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

ARRANGEMENT OF REGULATIONS

Regulation

1. Citation and commencement
2. Interpretation
3. Scope of Regulations
4. Requirements for registration
5. Application for registration
6. Payment of registration fees by specified public bodies
7. Processing of an application for registration
8. Approval and issuance of certificate of registration
9. Duration of certificate of registration
10. Refusal of registration
11. Renewal of registration
12. Refusal of renewal.
13. Exemption from mandatory registration
14. Register
15. Change of particulars
16. Cancellation or variation of registration
17. Electronic registration
18. Offences

SCHEDULES

REGISTRATION FORM FOR DATA CONTROLLERS AND DATA PROCESSORS

Fees charged by office

THRESHOLDS FOR MANADATOTY REGISTRATION

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

[Legal Notice 265 of 2021]

1. Citation and commencement

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

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

2. Interpretation

In these Regulations, unless the context otherwise requires—

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

"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.

3. Scope of Regulations

(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 (sub. leg).

4. Requirements for registration

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

5. Application for registration

(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 subregulation (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.

6. Payment of registration fees by specified public bodies

(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 subregulation (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 subregulation (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.

7. Processing of an application for registration

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

8. Approval and issuance of certificate of registration

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.

9. Duration of certificate of registration

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

10. Refusal of registration

(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 subregulation (3) shall be processed as any other application and in the manner specified under these Regulations.

11. Renewal of registration

(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 subregulation (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.

12. Refusal of renewal.

(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.

13. Exemption from mandatory registration

(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 subregulation (2), the data controller and data processor exempt under subregulation (2) shall be required to comply with the provisions of the Part IV and Part VI of the Act.

(4) The exemption provided under subregulation (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 subregulation (2), shall be required to undertake mandatory registration in accordance with Part III of the Act and these Regulations.

14. Register

(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.

15. Change of particulars

(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.

16. Cancellation or variation of registration

(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 (Cap. 7J).

17. Electronic registration

An application made under these Regulations shall be submitted through electronic means provided for on the Office website.

18. Offences

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

[r. 5(1)(a)]

REGISTRATION FORM FOR DATA CONTROLLERS AND DATA PROCESSORS

FORM DPR 1

SECTION 1 - BASIC DETAILS

Indicate if you are registering as a

Data Controller # Data Processor #

Name:

Postal Address:

Telephone Number:

Email Address:

County:

Country:

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: _____

FORM DPR 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

[r. 5(2)(b)]

Fees charged by office

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 5 Million	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 50 Million	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

[r. 13(1)(3)]

THRESHOLDS FOR MANADATOTY REGISTRATION

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 prevention and prosecution of offenders (including operating security CCTV system).

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.