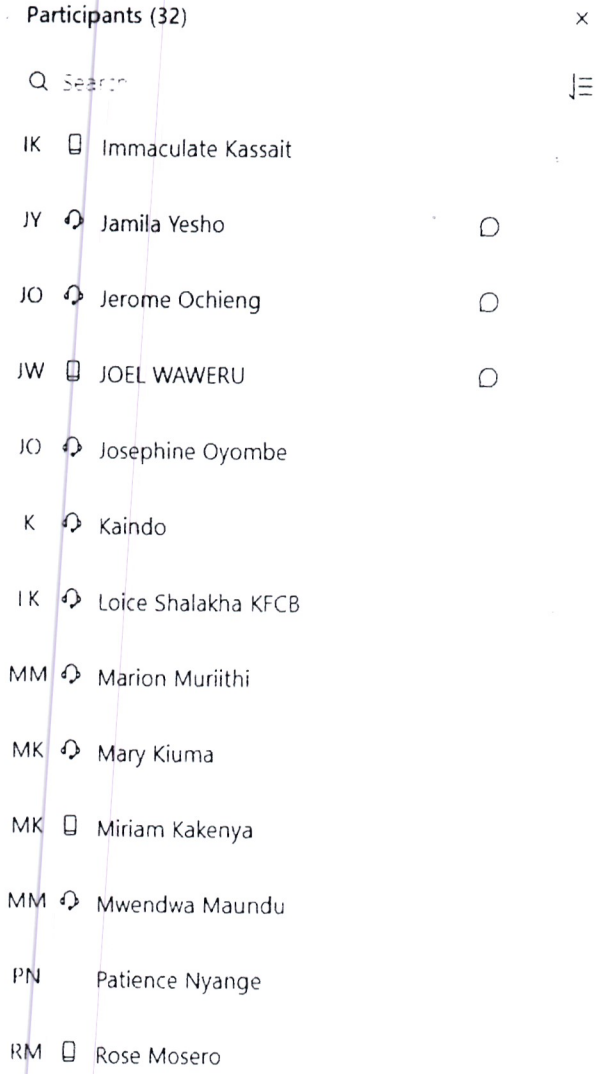
DN DAN ELOgAM

Dennis Gwaina

Edward Mwas

Esther Mwanza

[illegible]



Chat with the Media

from Rahab Juma to everyone: 9:08 AM

#dataprotectionke

from Rahab Juma to everyone: 9:08 AM

#publicparticipation

from Rahab Juma to everyone: 9:09 AM

Comments on the draft regulationcan be sent to dataprotectionregulations@odpc.go.ke

from Brenda Gabantu to everyone: 9:13 AM

https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/

from Brenda Gabantu to everyone: 9:17 AM

https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021

from Brenda Gabantu to everyone: 9:18 AM

https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/

from Brenda Gabantu to everyone: 9:18 AM

Please see the links to the Regulations

from Rahab Juma to everyone: 9:18 AM

The deadline for submitting comments on the draft regulations is Tuesday 11th May 2021

from Brenda Gabantu to everyone: 9:20 AM

Public Participation Forum - Tuesday 27th April 2021

https://bit.ly/3tFoHV8

Public Participation Forum-Wednesday 28th April 2021

https://bit.ly/3xoZu3E

Public Participation Forum-Thursday 29th April 2021

https://bit.ly/2QHJLvy

from Terence Bavon (privately): 9:24 AM

Terence Bavon from Media Council of Kenya

from Daniel Muoki Kiilu (privately): 9:26 AM

Daniel Muoki Kiilu - ICT, Kenya Yearbook Editorial Board

from JOEL WAWERU to everyone: 9:28 AM

Joel Waweru- Digital Broadcasters Association

from Caroline Julio (privately): 9:36 AM

Hi Raphael, for purposes of registration you can note Caroline Julio -caroline.julio@ke.wananchi.com (Wananchi Group)

from DANIEL OBAM to everyone: 9:38 AM

Kindly post the institution you are representing here

to Caroline Julio (privately): 9:51 AM

That has been noted. Thank you

from Caroline Julio (privately): 10:20 AM

how does someone chat everyone ?

from Caroline Julio (privately): 10:20 AM

theres no option for everyone on the participants

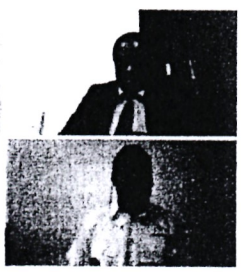
from Brenda Gabantu to everyone: 10:21 AM

Public Participation Forum - Tuesday 27th April 2021
https://bit.ly/3tFoHV8

Public Participation Forum-Wednesday 28th April 2021
https://bit.ly/3xoZu3E

Public Participation Forum-Thursday 29th April 2021
https://bit.ly/2QHJLvy

Attendance and Chat with the Professional Bodies & Associations – Tuesday, 27th April 2021 From 9-am - Stakeholder consultations on the proposed data protection regulation

Raphael Njeru			humphrey njogu	Victor B. Nzomo
immaculate Kassait	Anthony Muiyuro	arik karani	Brencil	Brenda Gabantu
Colins of LSK	DANIEL OBAM	Duncan Nyale		hnjogu
jothero	Preston	Rahab Juma	said ali	Sebastian Bwire EBK
sylvia cherotich chelogoi	Veronica Rose	Augustus Munywoki	chebett Koske	Daniel Nyoike
 hnjogu		jothero	Preston	Rahab Juma
said ali		sylvia cherotich chelogoi	Veronica Rose	Augustus Munywoki
chebett Koske	Daniel Nyoike	Glory Mutungi	Jeff	John Waweru
Joyanne Njau	Leah Eshitemi	Marion Murithi	Mary Kiuma	Maureen Koech
Miriam Kakenya	MWONGERA RUKARIA	Patrice Mutua		Sherry Bor

Attendance

Meeting [illegible]

Meeting Topic	[illegible]
Location	[illegible]
Meeting number	163 964 1399
Current host	Raphael Njeru
Current presenter	Brenda Gabaritu
Current user	Raphael Njeru
Current number of particip...	38

Participants (41)

RN Raphael Njeru

[redacted] Brenda Gebantu
Cohost

AM Anthony Muiyuro

AK ank karani

AM Augustus Munywoki

B Brencil

CK chebett Koske

CL Colins of LSK

DN Daniel Nyoike

DO DANIEL OBAM

DK Desislava Krusteva

DS Dr Kigondu Simon KMA SG

DN Duncan Nyale

GG Gibayi Gibson

GW Gichohi Waweru

GM Glory Mutungi

HN humphrey njogu

IK immaculate Kassait

J Jeff

JW John Waweru

JK JOSEPH KAMOLO

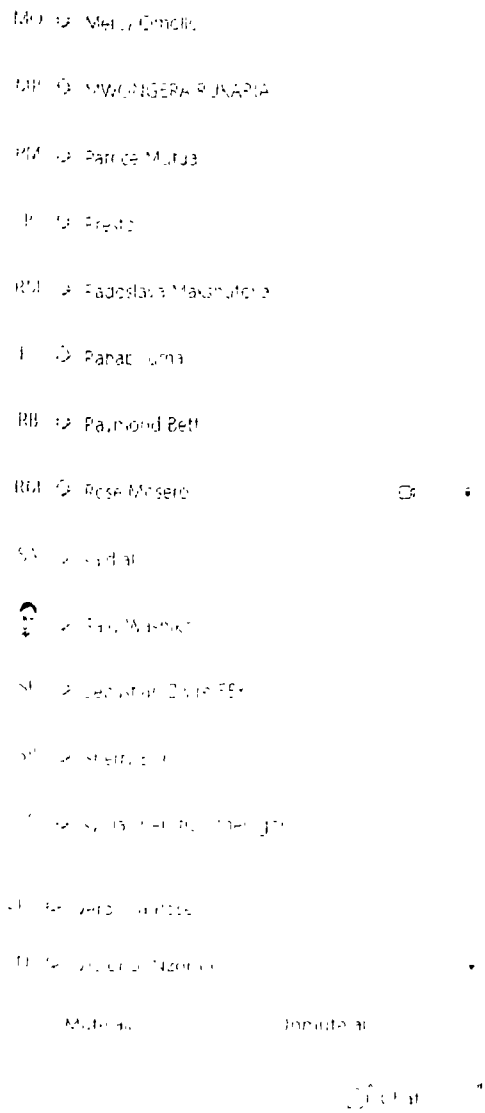
J jothero

JN Joyanne Njau

LE Leah Eshitemi

MK Mary Kiuma

MK Maureen Koech



Chat with the Professional Bodies & Associations

Do something to make the audio stable

from Rahab Juma to everyone: 9.27 AM

The Comments on the draft regulations can be sent to the following email address dataprotectionregulations@odpc.go.ke

from Rahab Juma to everyone: 9:28 AM

the regulations can be found on here

from Rahab Juma to everyone: 9:29 AM

for the Data Protection General Regulations, 2021 https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/

from Rahab Juma to everyone: 9:32 AM

For the Data Protection (Compliance and Enforcement) Regulations, 2021
https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/

from Rahab Juma to everyone: 9:33 AM

For the Data Protection (Registration of Data Controllers and Data Processors), 2021
https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021/

from Rahab Juma to everyone: 9:34 AM

The Links for Public participation forums are as follows:

from Rahab Juma to everyone: 9:35 AM

Public Participation Forum - Tuesday 27th April 2021

https://bit.ly/3tFoHV8

Public Participation Forum-Wednesday 28th April 2021

https://bit.ly/3xoZu3E

Public Participation Forum-Thursday 29th April 2021

https://bit.ly/2QHJLvy

to Sherry Bor (privately): 9:42 AM

Please mute your mic. Thanks

from Rose Mosero to everyone: 9:43 AM

Welcome All!

from Rose Mosero to everyone: 9:44 AM

To those joining us after the introdcutions, please introduce yourself on the chat by stating your name,designation and organisation you represent.

from Rose Mosero to everyone: 9:47 AM

If you have any questions or comments regarding the regulations, please feel free put them in the chat. We will address the questions as we go and after the presentations

from Gibayi Gibson (privately): 10:00 AM

Hello, My name is Gibayi Gibson working for Kenya Engineering Technology Registratiob Board as an ICT-Assistant . Sorry for beign late.

from Gibayi Gibson (privately): 10:04 AM

For Kenya Engineering Technology Registration Board- ICT Assistant

from Brencil to everyone: 10:07 AM

For better context, Kindly give a few examples of what automated decision processes currently exist in

from Rose Mosero to everyone: 10:12 AM

@Brencil, some examples are : applications for loans where there is no human interventions save for the intial inputs to enable machine learning;

from Rose Mosero to everyone: 10:14 AM

this would effectively cover any computer system decision making. Insurance cover, where profiling and systems are used to decide if you can receive a cover

from Brencil to everyone: 10:14 AM

Thank you

from Veronica Rose (privately): 10:16 AM

Will the option for "opt-out" on all services serve as a right to be forgotten?

from Anthony Muiyuro to everyone: 10:19 AM

For clarity, Is a DPIA limited to only those activities?

from Brencil to everyone: 10:25 AM

For clarity, kindly provide more contect on what complains qualify as scandalous or vexatious;

from Glory Mutungi to everyone: 10:32 AM

What is this fees like, hope not punitive,because already there so many requirements for learning institutions that require registration fees.

from Colins of LSK (privately): 10:37 AM

Please share with me the slides @

from Colins of LSK (privately): 10:38 AM

Please share with me the slides @ collins@lsk.or.ke

from Gibayi Gibson (privately): 10:39 AM

How does the government monitor the use of data captured as internet cookies despite the fact that an individual gives consent to that .

from jothero to everyone: 10:40 AM

Is there a possibility of a moratorium period for implementation of certain aspects of the Act/Regulations e.g Registration formalities

from Brencil to everyone: 11:13 AM

Thank you

from Preston to everyone: 11:13 AM

Thanks for the presentation

from Anthony Muiyuro to everyone: 11:13 AM

Thank you

from Glory Mutungi to everyone: 11:13 AM

Thank you

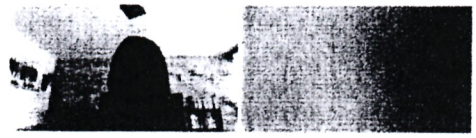
from Rose Mosero to everyone: 11:14 AM

thank you all!

Attendance and Chat with the Independent Commissions and Key State Offices – Wednesday, 28th April 2021 From 9-11Am - Stakeholder consultations on the proposed Data Protection Regulation

Speaking: kevin mpaka

Layout



Raphael Njeru	Bob ORPP			Ali Abdullahi
Allan Oluoch	CPA Florence Birya	Anne Nyokabi	Beatrice Zighe	Brenda Gabantu
Charles Ayoo	Cynthia Gichuki	DANIEL OBAM	David Kaboro	george
gyegon	humphrey njogu	isaac	Immaculate Kassait	janet
JOHN MAINA	JOSEPH KAMOLO	Josephine Kagucia	kevin mpaka	Lauranta
humphrey njogu	isaac	Immaculate Kassait	janet	JOHN MAINA
JOSEPH KAMOLO	Josephine Kagucia	kevin mpaka	Lauranta	Marion Munithi
Mary Kiuma	Michael	Mike Mwangi	Miriam Kakenya	Ocharo EACC
Patrice Mutua	Paul Mukeku	Paul Mukeku	Purissima Wambugu	Rahab Iuma
	Silas	Susan Jeruto	Thuranira	Victor B. Nzomo


Jerome Ochieng

Raphael Njeru Rose Mosero Josephine Kagucia anet Harry

Viewing Ramat Juma's applic

INTRODUCTION

The Office of the Data Protection Commissioner was established in Novemb 2020 pursuant to the Data Protection Act, 2019.

Mandate of the Office

To regulate the processing of personal data,

To ensure that the processing of personal data of a data subject is guided b the principles set out in Section 25 of the Act.

To protect the privacy of individuals

To establish the legal and institutional mechanism to protect personal da and

To provide data subjects with rights and remedies to protect their perso data from processing that is not in accordance with the Act.

Attendance

Meeting Information

Meeting Topic:	Independent Commissions and K...
Location:	moictke.webex.com
Meeting number:	183 569 0490
Current host:	Raphael Njeru
Current presenter:	Brenda Gabantu
Current user:	Raphael Njeru
Current number of particip...	40

Participants (40)

RN Raphael Njeru

BG Brenda Gabantu

CB CPA Florence Birya

KM kevin mpaka

CA Charles Ayoo

AA Al Abdullahi

AO Allan Oluoch

AN Anne Nyokabi

BZ Beatrice Zighe

BO Bob ORPP

CG Cynthia Gichuki

DO DANIEL OBAM

DK David kaboro

FK faith kaluai

G george

G gyegon

HN humphrey njogu

IK Immaculate Kassait

I isaac

J janet

JM JOHN MAINA

JK JOSEPH KAMOLO

JK Josephine Kagucia

L Lauranta

MM Marion Muriithi

MK Mary Kiuma

M Michael

MM Mike Mwangi

MK Miriam Kakenya

OI Ocharo EACC

PM Patrice Mutua

PM Paul Mukeku

PW Purissima Wambugu

RJ Rahab Juma

RM Rose Mosero

 Sally Washiko

S Silas

SJ Susan Jeruto

T Thuranira

VN Victor B. Nzomo

Mute all Unmute all

Participants Chat ...

Chat

from kevin mpaka (privately): 9:03 AM

do we have a program

from Cynthia Gichuki to everyone: 9:16 AM

Good morning, Cynthia Gichuki, Legal Officer Ethics and Anti-Corruption Commission

from Rose Mosero to everyone: 9:16 AM

Welcome All!

from Rose Mosero to everyone: 9:17 AM

For those who were not able to introduce themselves, please do so in the chat by stating your name, designation and organisation you represent.

from Rose Mosero to everyone: 9:18 AM

Thank yoou for joining this session

from Rahab Juma to everyone: 9:28 AM

comments on the regulations can be sent to the following email address dataprotectionregulations@odpc.go,ke

from Brenda Gabantu to everyone: 10:02 AM

https://bit.ly/3xoZu3E

from Brenda Gabantu to everyone: 10:03 AM

Public Participation Forum-Wednesday 28th April 2021

https://bit.ly/3xoZu3E

Public Participation Forum-Thursday 29th April 2021

https://bit.ly/2QHJLvy

from Brenda Gabantu to everyone: 10:23 AM

Please see the links to the Public forum this afternoon from 2pm and tomorrows link same time

Attendance for the Public – Thursday, 29th April 2021 From 2-4 Pm - Stakeholder consultations on the proposed data protection regulation

speaking DANIEL OBAM

Raphael Njeru

Anne nganga

Duncan Nyale | Brenda Gabantu | Humphrey Njogu | JOSEPH KAMOLO

Mary Kiuma | Miriam Kakenya | Patrice Mutua | Rahab Juma

Rose Mosero | Said Ali | Sally Washiko | sylvia chelogoi

Participants (126)

Search

Panelist: 18

RN Raphael Njeru

RJ Rahab Juma

AN Anne nganga

BG Brenda Gabantu

DO DANIEL OBAM

DN Duncan Nyale

HN Humphrey Njogu

IK Immaculate Kassait

JK JOSEPH KAMOLO

MM Marion Muriithi

MK Mary Kiuma

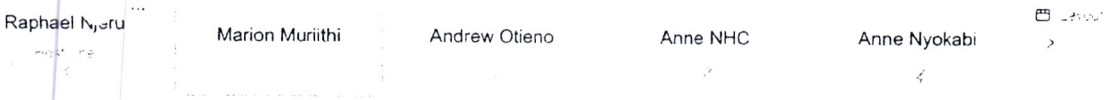
MK Miriam Kakenya

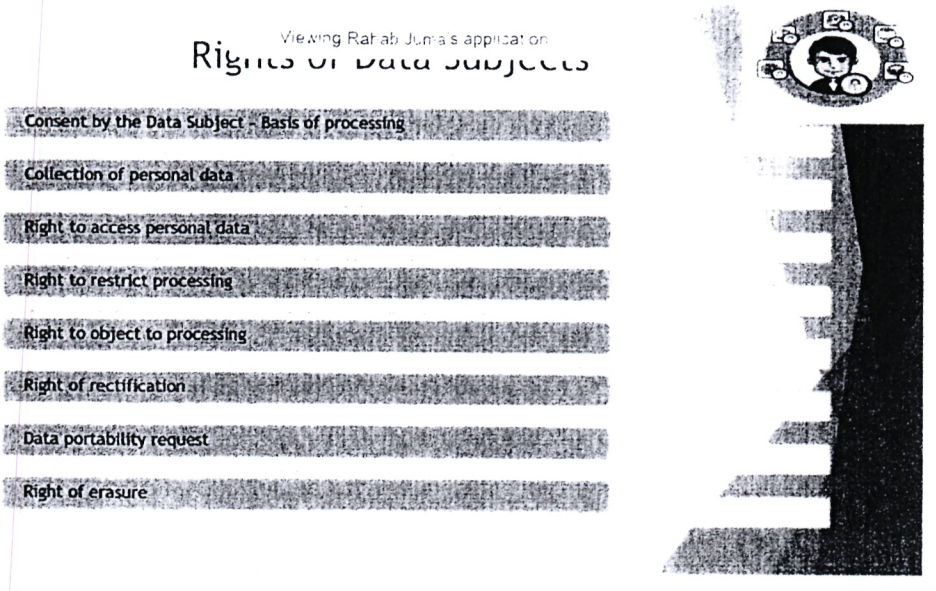
PM Patrice Mutua

Participants 125

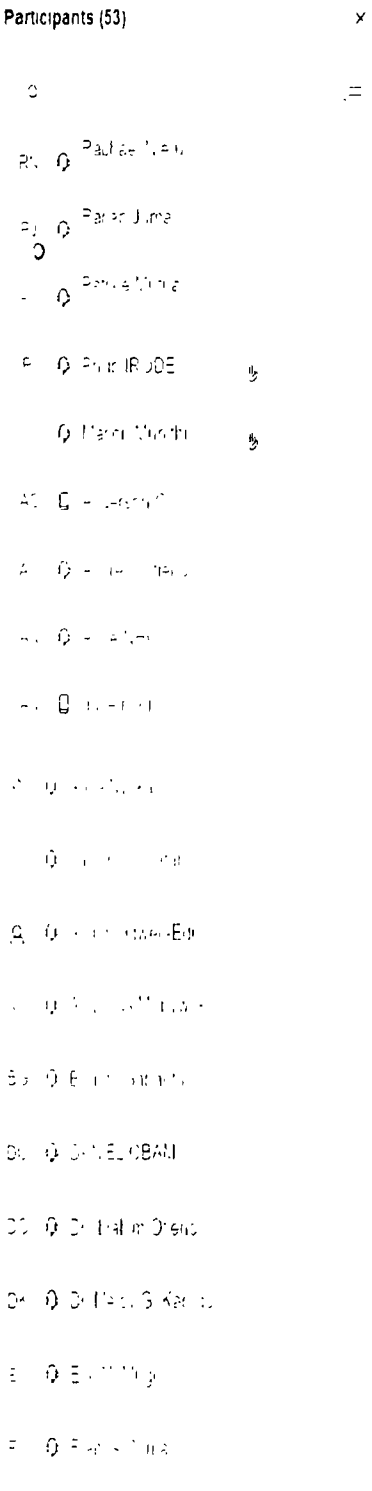
Attendee 107 (9 displayed)

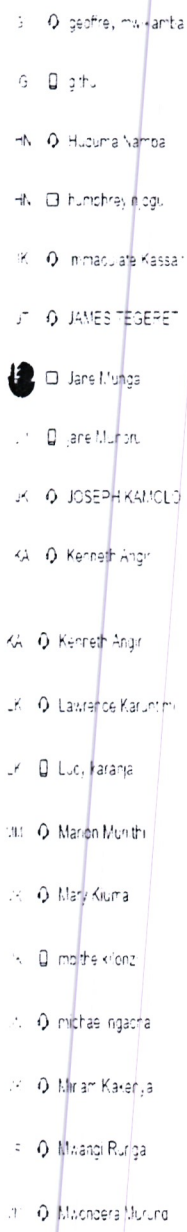
Attendance for the Key Government Entities – Friday, 30th April 2021 From 9-11 Am - Stakeholder consultations on the proposed data protection regulation





Participants (53)




geoffre, mwakamba
githu
Hudume Kamoa
humphrey mogu
immaculate Kassa
JAMES TEGERET
Jane Munga
jane Muroru
JOSEPH KAMOLO
Kenneth Angir
Kenneth Angir
Lawrence Karuri
Luc, Karanja
Marion Munthi
Mary Kiuma
mathe kilonz
michael ngacha
Miram Kaveinga
Mwangi Ruriga
Mwendera Muruno

How is cloud services covered for in data localization

5. Shouldnt the data capture the Criminal Records of the data subjects if applicable? Why capture selectively as opposed to holistic picture?
6. Shouldnt the regulations cite another entity or body to preside over disputes as opposed to Data Commissioner? An independent body with an appelate mechanism ?

What defines security matters in exemption

7. Arent there instances that consent MAY not be sought from the data subject? For example do you consult a criminal

Wanderi: The Security Agencies are defined under the Constitution of Kenya. Therefore, we did not define this under the Act.
2. The Data Protection (Civil Registration) Regulations, 2020 list registrar of marriages, department of immigration and other civil registries in the regulations. Hence they are not captured in the general regulations presented today.

7. In localization, intelligence sharing is the principle factor in eradicating crimes. How will this work ?

3. We note that National Police Service is not a civil registration agency and is addressed under the nation al security organs where exemption n national security are referenced.

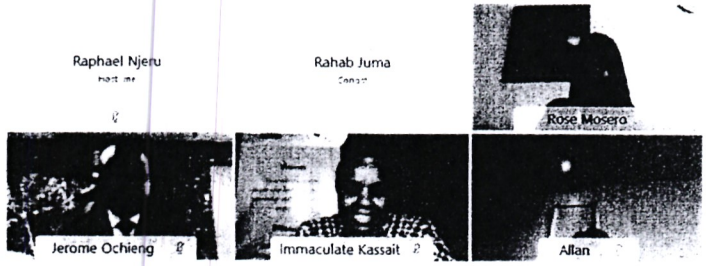
7. In the right to consent, why dont we have exemptions like persons who are unable to make informed decisions?

7. The General Regulations expounds on some matters in tha Act. Section 30 of the Data Protection Act lists 8 lawful purposes for processing personal data. Consent is one of those lawful purposes. However, the rothers such as performance of a mandate by a public authority, protecting other data subjects etc are listed.
8. There is provision given in the Act and General Regulations on obtaining consent from a legal guardian or parent where a person is a minor or lacks capacity to give consent.

I support the need for customised sensitisation of MDAs, especially Ministry of Education which has the National Education Management Information System (NEMIS) where data is captured at school level but there are multiple users, and data sharing APIs

Would you mind sharing the slides with the participants please

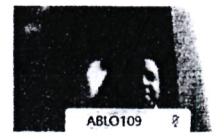
Attendance With the Financial Sector – Monday, 3rd May 2021 From 2-4 Pm - Stakeholder consultations on the proposed data protection regulation



Raphael Njeru

Rahab Juma

miriam ndulu Jubilee



Angela Kikechi

Augustus Munywoki

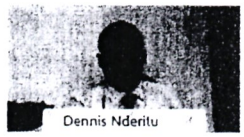
Benjamin Otieno

Benson Wakaba

Brenda Gabantu

Daisy Namayi

David Nguru



Dennis Miano

DERRICK ODUOR OHINDO

Diana

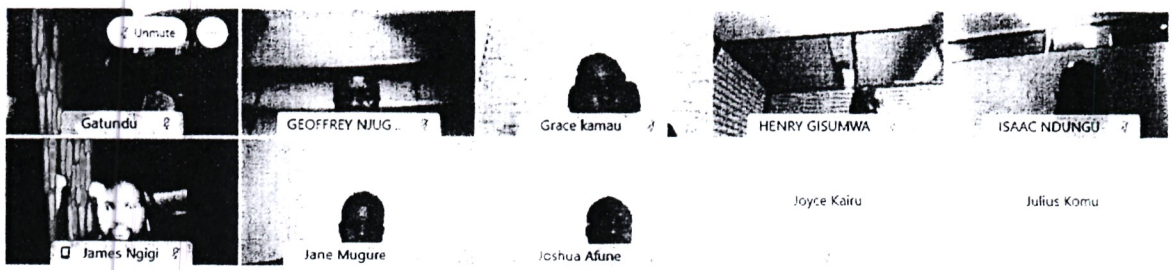
Dickson Maina Njuki

emwandawiro

Gabriel Olango

Gatundu

GEOFFREY NJUGUNA



Joyce Kairu

Julius Komu

Julius Mboya

Ken Kanyarati

Kennedy Karingithi

kmutisya

Lilian

Lilian Simiyu

lynette.k

lynn obwanda

Miriam Kakenya

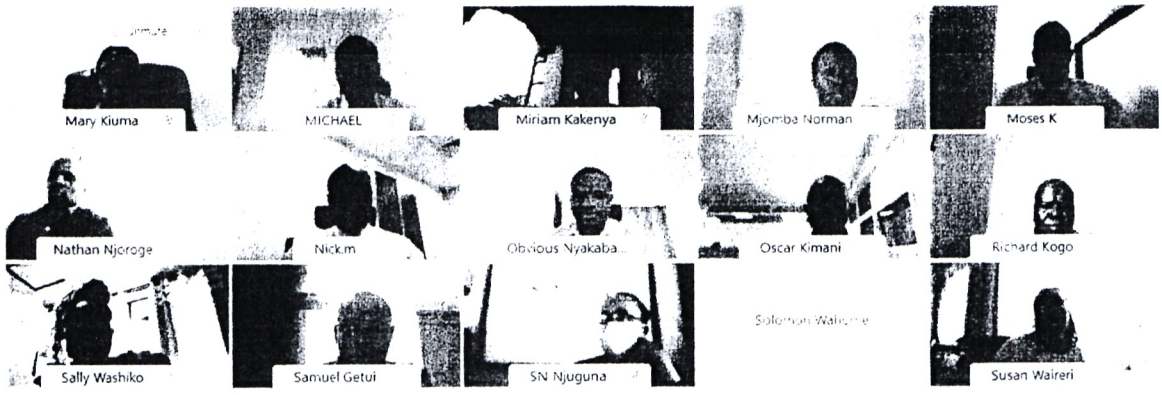
Moses K

Nathan Njoroge

Nick.m

Obvious Nyakabawo

Oscar Kimani



Tari Edward | Thuranira | Titus Sum | Vitalis Oloo | William

Wairimu Njeri Muhuri | Zachary | ABSK429 | Abigael Sungeli | Agnes Mukami

Amos | Angela Mwaniki | Benjamin Kamau | Brenda Mwai | Benjamin Mwai

Benson Wakalia | Bernice | Bethwel | Brian Mwaura | Boniface Kimutai

Brenda Gabantu | Brittah Muthuri | Catherine | Catherine Mbuthia | Chandni Shah

Christopher Ndiritu | Diana Nambafu | Elizabeth Wangechi Ngugi | David Sifuna | David Sieh

David Menza | David Nguru | Dennis Aguinda | Dennis Mwiti | Dennis Nderitu

Dennis Nderitu	Diana	Dickson Maina Njuki	Dorothy Maseke	dtimina
Duncan Kilungu	Duncan Kilungu	Edwin karanja	Elissa	ELIZABETH KANYUA
emwandawiro	ENMuiruri	Enock Munala	Esther Kungu	ESTHER MUENI KALII
Eugene Sanya	Eunice Omolo	Farhiya	Felix kipkulei	Francis Kariuki
Francis Timona	Frankline Obuya	Gabriel Inzoberi	Gabriel Olango	Gabriella Rading
Gatundu	GEOFFREY NJUGUNA	Gideon Okumu	Grace	Grace kamau
Gregory Okwaro	Gulshan Velji	Hannah Wambui	Hazel Kingori	hellen
HENRY GISUMWA	Henry karanja	humphrey njogu	Ian Njoroge Muiru	Immaculate Kassait
Irene Njagi	Isaac	Isaac Murugu	ISAAC NDUNGU	JACINTA ABWOGA
Jackson Kibor	Jackson Njenga	James Ngigi	James Njenga	James Njenga

Meeting information

Meeting topic	Meeting with Financial Sector Ke
Location	moictke.webex.com
Meeting number	183 640 6146
Current host	Raphael Njeru
Current presenter	Rahab Juma
Current user	Raphael Njeru
Current number of partici	254

Participants (250)

Q

EN Eunice Nge

RJ Rahab Juma

SA Said Ali

AW A Wazua

A ABEX 329

AB Abdinasir Songor

A ABEX08

AM Agnes Mukami

AM Alex Manyonde

A Allan

A Allan Jilinde

A Amaan

AS Amos Kipto

AB Andrew B

A Angela

AB Angela Birgen

AK Angela Kikechi

A Anne

AG Anne Gitau

AK ANNE KAMONI

AN Anne Nyokabi

AN Anthony Ndegwa

AN antony Ng'ang'a

AW Antony Wantaigwa

AM Arita Monica

AS Ashmi Shah

A Atandi

AM Augustus Munywoki

BC Beatrice Chelangat

BN beatrice nyagah

BT Beatrice Thumbi

BK Benard Kipkemoi

BN Benedict Njurai

BM Benjamin Maina

BO Benjamin Otieno

BW Benson Wakaba

BI Bernard Itebete

B Bernice

B Bethwel

D Diana

DE diana erukan

DN Dickson Maina Njuki

DO Donald Ouko

DM Dorothy Maseke

D Douglas

D dtimina

DK Duncan Kilungu

E Elissa

EK ELIZABETH KANYUA

EO Elvis Ogall

E EMMA

EO Emmanuel Opakasi

E emwandawiro

E ENMuiruri

EM Enock Munala

EM ERICK MUSAU

EK Esther Kungu

EM ESTHER MUTAHI

ES Eugene Sanya

EO Eunice Omolo

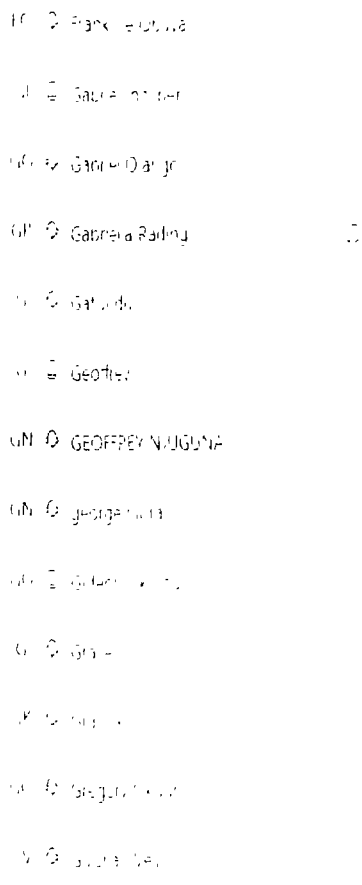
F Farhiya

FK Felix Kipkulei

FN FLORA NJAU

FK Francis Kariuki

FT Francis Timona



HK Hazel Kingori

H hellen

HG HENRY GISUMWA

HK Henry karanja

HN numphrey njogu

IM Ian Njoroge Muiru

IK Immaculate Kassait

IK Immaculate Kassait

IN Irene Nduva

I Isaac

IM Isaac Murugu

IN ISAAC NDUNGU

IA IACINTA ABWOGA

JG Jackson M Githu

JN Jackson Njenga

J James

JK James Kiumbe

JN James Ngig

JN James Njenga

JW James W

JW James Wangombe

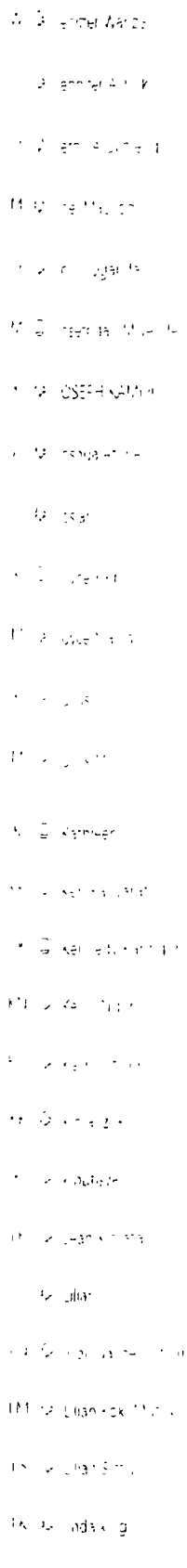
JM Jane Mugure

JM jane Munoru

JN Jane Njenga

J janet

JN Janice Nyokabi



LM Lorna Matindi

LM LUCY MURITHI

LW Lucy Wamatu

LW Lydiah Wangari

L lynette k

LO lynn obwanda

MN Magdalene Nekesa

MW Marion Wanjiku

MM Martin Murithi

MK Mary Kiuma

MM MARY MUMBI

M Matthew

MM Mercy Mayabi

MM Mercy Mayabi

MW Mercy Wambugu

M MICHAEL

MK Miriam Kakenya

M miriam ndulu Jubilee

MN Mjomba Norman

M Morine

MK Moses K

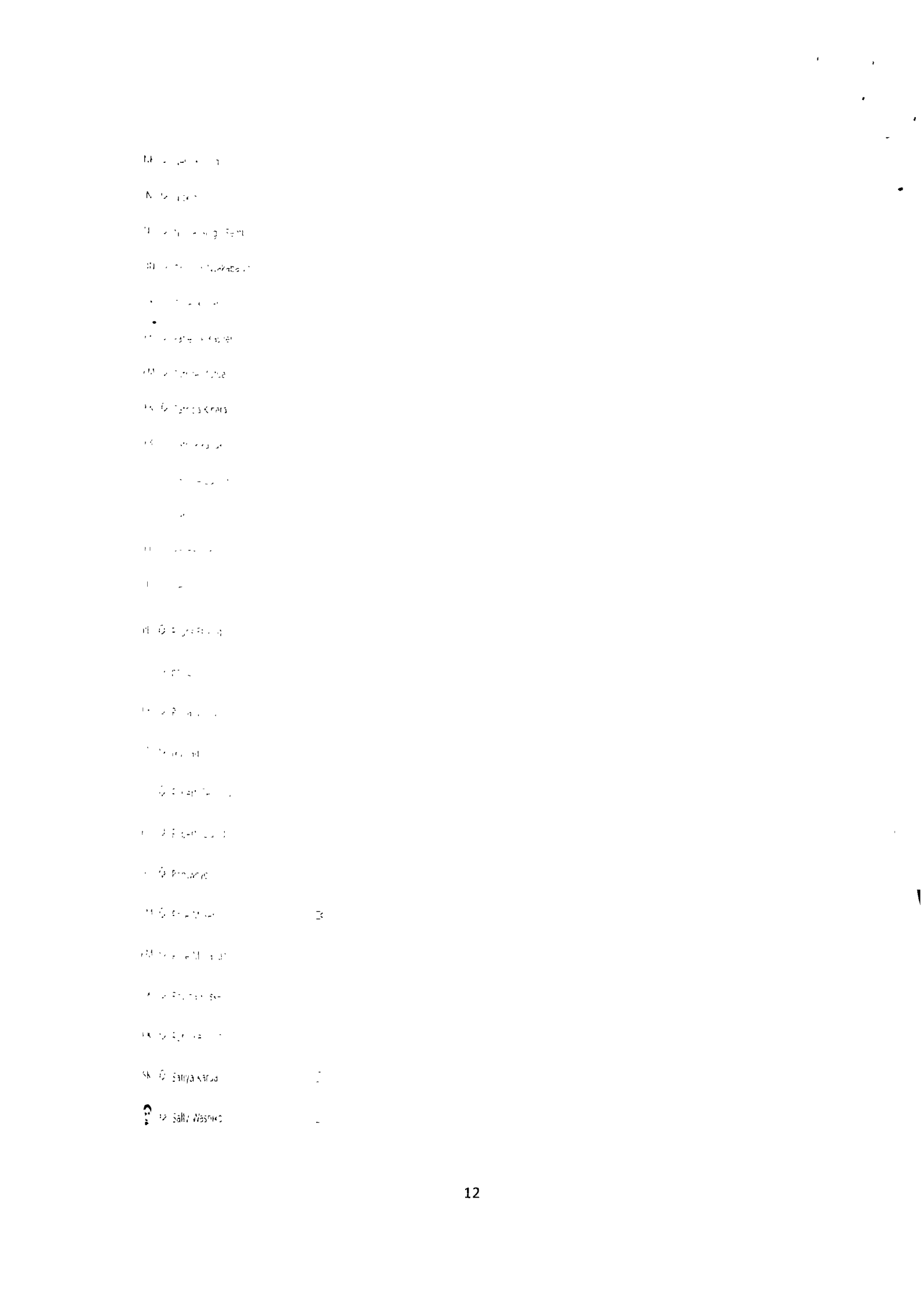
MM mukundpatel mukundpatel

MW mwangi wachira

NS Nancy Situma

NA Nasibo Abdullahi

NN Nathan Njoroge



SK Samantha Kungu

SN Sameera Nanji

SG Samuel Getui

SK SAMUEL KANGETHE

SK Samuel Kariuki

SW Samuel Wainaina

SC Sarah Chepsoi

SA Sauda Ahmed Ali Abdalla

SN Simon Ngura

SN SN Njuguna

SW Solomon Wahome

SM Stanley Mbogo

S stephen

SA Stephen Atenya

SK Stephen Kinyua

SM SUSAN MAINA

SW Susan Warreri

SC sylvia cherotich chelogoi

SI SYMON LARIAK

TN T Nasimiyu

TE Tari Edward

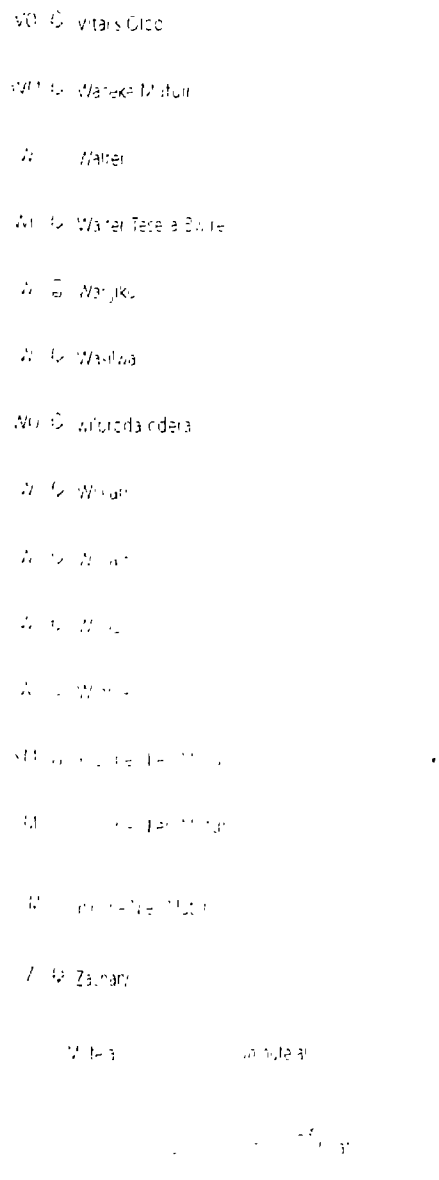
T Thuranira

TS Titus Sum

TM Triza Mathenge

UU undefined undefined

VN Victor B. Nzomo



Chat with the Financial Sector

from Rose Mosero (privately): 2:01 PM

please stop video, so we can start

from Gulshan Velji to everyone: 2:03 PM

Good afternoon. Gulshan Velji - Jubilee Insurance Company Ltd

from Mercy Wambugu to everyone: 2:04 PM

Hello everyone. Mercy Wambugu Faulu Microfinance Bank

from Alex Manyonde (privately): 2:04 PM

Alex Manyonde. Chief Information Officer at ZEP-RE (PTA Reinsurance)

from Nirmal Singh SEMBI (privately): 2:05 PM

Good Afternoon - Nirmal Singh Sembi - IS Auditor - Ecobank Kenya Limited

from Alex Manyonde (privately): 2:05 PM

I dont seem to have option to send chat to everyone

from Samuel Kariuki (privately): 2:05 PM

Good afternoon, Samuel Kariuki - SCB

from JACINTA ABWOGA (privately): 2:09 PM

Good afternoon. Jacinta Abwoga-Development Bank

from Benjamin Maina (privately): 2:11 PM

is there voice? I cant hear the speaker

to Benjamin Maina (privately): 2:12 PM

Yes there is please

from Benjamin Maina (privately): 2:12 PM

Now I am okey.

to Benjamin Maina (privately): 2:12 PM

Karibu sir

from Joel Chesire (privately): 2:12 PM

Afternoon Everyone,Joel Chesire-Jubilee General Insurance Ltd

from Rose Mosero (privately): 2:13 PM

please activate chat with everyone function

to Rose Mosero (privately): 2:13 PM

Done

from Rose Mosero to everyone: 2:14 PM

Welcome All!

from Rose Mosero to everyone: 2:15 PM

Please introduce yourselves on the chat by stating your name, designation and organisation you represent.

from Daisy Namayi to everyone: 2:15 PM

I'm Daisy Namayi, Compliance Manager at DIB Bank Kenya

from Felix kipkulei to everyone: 2:15 PM

Felix Kipkulei

from Joel Chesire to everyone: 2:16 PM

Afternoon Everyone, Joel Chesire-Jubilee General Insurance Ltd

from Lydiah Wangari (privately): 2:16 PM

Lydiah, In Charge of Risk & Compliance at Pacis Insurance

from Alex Manyonde to everyone: 2:16 PM

Hi Everyone. I am Alex Manyonde. Chief Information Officer at ZEP-RE (PTA Reinsurance)

from Anne to everyone: 2:16 PM

Hello. Anne Mureithi. Stanbic Bank.

from Benjamin Maina to everyone: 2:16 PM

Benjamin Maina - Underwriting Manager - Heritage Insurance

from Titus Sum to everyone: 2:16 PM

Titus Sum - Compliance Manager, Standard Chartered Bank

from Calvince to everyone 2.16 PM

Calvince Onduru

Head-Life Operations

CIC Life Assurance

from Rose Muyanga to everyone: 2.16 PM

Rose Muyanga - Kenya Women Microfinance Bank Head of Risk and Compliance

from Nirmal Singh Sembi to everyone: 2.17 PM

Nirmal Singh Sembi

Senior Manager, Information Systems Audit

Internal Audit & Management Services

from Lydiah Wangari to everyone: 2:17 PM

Lydiah, In Charge of Risk & Compliance at Pacis Insurance14

from Matthew to everyone: 2:17 PM

Good afternoon, Matthew Kimweli - Jubilee General Insurance Limited

from Sameera Nanji to everyone: 2:17 PM

Sameera Nanji, Head of Operations, Jubilee Life Insurance Limited

from Dennis Nderitu to everyone: 2:17 PM

Dennis Nderitu - Ag. Head of Ops Faulu Microfinance

from emwandawiro to everyone: 2:17 PM

Edgar Mwandawiro, CRO SBM Bank

from ABLO109 to everyone: 2:17 PM

Good afternoon all. Laban Omangi from Absa Bank and also Chairman Kenya Bankers Association Compliance Committe.

from Samuel Getui to everyone: 2:17 PM

Samuel Getui. Data processing UAP Oldmutual group

from Pauline Gathuri to everyone: 2:17 PM

Pauline Gathuri - Association of Kenya Insurers

from linda koigi to everyone: 2:18 PM

Good Afternoon all. Linda Koigi - BRITAM Insurance { Head of Legal Gen Insurance}

from SN Njuguna to everyone: 2:18 PM

Susan Njuguna - KWFT

from Francis Kariuki to everyone: 2:18 PM

Francis Kariuki, Diamond Trust Bank Kenya Limited

from Dennis Miano to everyone: 2:18 PM

Miano Dennis - East Africa Reinsurance Company Limited

from Eugene Sanya to everyone: 2:18 PM

Eugene Sanya , ICT Manager, AAR Insurance Kenya Ltd

from Chandni Shah to everyone: 2:18 PM

Chandni Shah Bank of India Risk and Compliance

from Dennis Agunda to everyone: 2:18 PM

Dennis Agunda - Bank of Africa

from Nasibo Abdullahi to everyone: 2:18 PM

Nasibo Abdullahi-Victoria Commercial Bank

from Joshua Afune to everyone: 2:18 PM

Hello, Joshua Afune - Group Head of Compliance, Britam Holdings Plc

from Waceke Mutuiri (privately): 2:18 PM

Susan Mutuiri - Britam GI

from Jackson Njenga to everyone: 2:18 PM

Jackson Njenga- Credit Bank Plc

from Duncan Kilungu to everyone: 2:18 PM

Duncan Kilungu - UAP Insurance Co. Ltd

from Angela Birgen to everyone: 2:18 PM

Angela Birgen, Risk & Compliance Officer - Pacis Insurance Ltd.

from Kennedy Karingithi to everyone: 2:18 PM

Kennedy Karingithi Internal Audit DTB

from Joshua Afune to everyone: 2:18 PM

Hello, Joshua Afune - Group Head of Compliance, Britam Holdings Plc

from David Nguru to everyone: 2:18 PM

Good afternoon all. David Nguru Pioneer Assurance Company Limited Claims head.

from Allan to everyone: 2:18 PM

Allan Mwangi SBM Bank

from Richard Kogo to everyone: 2:18 PM

Good afternoon. Richard Kogo -East Africa Re -Finance

from ENMuiruri to everyone: 2:18 PM

Good Afternoon all, Esther Muiruri - Salvage Administrator and Claims Analyst - UAP Old Mutual

from Isaac Murugu to everyone: 2:18 PM

Isaac Murugu, Risk & Compliance, Madison Group

from mukundpatel mukundpatel to everyone: 2:18 PM

Mukund Patel - Victroria Commercial Bank Ltd.

from Bethwel to everyone: 2:19 PM

Good Afternoon, Bethwel Cheuiyot- Risk& Compliance-East Africa Reinsurance Cl Ltd

from Grace kamau to everyone: 2:19 PM

Graceanne Kamau -Head of Risk and Compliance, AAR Insurance Kenya

from Joyce Kairu to everyone: 2:19 PM

Hello Everyone, Joyce Kairu-Risk and Compliance at UAP Old Mutual Group

from Samantha Kungu to everyone: 2:19 PM

Samantha Kung'u - Ecobank Kenya Ltd

from Dickson Maina Njuki to everyone: 2:19 PM

Dickson Maina Njuki, Ciso, Sidian Bank

from lynette.k to everyone: 2:19 PM

Goodafternoon. Lynette Kamande- Head Legal Mayfair CIB Bank Ltd

from Ian Njoroge Muiru to everyone: 2:19 PM

Ian Njoroge, Risk & Compliance - Mayfair Insurance Company Ltd

from James Njenga to everyone: 2:19 PM

James Njenga - DPO - I&M Bank Limited

from Jeniffer Wanza (privately): 2:19 PM

Hi Everyone,

from Henry karanja to everyone: 2:19 PM

Henry Karanja, Head Compliance Coopertiave Bank of Kenya

from hellen to everyone: 2:19 PM

Hellen Omiti - Machora GM-Legal, GA Insurance Limited

from Susan Waireri to everyone: 2:19 PM

Susan Waireri, Legal, UAP Old Mutual

from Edwin karanja (privately): 2:19 PM

Edwin Karanja- Kenyan Alliance Insurance.

from David Kieti to everyone: 2:19 PM

David Kieti - Head, ICT Kingdom Bank LTD

from Julius Mboya to everyone: 2:19 PM

Julius Mboya - ICT Manager, Fidelity Insurance

from Francis Timona to everyone: 2:19 PM

Francis Timona, AAR Insurance

from Teresa Babua (privately): 2:19 PM

Teresa Babua, Compliance - DIB Bank Kenya Ltd

from stephen to everyone: 2:19 PM

stephen wales - internal audit -M Oriental Bank

from Gabriella Rading (privately): 2:19 PM

Hello, Gabriella Rading -Prudential Life Assurance Kenya Ltd.

from Kevin Otieno (privately): 2:19 PM

Good afternoon all, Kevin Otieno Jubilee Health Insurance

from Moses K to everyone: 2:19 PM

Hello good people, Am Moses Kariuki, I head the Risk and Compliance Division at Kingdom Bank (formerly Jamii Bora Bank).

from SYMON LARIAK to everyone: 2:20 PM

Symon Lariak-Ass.Manager Legal-GA Insurance Ltd,

from Ashmi Shah (privately): 2:20 PM

Ashmi Shah, Risk and Compliance Officer - Prudential Life Assurance Kenya Limited

from James Ngigi to everyone: 2:20 PM

James Ngigi, Head ICT, Jubilee Life

from dtimina to everyone: 2:20 PM

Dorothy Timina - Head Data & Analytics Co-operative Bank

from HENRY GISUMWA to everyone: 2:20 PM

Henry Gisumwa - Manager UAP OLDMUTUAL Insurance co. Ltd.

from William to everyone: 2:20 PM

William Thiong'o-Internal Audit, GA Insurance

from Nelly Kirongo to everyone: 2:20 PM

Nelly Kirongo, Risk & Compliance, Development Bank of Kenya

from Catherine Mbuthia to everyone: 2:20 PM

Catherine Mbuthia - Compliance Officer - Jubilee Insurance Ltd

from Felix kipkulei to everyone: 2:21 PM

Felix Kipkulei, Undewriting Department ,Kenyan Alliance Insurance Company

from lynn obwanda (privately): 2:21 PM

Good Afternoon, participants are also from the insurance industry

from Oscar Kimani (privately): 2:21 PM

Oscar Kimani - Data Governance, Absa Bank Kenya

from Ashmi Shah to everyone: 2:21 PM

Ashmi Shah, Risk and Compliance Officer - Prudential Life Assurance Kenya Limited

from Joel Machogu to everyone: 2:21 PM

Joel Machogu - Risk & Compliance, Credit Bank

from Ken Kanyarati to everyone: 2:21 PM

Ken Kanyarati-Regional Head of Compliance-Stanbic Bank Limited

from Amaan to everyone: 2:22 PM

Amaan Kassam - Legal. Diamond Trust Bank (K) Ltd

from Arita Monica to everyone: 2:22 PM

Arita Monica, Risk and Complinace, Saham Assurance

from Elissa to everyone: 2:22 PM

Elissa Otemba-Legal Officer Co-operative Bank Ltd

from Benedict Njurai to everyone: 2:22 PM

Benedict Njurai, Risk and Compliance at UAP OM Group

from Sauda Ahmed Ali Abdalla (privately): 2:23 PM

Sauda Ahmed- Ga Insurance Ltd.

from Antony Wantaigwa (privately): 2:23 PM

Anthony Wantaigwa, Claims ICEA LION General

from Joyce Maina (privately): 2:23 PM

Joyce Maina- Compliance Sidian Bank

from Lilian to everyone: 2:23 PM

Lilian Machanga -Internal Audit - Geminia Insurance

from Nathan Njoroge to everyone: 2:24 PM

Good afternoon Everyone! Nathan Njoroge Kihungi - General Counsel, Citibank, N.A. Kenya.

from David Kiboi (privately): 2:24 PM

David Kiboi; Jubilee Insurance - Forensic Security Services

from Tari Edward to everyone: 2:24 PM

Tari Edward - Underwriting Icea Lion Gen Ins.

from Lilian Koki Mutiso to everyone: 2:25 PM

Lilian Mutiso-Assistant Claims Manager-UAP Oldmutual

from Jeniffer Wanza (privately): 2:26 PM

Jeniffer Wanza,Libertylife

from ELIZABETH KANYUA to everyone: 2:27 PM

Elizabeth Kanyua- Underwriting Uap Old Mutual

from data protection regulations stakeholders to everyone: 2:27 PM

Lawrence Simiyu-THE MONARCH INSURANCE CO.LTD

from David Menza (privately): 2:27 PM

David Menza - HF Group

from kmutisya to everyone: 2:28 PM

Hi. I am Kennedy Mutisya Representing Kenya Bankers Association

from T. Nasimiyu to everyone: 2:28 PM

Teresia Nasimiyu - Claims ICEALION Gen Ins

from Rovina Koske to everyone: 2:28 PM

Rovina Koske - APA Insurance

from data protection regulations stakeholders to everyone: 2:30 PM

Hie,i'm Mr.Lawrence Simiyu-(National Check-off Coordinator-Life Division) THE MONARCH INSURANCE COMPANY LTD

from linda koigi to everyone: 2:32 PM

How about if this personal data is anonymised? If the products are for a particular cohort?

from Lilian Koki Mutiso (privately): 2:39 PM

You're breaking up We can't hear you

from James (privately) 2 40 PM

I cant hear you

from ABLO109 to everyone: 2:42 PM

Thuranira- What about sharing within a group crossborder?

from ESTHER MUENI KALII (privately): 2.46 PM

Esther Kalii -Uap Old Mutual Group

from Gulshan Velji to everyone: 2:48 PM

Does anonymisation apply to transactions the data subject is seeking to make with the financial institution?

from Gulshan Velji to everyone: 2:48 PM

If so, how will this work with regards to the POCAMLA Act that requires us to identify and verify identity of the data subject (this includes all KYCs - personal data)

from emwandawiro to everyone: 2:49 PM

Thuranira, please clarify is sharing of personal customer data withing banking groups or branches or entities is allowed

from Gulshan Velji to everyone: 2:50 PM

Please also clarify on sharing of personal data with Third Parties for the fulfilment of the contract with the data subject

from James (privately): 2:53 PM

James Pamba - Kenindia Assurance Company Ltd

from Titus Sum to everyone: 2:54 PM

Should the country have all the 3 requirements or atleast 1?

from Rose Mosero to everyone: 2:54 PM

@Gulshan, the matter of anonymisation only comes into effect as a methos of erasure. If your institution is still transacting with a customer, you may wish to apply pseudonymisation to protect the data from unauthorised disclosure. However, the provision of POCAMLA still apply.

from Ken Kanyarati to everyone: 2:55 PM

All 3 or at least 1 of the requirements-regarding considerations for countries with appropriate safeguards?

from Rose Mosero to everyone: 2:56 PM

The General Regulations state that sharing of personal data within the same organisation is not deemed as "data sharing".

from Rose Mosero to everyone: 2:57 PM

Issues of data sharing to third parties will require that their are binding contractual obligations on the third party to offer the same safeguards as a data controller or data processor is obligated to have under the data protection laws.

from Rose Mosero to everyone: 2:58 PM

@Ken Kanyarati: one of the three suffices

from Gulshan Velji to everyone: 3:00 PM

What is the strategy the Data Commissioner is exercising in the acquisition of consents especially for existing clients. Will there be a time frame allowed for collection of the consent?

from David Nguru to everyone: 3:01 PM

On setting timelines for a period a company can hold personal data, we would like to know if the act provides maximum timelines because if a claim remain unsettled for more than even 30 years, ultimately insured or beneficiary should be paid. We know unclaimed Assets regulation requires that unpaid claims for 2 years after maturity be passed to UFA, however even after passing such cases to the Authority, if a customer claim with UFA 40 or even 60 years later, currently UFA requires a submission letter from the forwarding company. Therefore should a personal data on the data subject have been destroyed, then such data subject would have been denied benefits they deserve.

from Gulshan Velji to everyone: 3:04 PM

Requirement is that sensitive personal data should be collected directly from the data subject, for Insurers this may not be feasible since data is generally from third parties like intermediaries and health care providers.

from James Ngigi to everyone: 3:05 PM

Please clarify on when data is shared as a medium of storage or transfer/communication. eg. AWS as data backup, Safaricom as a medium of communication, bulk sms providers etc.

from Dorothy Maseke to everyone: 3:05 PM

Thuranira/Rose - So to carry out a DPIA it needs to be approved by the Data Commissioner and there is a fee of Kshs 15,00 charged for each DPIA? Please clarify?

from Gulshan Velji to everyone: 3:06 PM

No mention of whether the respondents shall be notified of all complaints lodged against them. Will they be notified for all or only those that have been admitted only?

from ESTHER MUENI KALII to everyone: 3:06 PM

Esther Kalii -Uap Old Mutual Group

from Gulshan Velji to everyone: 3:07 PM

Where the contracting party is a corporate insuring its staff for life or medical, is there a requirement to get consents from each employee and/or dependent under the corporate policy.

from Bethwel to everyone: 3:09 PM

What constitutes data subject's consent when it comes to reinsurance companies who deal with insurance companies directly and not the data subjects, in such a case then, can consent be implied?

from Dorothy Maseke to everyone: 3:11 PM

14(2) indicates that " Where parties to a complaint agree to negotiation, mediation or conciliation, the Office shall in consultation with the parties facilitate the process." This may be limiting. Does the commissioner have to faciliate this? Perhaps consider allowing an independent means for this process i.e. enable this to be settled between the complainant and the insitution without necessarily having the commissioner faciltate this process.

from Gulshan Velji to everyone: 3:11 PM

law and everyone is getting to understand it, isnt KShs. 10K per day not high?

from Rose Mosero to everyone: 3:12 PM

@Dorothy, the next presenter on registration will touch on the fees.

from Rose Mosero to everyone: 3:13 PM

@Gulshan, the draft Enforcement and Complaints regulations in reg. 11 set out procedure for notification to a respondent that a complaint has been made against it

from Rose Mosero to everyone: 3:15 PM

@ Bethwel, Consent can be obtained by the insurer. The Insurer must ensure that it lists any reinsurer as a possible third party that personal data will be shared with and the reasons.

from Gulshan Velji to everyone: 3:16 PM

Insurance agents deal with personal information which they collect through the quotation requests/application forms - will they be able to afford to meet the registration requirements of this law?

to Josiah (privately): 3:16 PM

We can mute our videos and activate during the group photo please

to Donald Ouko (privately): 3:17 PM

We can mute our videos and activate during the group photo please

to Douglas (privately): 3:18 PM

We can mute our videos and activate during the group photo please

to Beatrice Thumbi (privately): 3:18 PM

We can mute our videos and activate during the group photo please

from Benjamin Otieno to everyone: 3:21 PM

Certification of the copies of the certificate to be displayed in the branches seem to lengthy and uneccessary exercise. Can the DC come up with some other way of dealing with this?

from James Ngigi to everyone: 3:22 PM

which certifications?

from Dorothy Maseke to everyone: 3:23 PM

Being a regulator, why charge institutions for a compliance audit? Struggling to understand that. 250K for certification is extremely high. Once certified is it perpetual?

from Benjamin Otieno to everyone: 3:23 PM

Certified copy of registration certificate

from Donald Ouko to everyone: 3:23 PM

What is the relevance of this Certification Fee of KES 250,000?

from Dorothy Maseke to everyone: 3:23 PM

The fees seem extremely high to be honest. Comparing with other regulatory fees that we pay. Any reason for this?

from Dorothy Maseke to everyone: 3:25 PM

Considering annual renewal fees, and all those other charges. I can only imagine the number of DPIAs a data intensive insitution may need to do. Perhaps reconsider those charges.

from Titus Sum to everyone: 3:31 PM

Are the Guidance notes published on the ODPC website (specifically on Consent) Final and how do they link with the draft regulations?

from Susan Waireri to everyone: 3:35 PM

The Data Protecton Act enshrines other lawful basis for the processing of Personal Data other than consent. The Regulations do not expound on these lawful basis. Do we still have to rely on consent for processing even where there is another lawful basis applicable such as performance of contract or legal obligations?

from Amos Kiptui (privately): 3:39 PM

Where a company has a subsidiary (s), should they parent company register on behalf of the subsidiaries or they have to be registered independently?

from Amos Kiptui to everyone: 3:40 PM

Where a company has a subsidiary (s), should they parent company register on behalf of the subsidiaries or they have to be registered independently?

from Douglas to everyone: 3:53 PM

WIll you have guidance on Accountability requirements by the Data Controller and Data Processors. As a regulator what are your expectations towards us in as far as this principle of Accountability in all obligations is concerned?

from Mercy Wambugu to everyone: 3:56 PM

Are there timelines for compliance and if so when

from Amos Kiptui to everyone: 3:57 PM

What are the timelines for compliance?

from Julius Mboya to everyone: 3:58 PM

If I am a systems vendor and have offered ERP systems to X clients that capture and process personal data. In the process of support, I have access to the data of my clients subject to existing controls, do I have to register with the DC?

from antony Ng'ang'a to everyone: 4:00 PM

Can the registration certificate be certified by an Advocate or does it have to certified by the commission? If yes, why?

from Stephen Kinyua to everyone: 4:01 PM

Can a company register as both a Data Controller and Data Processor? Insurance companies from the diefinition of the act can be categorized under both. Please clarify on this.

from Yvonne Njeri Muturi to everyone: 4:01 PM

Greetings All. I did not introduce myself on the chat earlier - Yvonne Njeri Muturi, Head of Compliance, Citibank East Africa

from Rose Muyanga to everyone: 4:02 PM

Apologies..have to exit.

from Benjamin Otieno to everyone: 4:02 PM

I asked a question on the need to have the registration certificate certified by the DC. Can it be certified by some other person other than the DC?

from linda koigi to everyone: 4:02 PM

is the DPIA still valid if it does not go through the office of the data comissioner?

from Daniel to everyone: 4:03 PM

Requirements of the regulations will require process and system enhancements. Will there be a Grace period to allow for this?

from Patrick kariuki to everyone: 4:05 PM

CBK has been requesting DPIAs for all new technology driven products leveraging on BOTs and AI. Additionally third parties providing funding for banks also request for DPIAs. Do all DPIAs have to go through the ODPC?

from Kennedy Karingithi to everyone: 4:07 PM

Do banks need to carry out Data protection Impact Assessment on data processing on activities they have been processing before the enactment of the DPA?

from Stephen Kinyua to everyone: 4:09 PM

Can a company register as both a Data Controller and Data Processor? Insurance companies from the diefinition of the act can be categorized under both. Please clarify on this.

from Patrick kariuki to everyone: 4:14 PM

The consent to share the data to the insurance company should be captured in the employee contract during onboarding if that benefit is being offered by the company to the employee

from linda koigi to everyone: 4:15 PM

please clarify on the issue of DPIA, the fee of 15,000 per assement what is this in regrard to? does this mean the commissioners office is carrying out this assesment?

Event Count	Event Name	Invited	Registered	Attended	Absent	Date & Time	
1	Meeting Registration Test Meeting at 10: 15 Am	0	2	2	0	April 20, 2021 10:32 am Nairobi Time	
2	Public Participation Forum - Tuesday 27th April 2021(2pm-4pm)- Stakeholder consultations on proposed Data Protection Regulation	23	436	308	134	April 27, 2021 4:38 pm Nairobi Time	
3	Public Participation Forum-Wednesday 28thApril 2021(2pm-4pm) on Stakeholder consultations on proposed Data Protection Regulation	0	282	212	70	April 28, 2021 5:37 pm Nairobi Time	
4	Test Public Stakeholder Consultations on the proposed Data Protection Regulation, 2021	0	7	4	3	April 20, 2021 1:09 pm Nairobi Time	