THE REPUBLIC OF KENYA

LAWS OF KENYA

THE DATA PROTECTION (CIVIL REGISTRATION) REGULATIONS

NO. 196 OF 2020

Revised and published by the National Council for Law Reporting
with the authority of the Attorney-General as gazetted by the Government Printer

www.kenyalaw.org

Kenya

Data Protection Act

The Data Protection (Civil Registration) Regulations

Legal Notice 196 of 2020

Legislation as at 31 December 2022

FRBR URI: /akn/ke/act/ln/2020/196/eng@2022-12-31

The Data Protection (Civil Registration) Regulations (Legal Notice 196 of 2020)
Contents

DATA PROTECTION ACT

THE DATA PROTECTION (CIVIL REGISTRATION) REGULATIONS

LEGAL NOTICE 196 OF 2020

Commenced on 16 October 2020

[Revised by 24th Annual Supplement (Legal Notice 221 of 2023) on 31 December 2022]

Part I – PRELIMINARY

1. Citation.

These Regulations may be cited as the Data Protection (Civil Registration) Regulations.

2. Interpretation.

In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection Act (Cap. 411C);

"authorized officer" means an officer of the civil registration entity who is expressly permitted by the civil registration entity to access the civil registration entity's database and database system;

"child" has the meaning assigned to it under the Children Act (Cap. 141);

"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 as provided under the existing laws;

"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.

"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 the Act.

3. Scope of the Regulations.

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 persons;

(d) issuance of passport;

(e) registration of marriages;

(f) registration of deaths; or

(g) issuance of any document of identity.

Part II – DATA PROTECTION PRINCIPLES

4. Lawful processing of personal data.

The processing of personal data is lawful, if undertaken pursuant to the Act and in accordance to the provisions of the following laws—

(a) the Registration of Persons Act (Cap 107);

(b) the Births and Deaths Registration Act (Cap. 149);

(c) the Kenya Citizenship and Immigration Act (Cap. 170);

(d) the Marriage Act (Cap. 150);

(e) the Children Act (Cap. 141);

(f) the Refugee Act (Cap. 173); or

(g) any other law relating to the issuance of identity document.

5. Privacy in processing personal data.

A civil registration entity shall take all practical measures to ensure—

(a) access to the data in its system is only by authorized officers;

(b) the database system has adequate technical and procedural safeguards for processing personal data;

(c) the data subject is provided with the necessary information relating to the processing 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.

6. Consent.

(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.

7. Manner of giving consent.

(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 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.

8. Collection of personal data.

(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.

(3) Where the new purpose is not compatible with the initial purpose, the civil registration entity shall seek fresh consent from 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 for the new purpose by the civil registration entity.

9. Limitation in processing of personal data.

(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 1 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 within seven days notify the data subject of such decline giving reasons for the decision.

(5) Where the application for restriction in limitation of processing of the data is declined, the data subject may appeal to the Data Commissioner.

Part III – RIGHTS OF A DATA SUBJECT

10. Access to personal data.

(1) A data subject shall make a request to access their personal data in Form 2 set out in the First Schedule.

(2) A civil registration entity shall—

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

(b) put in place electronic or manual mechanisms to enable data subjects to access their personal data.

11. Rectification of personal data.

(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 1 set out in the First Schedule.

(3) An application for rectification of personal data shall be supported by the necessary documents, relevant to the rectification being sought.

(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 within thirty days 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) and provide reasons thereto.

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

(8) 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.

12. Objection to processing of personal data.

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

13. Data portability request.

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 within thirty days from the date of receipt of the request and upon payment of the required fees.

14. Exercise of data subject rights by others.

(1) Subject to section 27 of the Act, where a person duly authorized by the data subject seeks to exercise the rights 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 there is doubt as to the existence of a relationship between the duly authorized person and the data subject, the civil registration entity shall halt the request of exercising a right on behalf of the data subject until evidence to the contrary is adduced.

(3) Where the right is being exercised on behalf of a minor, the persons exercising that right may produce #

(a) a birth certificate;

(b) an adoption certificate;

(c) a court Order; or

(d) any other relevant document.

15. Processing of Personal data relating to a child.

(1) When processing personal data of a child, the civil registration entity shall ensure that—

(a) consent is given by the child's parent or guardian;

(b) processing is done lawfully and safeguards the best interest of the child;

(c) where required, that the child is present;

(d) unauthorized access to personal data relating to a child is prohibited;

(e) it has design systems and processes that safeguard the best interest of the child; and

(f) the risks and consequences of the processing are identified, and appropriate safeguards are put in place.

Part IV – OBLIGATION OF THE CIVIL REGISTRATION ENTITY

16. Duty to notify.

(1) The information given by the civil registration entity pursuant to section 29 of the Act shall be simple, clear and in an understandable language.

(2) In giving the information envisaged under paragraph (1), a civil registration entity may use physical or electronic formats, verbal means or any other technology.

17. Retention of personal data.

(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 shall be deleted, anonymised or pseudonymised.

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

18. Notification of breach of personal data.

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

(2) Where a data subject suspects that their personal data has been breached, the data subject may, within fourteen days from the date of such suspicion, notify the respective civil registration entity and the Data Commissioner of such personal data breach in writing.

(3) The provisions of regulation 23 shall apply to this regulation with necessary modifications.

19. Data protection impact assessment.

(1) 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 guided by Form 1 set out in the Second Schedule.

(2) The data impact assessment report prepared pursuant to paragraph (1) shall, with the approval of the Data Commissioner, be published in the manner determined by the Data Commissioner.

20. Responsibilities of Data Protection Officer.

(1) Subject to section 24(7) of the Act, the responsibilities of the Data Protection Officer includes to—

(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 to be transferred;

(f) 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.

21. Sharing of personal information with public agencies.

(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.

22. Automated individual decision making.

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

(a) inform the data subject when engaging in the automated processing;

(b) provide meaningful information about the logic involved;

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

(d) ensure the prevention of 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.

23. Internal complaints handling procedure.

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

(2) A complaint made under paragraph (1) may be made orally or in writing.

(3) A civil registration entity shall reduce an oral complaint into writing and shall be executed by the complainant.

(4) A complaint by a data subject may 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; or

(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 completion of the investigation and any action taken where the complaint has been upheld.

(6) The civil registration entity shall inform the data subject of the right to appeal to the Data Commissioner, where the data subject is dissatisfied with the decision of the civil registration entity.

Part V – SECURITY SAFEGUARDS

24. Data protection by design or default.

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

(2) A civil registration entity's 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.

25. Security safeguards of personal data.

A civil registration entity shall put in place security safeguards to ensure that 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.

26. Database security.

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.

27. Monitoring by the Data Commissioner.

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

28. Data security procedure.

(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 officer 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 officer of the database and database systems regarding the protection of data stored in the database;

(e) the risks to which the data in the database is exposed in the course of the civil registration entity's ongoing activities;

(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 that concerns all databases it controls.

29. Database systems and a risk assessment.

(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, monitor and secure its activity;

(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 4(a) shall carried out on a periodical basis.

(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.

30. Physical protection and secure surroundings.

(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.

31. Data security in manpower management.

(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 officers, 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 authorized officers gaining access to the database or before a change in the scope of their authorizations, the civil registration entity shall train authorized officer on the obligations embodied in the Act and these Regulations.

32. Access permission management.

(1) A civil registration entity shall determine access permission of authorized users to the database and database systems in accordance with the authorized officer’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 ceased working in their role, and change the passwords to the database and database systems to which the authorized user could have known.

33. Monitoring and documenting access.

(1) An automatic recording mechanism shall be incorporated in the database system to enable monitoring access to the database systems including on—

(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—

(a) not enable disabling or modifying its operation; and

(b) in the event of disabling or modifying, send alerts to the authorized officer or any other relevant person.

34. Documentation of security incidents.

(1) A civil registration entity shall document cases in which a data security incident 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.

35. Network security.

(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.

36. Periodical audits.

(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.

37. Data backup and restoration.

(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.

38. Transfer of personal data outside Kenya.

(1) A civil registration entity shall not transfer personal data collected for civil registration purposes out of Kenya, except with the written approval of the Data Commissioner.

(2) A person who contravenes Paragraph (1) shall, on conviction, be liable to a penalty specified under section 73 of the Act.

Part VII – GENERAL PROVISIONS

39. Reports to the Data Commissioner.

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

40. Outsourcing.

(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 quarterly, 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 that includes access to the databases by the external service provider, may enter into a single agreement concerning all databases.

FIRST SCHEDULE [r.9 (2), (r.11(2), r.12]

REQUEST FOR RESTRICTION OR OBJECTION TO THE PROCESSING OF PERSONAL DATA

FORM 1

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 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) .....

(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 (1))

REQUEST FOR ACCESS TO PERSONAL DATA

Note:

5. Affidavits or other documentary evidence as applicable in support of the request may be attached.

6. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

7. 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.

8. On receipt of a duly filled form, you will receive a response within three working days

Fill as appropriate

Full Name:

Birth Certificate/ Notification/

Identity Card/ Passport No:

*Telephone/Mobile No:

*Email address:

SECTION 2: PERSON INITIATING THIS REQUEST.

Full Name:

Birth Certificate/ Notification

Identity Card/ Passport number:

Mobile No. / Email address:

SECTION 3: PROPOSED CHANGE (S)

	Personal Information currently on file to be corrected e.g. name, residential status, and mobile number, email address.	**The proposed change**	**Reason for the proposed change**
1.			
2.			
3.			
4.			
5.			
6.			
7.			

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:

(d) A duly completed request form.

(e) Attached document(s), including proof of authorization (if applicable).

(f) Signed and dated the request form.

SECOND SCHEDULE [r. 19(1)]

DATA PROTECTION IMPACT ASSESSMENT

FORM 2

Part 1 - Description of the processing operations.

1. Project Name	
2. Project Outline: What and why Explain broadly what the project aims to achieve and what type of processing it involves	
3. Describe the Information Flow— Describe the collection, use and deletion of personal data here. It may in a flow diagram or another format of explaining data flows— (a) where you are getting the data from; (b) where the data will be stored; (c) where data could be transferred to; and (d) how many individuals are likely to be affected by the project.	

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

Describe compliance and proportionality measures, in particular:	
1. What is your lawful basis for processing?	
2. Does the processing actually achieve your purpose?	
3. Is there another way to achieve the same outcome?	
4. How will you ensure data quality and data minimization?	
5. What information will you give individuals?	
6. How will you help to support their rights?	
7. What measures do you take to ensure processors comply?	
8. 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?		
2. Will the project compel data subjects to provide information about themselves, i.e. where they will have little awareness or choice?		

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?		
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.		
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?		
6. Will the project require you to contact data subjects in ways, which they may find intrusive, such as telephoning or emailing them without their prior consent?		
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?		
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?		

9. Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract?		
10. Is processing of identifiable/potentially identifiable data being moved to a new organization (but with same staff and processes)		

Part 4: The measures envisaged 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

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