



LEGAL NOTICE NO.....

**THE DATA PROTECTION ACT, 2019**

*(No. 24 of 2019)*

**THE DATA PROTECTION (CIVIL REGISTRATION) REGULATIONS, 2020.**

**ARRANGEMENT OF REGULATIONS**

*Regulation*

**PART I—PRELIMINARY**

- 1—Citation.
- 2—Interpretation.
- 3—Scope of the Regulations.

**PART II—DATA PROTECTION PRINCIPLES**

- 4—Lawful processing of personal data.
- 5—Privacy in processing of personal data.
- 6—Consent.
- 7—Manner of giving consent
- 8—Collection of personal data.
- 9—Limitation in processing of personal data.

**PART III—RIGHTS OF A DATA SUBJECT**

- 10—Access to personal data.
- 11—Rectification of personal data.
- 12—Objection to processing of personal data.
- 13—Data portability request.
- 14—Exercise of data subject rights by others.
- 15— Personal data relating to a child.

**PART IV—OBLIGATION OF THE CIVIL REGISTRATION ENTITIES**

- 16—Duty to notify.
- 17—Retention of personal data.
- 18— Notification of breach of personal data.
- 19—Data protection impact assessment.
- 20— Responsibilities of a Data Protection Officer.
- 21—Sharing of personal data.
- 22—Automated individual decision-making
- 23—Internal complaints handling procedure.

**PART V—SECURITY SAFEGUARDS**

- 24—Data protection by design or default.
- 25—Security safeguards of personal data.
- 26—Database security.
- 27—Monitoring by the Data Commissioner.
- 28—Data security procedure.
- 29—Database systems and risk assessment.
- 30—Physical protection and secure surroundings.
- 31—Data security in manpower management.

- 32—Access permission management.
- 33—Monitoring and documenting access.
- 34—Documentation of security incidents.
- 35—Network security.
- 36— Periodical audits.
- 37—Data backup and restoration.
- 38—Transfer of personal data outside Kenya.

**PART VI—MISCELLANEOUS PROVISIONS**

- 39—Reports to the Data Commissioner.
- 40—Outsourcing.

**SCHEDULE—FORMS**

**FOR PUBLIC ENGAGEMENT**

**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 and Technology makes the following Regulations—

**THE DATA PROTECTION (CIVIL REGISTRATION)  
REGULATIONS, 2020**

**PART I—PRELIMINARY**

Citation.           **1.** These Regulations may be cited as the Data Protection (Civil Registration) Regulations, 2020.

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

“Act” means the Data Protection Act, 2019;

“authorized user” means an officer or employee of the civil registration entity who is expressly permitted to access the civil registration entity’s database and database system;

“biometric data” has the meaning assigned to it under the Act;

“civil registration” means the continuous permanent, compulsory and universal recording of the occurrence and characteristics of vital events to the population including registration of births, adoption, marriage and death;

“civil registration entity” means a public agency responsible for administering laws under regulation 3, and includes—

(a) the National Registration Bureau;

(b) the Civil Registration Service;

(c) the Registrar of Marriages;

(d) the Department of Immigration;

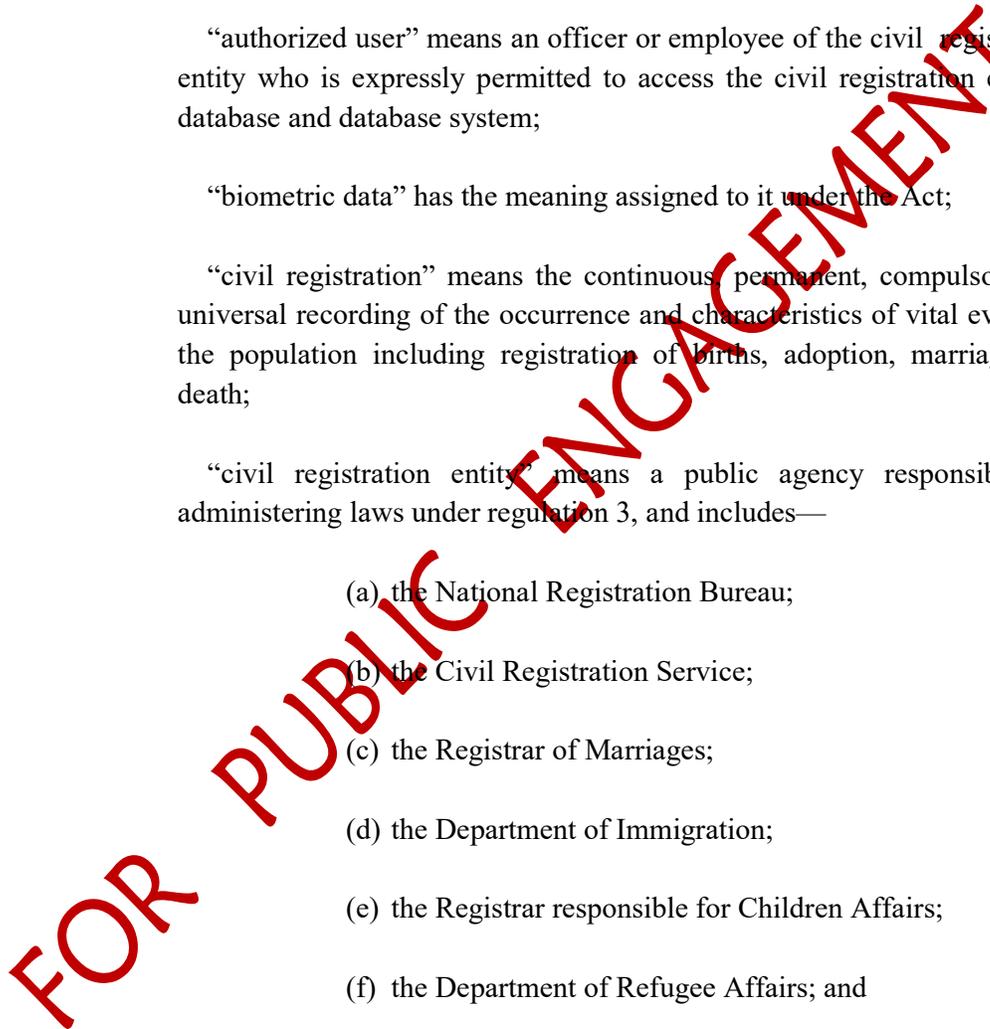
(e) the Registrar responsible for Children Affairs;

(f) the Department of Refugee Affairs; and

(g) the Principal Secretary responsible for the National Integrated Identity Management System database.

“child” has the meaning assigned to it under the Children Act, 2001;

“database” includes personal data stored by the civil registration entity;



“database system” means a software serving the database;

“data controller” means the Principal Secretary for the time being responsible for civil registration;

“Data Commissioner” has the meaning assigned to it under of the Act;

“National Security Council” means the National Security Council established under Article 240 (1) of the Constitution.

Scope of the Regulations

**3.** These Regulations shall apply to a civil registration entity involved in the processing of personal data relating to—

- (a) registration of births;
- (b) registration of adoptions;
- (c) registration of person;
- (d) issuance of passport and other identity documents;
- (e) registration marriages; or
- (f) registration deaths.

**PART II—DATA PROTECTION PRINCIPLES**

Lawful processing of personal data.

**4.** The processing of personal data is lawful, if undertaken pursuant to the following laws—

Cap 107.

Cap 149.

No. 12 of 2011.

No. 4 of 2014.

No. 8 of 2001.

No. 13 of 2006.

- (a) the Registration of Persons Act;
- (b) the Births and Deaths Registration Act;
- (c) the Kenya Citizenship and Immigration Act;
- (d) the Marriage Act;
- (e) the Children Act; and
- (f) the Refugee Act.

Privacy in processing personal data.

5. A civil registration entity shall ensure—

- (a) access to the data in its system is by authorized users;
- (b) the data processing system has adequate technical and procedural safeguards for processing personal data;
- (c) the data subject is provided with the necessary information relating to their personal data;
- (d) the personal data being processed is verified; and
- (e) compliance to the code of conduct relating to confidentiality, privacy and security guidelines as specified by the Data Commissioner from time to time.

Consent.

6. (1) A civil registration entity shall seek consent from a data subject for processing of personal data at the time the personal data is collected.

(2) A civil registration entity shall, before processing personal data, inform the data subject—

- (a) the type of personal data to be processed;
- (b) the magnitude of personal data to be processed;
- (c) the reasons for the processing the required personal data; and
- (d) whether the personal data processed shall be shared with third parties.

(3) A civil registration entity shall obtain consent from the data subject while ensuring that —

- (a) the data subject is informed in a language they understand;
- (b) the data subject voluntarily gives consent;
- (c) consent is specific; and

(d) the data subject has capacity to understand and communicate their consent.

(4) A civil registration entity shall obtain the consent in physical or electronic form.

Manner of giving consent.

7. (1) Consent shall be given either orally or in writing and may include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

(2) A civil registration entity shall not presume that a data subject has given consent on the basis that the data subject did not object to a proposal to handle personal data in a particular manner.

(3) Consent shall not be implied, where the intention of the data subject is ambiguous or there is reasonable doubt as to the intention of the data subject.

(4) Subject to section 32 (2) and (3) of the Act, the data subject shall be informed of the implications of providing, withholding or withdrawing consent by the civil registration entity.

Collection of personal data

8. (1) A civil registration entity shall have regard to the following during the 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; and,

(c) undertake processes to secure personal data.

(2) Where a civil registration entity intends to use personal data for a new purpose, it shall ensure that the new purpose is compatible with the initial purpose.

Limitation of processing personal data in of

9.(1) A data subject may request a civil registration entity to restrict the processing of their personal data, pursuant to section 34 of the Act.

(2) A request envisaged under paragraph (1) shall be in Form 5 set out in the First Schedule.

(3) A civil registration entity shall upon receiving the request envisaged under paragraph (2)—

- (a) consider the restriction request;
- (b) respond in writing to the data subject within fourteen days from the date of receiving the restriction request;
- (c) indicate on its system that the processing of personal data has been restricted; and
- (d) notify any relevant third party where personal data subject to such restriction may have been shared.

(4) Where a civil registration entity declines to comply with a request for restriction in processing, it shall notify the data subject of such decline giving reasons for the decision.

### PART III—RIGHTS OF A DATA SUBJECT

Access to personal data

**10.** (1) The civil registration entity shall provide access to the data subject to personal data in its possession.

(2) A data subject may request access to personal data held by a civil registration entity.

(3) A civil registration entity shall put in place electronic or manual mechanisms to enable a data subject to access their personal data.

(4) A data subject shall make a request to access personal data in Form 2 set out in the First Schedule, and upon payment of the requisite fee.

Rectification of personal data

**11.** (1) Pursuant to section 40 of the Act, a data subject may request a civil registration entity to rectify their personal data which is inaccurate, outdated, incomplete or misleading.

(2) A request for rectification envisaged under paragraph (1) shall be made in Form 2 set out in the First Schedule.

(3) An application made for rectification of personal data shall be supported by the necessary documents.

(4) A rectification request shall include sufficient detail to enable the civil registration entity to identify —

- (a) the data subject making the request;
- (b) the personal data requested;
- (c) the rectification requested by the data subject;
- (d) the information useful to warrant the rectification; and
- (e) the justification for rectification of the personal data.

(5) A civil registration entity shall rectify an entry of personal data in the database where the civil registration entity is satisfied that a rectification is necessary.

(6) A civil registration entity shall in writing notify the data subject of its objection to rectify the personal data where such data is required as envisaged under section 40 (3).

(7) In case of any change in personal data in possession of the civil registration entity, the data subject shall notify the civil registration entity to update their personal data.

(8) The civil registration entity may decline rectification of personal data and shall in writing provide reasons thereto.

(9) Where rectification of personal data has been denied by the civil registration entity, the data subject may, where dissatisfied with the decision of the civil registration entity lodge a complaint with the Data Commissioner.

Objection to processing of personal data.

**12.** A data subject who objects to the processing of personal data pursuant to section 26 (c) of the Act, shall submit the application to the civil registration entity in Form 1 set out in the First Schedule.

Data portability request

**13.** A civil registration entity shall upon request in writing by the data subject, provide the data subject with their personal data in a structured,

commonly used and machine readable format and upon payment of the required fees.

Exercise of data subject rights by others.

**14.** (1) Subject to section 27 of the Act, where a person duly authorized by the data subject seeks to exercise the right of a data subject on their behalf, the person exercising that right shall take into consideration the best interests of the data subject.

(2) Where a person seeks to exercise the right of a data subject under paragraph (1), the civil registration entity shall presume the existence of the relationship between the person and the data subject unless evidence to the contrary is adduced.

(3) Despite paragraph (2), where evidence to the contrary is adduced, the civil registration entity shall halt the request of exercising a right on behalf of the data subject and any further processing of personal data, until the civil registration entity is satisfied.

(4) Where the right is being exercised on behalf of a minor, the persons exercising that right shall—

- (a) produce a Birth Certificate;
- (b) an Adoption Certificate;
- (c) court Order; or
- (d) any other relevant document.

Personal data relating to a child.

**15.** (1) When processing personal data relating to a child, the civil registration entity shall ensure—

- (a) consent is given by the child's parent or guardian; and
- (b) processing is done lawfully and safeguards the best interest of the child.

(2) When processing personal data relating to a child, the a civil registration entity shall—

- (a) restrict access to personal data relating to a child;
- (b) ensure it has design systems and processes that safeguard the best interest of the child; and
- (c) ensure the risks and consequences of the processing are identified, and age appropriate safeguards are put in place.

**PART IV—OBLIGATION OF THE CIVIL REGISTRATION ENTITY**

Duty to notify

**16.** (1) The notice issued by the civil registration entity pursuant to section 29 of the Act, the civil registration entity shall ensure that the notice is simple, clear and in an understandable language; and

(2) A civil registration entity may use physical or electronic formats, verbal means or any other technology to issue the notice envisaged under paragraph (1).

Retention of personal data

**17.** (1) A civil registration entity shall retain processed personal data in perpetuity and in accordance with the enabling written laws.

(2) Where a civil registration entity processes personal data for a specific reason and does not require retention of the personal data in perpetuity, personal data may be deleted, anonymised or pseudonymised.

(3) A civil registration entity shall formulate administrative mechanisms that describe what categories of personal data may be deleted, erased, anonymised or pseudonymised.

Notification of breach of personal data.

**18.** (1) Pursuant to section 43 of the Act, a civil registration entity shall notify the Data Commissioner and the data subject of personal data.

(2) Where a data subject suspects that personal data has been breached, the data subject shall immediately notify the civil registration entity of the personal data breach in writing.

Data protection impact assessment.

**19.** Where a data protection impact assessment may be required in accordance with section 31 of the Act, a civil registration entity shall conduct the data protection impact assessment in Form 1 set out in the Second Schedule.

Responsibilities of  
data Protection  
Officer.

**20.** (1) In addition to the functions set out under section 24 (7) of the Act, the responsibilities of the Data Protection Officer shall include—

- (a) monitor and evaluate the efficiency of the data systems in the organization; and
- (b) keep written records of the processing activities of the civil registration entity.

(2) The records specified under paragraph (1) (b) shall be in writing or electronic form and shall include the following information—

- (a) the name and contact details of the civil registration entity;
- (b) the purpose for processing the data;
- (c) a description of the categories of the data subjects and of the categories of the personal data;
- (d) the categories of recipients to whom personal data have or shall be disclosed to, including to those outside Kenya;
- (e) any transfers of personal data outside Kenya including the identification of the third party or an organization outside Kenya to which the data is transferred;
- (f) where possible, a description of the technical and security measures that have been utilized to alleviate data-related risks;
- (g) number of staff trained on the data protection; and
- (h) data protection impact assessment undertaken, if any.

Sharing of  
personal  
information with  
public agencies

**21.** (1) Subject to section 25 of the Act, a civil registration entity may make personal data collected by it, available to a public agency, upon request.

(2) A request for personal data envisaged under paragraph (1) shall be—

- (a) made by an authorized officer of the requesting public agency;

- (b) in writing, specifying—
  - (i) the purpose for which personal data is required;
  - (ii) the duration for which personal data shall be kept; and
  - (iii) proof of the safeguards put in place to secure personal data from unlawful disclosure.

(3) Personal data collected by a public agency, pursuant to this regulation shall—

- (a) be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is requested; and
- (b) not be processed in a manner that is incompatible with the purpose for which it was requested.

Automated individual decision making.

22. (1) A civil registration entity making automated decisions shall—

- (a) inform the data subject that they are engaging in the automated processing;
- (b) provide meaningful information about the logic involved;
- (c) explain the significance and envisaged consequences of the processing;
- (d) take steps to prevent errors, bias and discrimination;
- (e) use appropriate mathematical or statistical procedures;
- (f) put appropriate technical and organizational measures in place, so that it can correct inaccuracies and minimize the risk of errors;

- (g) secure personal data in a way that is proportionate to the risk to the interests and rights of the data subject, and that prevents discriminatory effects; and
- (h) ensure that data subjects can—
  - (i) obtain human intervention; and
  - (ii) express their point of view.

Internal  
complaints  
handling  
procedure.

23. (1) Where a data subject is aggrieved by the processing of his personal data, the data subject may lodge a complaint to the civil registration entity.

(2) A complaint envisaged under paragraph (1) shall be made orally or into writing—

(3) A civil registration entity shall as soon as practicable reduce an oral complaint into writing.

(4) A complaint by a data subject shall provide—

- (a) the full name of the data subject lodging the complaint;
- (b) contact details of the data subject;
- (c) details of the complaint;
- (d) period over which the suspected wrongdoing occurred; and
- (e) documentary evidence in support of the complaint where available.

(5) The civil registration entity shall investigate the complaint and notify the data subject of the investigation outcome in writing within seven days from the date of the investigation and any action taken where the complaint has been upheld.

(6) The civil registration entity shall inform the data subject of his right of appeal to the data commissioner.

#### PART V—SECURITY SAFEGUARDS

Data protection by design or default

**24.** (1) A civil registration entity shall embed data privacy features directly into the design of the data base to ensure protection of personal data.

(2) A civil registration entity operational and technical systems shall incorporate—

- (a) data protection principles;
- (b) enforceability mechanisms of the data subject's rights;
- (c) risk management mechanisms for data protection and for information security;
- (d) cyber security measures;
- (e) access security;
- (f) physical security; and
- (g) de-identification measures.

(3) A civil registration entity shall take reasonable steps to—

- (a) protect personal data it holds from misuse, interference and loss, and unauthorized access, modification or disclosure; and
- (b) protect personal data at all stages of the personal data lifecycle.

FOR PUBLIC ENGAGEMENT

Security safeguards of personal data.

**25.** A civil registration entity shall put in place security safeguards to ensure personal data held by them is accessed by authorized persons which include—

- (a) technical safeguards for encryption of personal data at rest or in transit;
- (b) personnel safeguards through the vetting of personnel involved in the processing of personal data; and
- (c) procedural safeguards which may include restricted access control to data Centre or system holding or carrying personal data.

Database security

**26.** A civil registration entity shall implement restriction of unauthorized access, configuration to prevent distributed denial of service attack or user overload and continuous database backup to enhance database security.

Monitoring by the Data Commissioner.

**27.** The Data Commissioner shall on a periodic basis conduct monitoring and evaluation of security safeguards employed by a civil registration entity.

Data security procedure.

**28.** (1) A civil registration entity shall formulate a written data security procedure for its entity.

(2) The procedure specified under paragraph (1) shall be binding upon the authorized users and shall include—

- (a) instructions concerning physical protection of the database sites and their surroundings;
- (b) access authorizations to the database and database systems;
- (c) description of the means intended to protect the database systems and the manner of their operation for this purpose;
- (d) instructions to authorized users of the database and database systems regarding the protection of data stored in the database;

FOR PUBLIC ENGAGEMENT

- (e) the risks to which the data in the database is exposed in the course of the civil registration entity's ongoing activities, including those originating from the database systems structure, the manner in which the risks are identified and dealt with, including encryption mechanisms to protect the data stored in the database or in the database systems;
- (f) the manner of dealing with information security incidents, according to the severity of the incident;
- (g) instructions concerning the management and usage of portable devices;
- (h) instructions with respect to conducting periodical audits to ensure that appropriate security measures, in accordance with the Procedure and these Regulations exist; and
- (i) instructions regarding backup of personal the data.

(3) The civil registration entity shall, on an annual basis, assess the need to update the security procedure.

(4) Despite paragraph (3), the civil registration entity shall assess whether the security procedure requires to be updated in the following instances—

- (a) material modifications in the database systems; or
- (b) new technological risks relating to the database systems are known.

(5) A civil registration entity that controls several databases may develop a data security procedure in accordance with these Regulations in a single document which concerns all databases it controls.

Database systems and a risk assessment.

**29** (1) A civil registration entity shall maintain an up-to-date document of the database structure, and an up-to-date inventory of the database systems, including—

- (a) infrastructure and hardware systems, types of communication and data security components;
- (b) the software systems used to operate, administer and maintain the database, to support its activity, monitor and secure;
- (c) software and interfaces used for communication to and from the database systems;
- (d) a diagram of the network in which the database is operating, including a description of the connections between the different system components and the physical location of components; and
- (e) the dates in which the document and the inventory were last updated.

(2) The up-to-date database structure document and inventory shall be secured in such a manner that only authorized users who require them for the performance of their role shall be provided access.

(3) The civil registration entity shall be responsible to conduct a data security risk assessment.

(4) The civil registration entity shall consider—

- (a) the findings of the risk assessment provided; and
- (b) the need to update the database definitions document or the data security procedure as a result, and act to amend the shortcomings found in the course of the assessment, if any.

(5) The risk assessment specified under paragraph 3(a) shall take place at least once every eighteen months.

(6) The civil registration entity is responsible to conduct, at least once every eighteen months, access tests to the database systems in order to test their vulnerability to external and internal threats.

(7) The civil registration entity shall consider the results of the access tests and amend the faults found, if any.

Physical protection  
and secure  
surroundings

**30.** (1) A civil registration entity shall ensure that the database and database systems are maintained in a secure place, preventing unauthorized access, and which is suitable to the nature of the database activity and the sensitivity of information therein.

(2) A civil registration entity shall take measures to monitor and document the entry to and exit from sites in which the database or database systems are located, including the setting and removing of equipment in and from the database systems.

Data security in  
manpower  
management

**31.** (1) A civil registration entity shall not grant access to information stored in the database and shall not change the scope of authorization granted, unless the civil registration entity has undertaken reasonable measures, to screen and place authorized users, to ensure that the unauthorized user is not granted access to the personal data stored in the database.

(2) The measures specified under paragraph (1) shall be taken in accordance with the sensitivity of the information in the database and the scope of access permissions attached to the role proposed to the relevant person.

(3) Prior to authorised users gaining access to the database or before a change in the scope of their authorizations, the civil registration entity shall hold training sessions for authorized users regarding the obligations embodied in the Act and these Regulations, and the data security procedure.

Access permission  
management.

**32.** (1) A civil registration entity shall determine access permission of authorized users to the database and database systems in accordance with the authorized user's responsibilities.

(2) Access permission shall be granted to the extent required for performing the role.

(3) A civil registration entity shall keep an up-to-date record of authorized user's roles, user permission granted to these roles and the authorized users performing such roles.

(4) Immediately following the termination of an authorized user's role, a civil registration entity shall revoke the permission of an authorized user who has stopped working in his role, and change the passwords to the

database and database systems to which the authorized user could have known.

Monitoring and documenting access.

**33.** (1) In the systems of a database subject to medium or high security level, an automatic recording mechanism shall enable monitoring the access to the database systems including the following data—

- (a) user identity;
- (b) date and time of access attempt;
- (c) system component to which access was attempted; and
- (d) access type, its scope, and whether access was granted or denied.

(2) The monitoring mechanism shall not enable—

- (a) disabling or modifying its operation; and
- (b) such modifications or the disabling of its operation and shall send alerts to the authorized user or any other relevant person.

Documentation of security incidents.

**34.** (1) A civil registration entity shall document cases in which an event was discovered, raising concern regarding a breach of personal data integrity, unauthorized use thereof or deviation from authorization.

(2) The documentation specified under paragraph (1) shall, as far as is practicable, be stored in electronic form.

(3) In the data security procedure, a civil registration entity shall prescribe instructions with respect to handling information security incidents, depending on the event severity and the information sensitivity level, including—

- (a) revoking authorizations and other necessary immediate measures; and
- (b) reporting security incidents, to the Data Commissioner and the actions taken in response to the security incidents.

(4) In a database subject to high security level, the civil registration entity shall hold a discussion regarding data security incidents on a quarterly basis.

Network security.

**35.** (1) A civil registration entity shall not connect the database systems to the internet or to another public network without installing the appropriate safeguards against unauthorized access or against software that may damage or disrupt computers or computer material.

(2) The transfer of personal data from the database through a public network or the internet shall be conducted by commonly used encryption methods.

Periodical audits.

**36.** (1) The civil registration entity shall conduct, at least once in twenty-four months, an internal or external audit by an auditor adequately trained in the field of data security who is not the civil registration entity's data protection officer, in order to ensure it complies with the provisions of the Act and these Regulations.

(2) The auditor shall report on the adherence of the security measures to the data security procedure and to these Regulations, identify shortcomings and recommend the necessary measures to correct the situation.

(3) A civil registration entity shall review the audit reports specified under sub-regulation (2) and assess the need to update the database definitions document or the data security procedure, accordingly.

(4) A civil registration entity that controls several databases may comply with the duty prescribed in this regulation by performing a single audit for all the databases it controls which have the same security level.

Data backup and restoration.

**37.** (1) The civil registration entity shall retain the backup copy of the data and of the security procedures in a manner that ensures the integrity of the personal data and the ability to restore the information in case of loss or destruction.

(2) The civil registration entity shall formulate –

- (a) procedures for routine periodical backup in accordance with these Regulations; and
- (b) procedures to ensure restoration of the data.

(3) In documenting security incidents pursuant to regulation 34, data restoring processes shall also be documented, including the identity of the person who performed the data restoration and the details of the personal data restored.

Transfer of personal data outside Kenya

**38.** A civil registration entity shall not transfer personal data collected for civil registration purposes out of Kenya, except with the written approval of the National Security Council.

#### PART VII—MISCELLANEOUS PROVISIONS

Reports to the Data Commissioner.

**39.** A civil registration entity shall, on a quarterly basis, submit a compliance report to the Data Commissioner.

Outsourcing.

**40.** (1) A civil registration entity entering into an agreement with an external service provider in order to receive a service which involves granting external service provider access to the database shall—

(a) assess, prior to entering an agreement with the external service provider, the data security risks involved in the engagement;

(b) expressly agree with the external service provider on the following, taking into account the risks mentioned under paragraph (a)—

(i) the data the external service provider may process and the permitted purposes of its use as required by the agreement between the parties;

(ii) the database systems that the external service provider may access;

(iii) the type of processing or activities the external service provider may perform;

(iv) the agreement duration, the manner of returning the data to the civil registration entity at the end of the agreement, its destruction at the disposal of the external

service provider and of reporting accordingly to the civil registration entity;

(v) the manner data security obligations which apply to the processor of the database according to these Regulations are implemented, and additional data security instructions set by the civil registration entity, if any;

(vi) the external service provider shall have his authorized users sign an undertaking to protect the information confidentiality, to use the data only according to the agreement and to implement the data security measures prescribed in the agreement; and

(vii) where a civil registration entity permitted the external service provider to provide the service through another entity, it shall be the duty of the civil registration entity to include in the agreement with the other entity all the matters detailed in these Regulations.

(2) The external service provider shall report to the civil registration entity, at least annually, the manner the obligations by these Regulations and the agreement are implemented, as well as to notify the civil registration entity any security incident.

(3) The civil registration entity shall take measures to monitor and supervise the compliance of the external service provider with the provisions of the agreement and these Regulations, as appropriate, taking into account any risks.

(4) A civil registration entity that controls several databases and enters into an agreement with an external service provider which involves access to these databases by the external service provider may enter into a single agreement concerning all databases, provided that they all have the same security level.

**SCHEDULE**

**FIRST SCHEDULE**

FORM 1

(r. 12)

**REQUEST FOR RESTRICTION OR OBJECTION TO THE PROCESSING OF  
PERSONAL INFORMATION**

Note:

- (i) Affidavits or other documentary evidence in support of the objection may be attached.
- (ii) If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
- (iii) Where an objection is initiated by a person other than the data subject, the initiator must attach proof of authority to act on behalf of the data subject.

**A. SECTION: NATURE OF REQUEST**

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

RESTRICTION

OBJECTION

**B. DETAILS OF THE DATA SUBJECT**

.....  
Surname

Middle name

First name

Birth Certificate/ Notification/ National Identity Card/ Passport number: .....

Postal address: .....

Contact number(s): .....

e-mail address: .....

**C. DETAILS OF PERSON INITIATING THE OBJECTION (where the data subject is a  
minor or mentally incapacitated)**

.....  
Surname

Middle name

First name

National Identity Card/ Passport number: .....

Postal address: .....

Contact number(s): .....

e-mail address: .....

**REASONS FOR RESTRICTION**

**OBJECTION**

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

- (a) .....
- (b) .....
- (c) .....
- (d) .....
- (e) .....
- (f) .....
- (g) .....

**SECTION 5: DECLARATION**

Please note that any attempt to gain access to personal information 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.

**DOCUMENT CHECKLIST: I HAVE PROVIDED:**

- (a) A duly completed request form.
- (b) Attached document(s), including proof of authorization (if applicable).
- (c) Signed and dated the request form.

Signature

Date

FORM 2

(r. 10(4), (r. 11(2))

**REQUEST FOR RECTIFICATION OF PERSONAL INFORMATION**

**Note:**

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Where a request for rectification is made by a person other than the data subject, the person making the request must attach proof of authority to act on behalf of the data subject.
4. On receipt of a duly filled form, you will receive a response within three working days

**Fill as appropriate**

**SECTION 1 : DETAILS OF THE DATA SUBJECT**

Full Name:

Birth Certificate/ Notification/

Identity Card/ Passport no.

Postal Address

\*Telephone/Mobile No.

\*Email address

**SECTION 2: PERSON INITIATING THIS REQUEST.**

Full Name:

Birth Certificate/ Notification

Identity Card/ Passport number.

Postal Address

Mobile No/ Email address

**SECTION 3: REASONS FOR REQUEST**

<b>Personal Information currently on file to be corrected e.g. name, mobile number, email address</b>	<b>Reason why that personal information should be rectified e.g. is the information inaccurate or out of date?</b>

**SECTION 4: DECLARATION**

Please note that any attempt to gain access to personal information 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

**DOCUMENT CHECKLIST:**

***I have provided:***

- (a) A duly completed request form.
- (b) Attached document(s), including proof of authorization (if applicable).
- (c) Signed and dated the request form.

**SECOND SCHEDULE**

FORM 1

(r.19)

**DATA PROTECTION IMPACT ASSESSMENT**

**Part 1: Description of the processing operations.**

a. Project Name	
b. Project Outline :What and Why Explain Broadly what the project aims to achieve and what type of processing it involves	
c. Describe the Information Flow – You should describe the collection, use and deletion of personal data here. It may also be useful to refer to a flow diagram or another format of explaining data flows,	

<ol style="list-style-type: none"> <li>1. Where you are getting the data from.</li> <li>2. Where the data will be stored.</li> <li>3. Where data could be transferred to.</li> <li>4. How many individuals are likely to be affected by the project</li> </ol>	
--	--

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

<b>Describe compliance and proportionality measures, in particular:</b>	
a. What is your lawful basis for processing?	
b. Does the processing actually achieve your purpose?	
c. Is there another way to achieve the same outcome?	
d. How will you ensure data quality and data minimization?	
e. What information will you give individuals?	
f. How will you help to support their rights?	
g. What measures do you take to ensure processors comply?	
h. How do you safeguard any international transfers?	

**Part 3: An assessment of the risks to the rights and freedoms of data subjects.**

Assessment Questions		
Explain what practical steps you will take to ensure that you identify and address privacy risks..	Yes (Please give explanation)	No (Please give explanation)
1. Will the project involve the collection of new identifiable or potentially identifiable data about data subjects?		

<p>2. Will the project compel data subjects to provide information about themselves, i.e. where they will have little awareness or choice?</p>		
<p>3. Will identifiable information about the data subjects be shared with other organizations or people who have not previously had routine access to the information?</p>		
<p>4. Are you using information about data subjects for a purpose it is not currently used for in a new way, i.e. using data collected to provide care for an evaluation of service development.</p>		
<p>5. Where information about data subjects is being used, would this be likely to raise privacy concerns or expectations, i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress?</p>		
<p>6. Will the project require you to contact data subjects in ways which they may find intrusive, i.e. telephoning or emailing them without their prior consent?</p>		
<p>7. Will the project result in you making decisions in ways which can have a significant impact on data subjects, i.e. will it affect the services a person receives?</p>		
<p>8. Does the project involve you using new technology which might be perceived as being privacy intrusive, i.e. using biometrics, facial recognition or automated decision making?</p>		
<p>9. Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract?</p>		
<p>10. Is processing of identifiable/potentially identifiable data being moved to a new organization (but with same staff and processes)</p>		

FOR PUBLIC ENGAGEMENT

**Part 4: 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 the Data Protection Act**

**Identification of risks – Civil Registration Entities should carry out the risk analysis using exactly the same methodology as they do for other project risks. Enter the key risks that have been identified, and the options for avoiding or mitigating those risk into this table.**

Risk description	Options for avoiding or mitigating the identified risk	Residual Privacy Risk after implementation of mitigation (High, medium, or low)		
		Impact	Likelihood	Exposure

Made on the ....., 2020.

FOR PUBLIC ENGAGEMENT

**JOE MUCHERU,**  
Cabinet Secretary,

Ministry of Information, Communication, Technology, Innovation and Youth Affairs.