



## **OFFICE OF THE DATA PROTECTION COMMISSIONER**

# **GUIDANCE NOTE ON REGISTRATION OF DATA CONTROLLERS & DATA PROCESSORS**



## Definitions:

**"Act"** means the Data Protection Act, No 24. of 2019.

**"Data Commissioner"** means the person appointed pursuant to section 6 of the Act.

**"Data Controller"** means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing of Personal Data;

**"Data Processor"** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

**"Data Subject"** means an identified or identifiable natural person who is the subject of Personal Data.

**"Entity" or "Entities"** means a natural (individual) or legal person, public authority, agency or other body that processes (handles) Personal Data.

**"Establishment documents"** includes

- (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.

**"Non-exempt mandatory registration Entities"** means Entities that are required to register regardless of their Turnover/ Revenue, or the number of staff employed.

**"Office"** means the Office of the Data Protection Commissioner as established in section 5 of the Act.

**"Personal Data"** means any information relating to an identified or identifiable natural person.

**"Processing"** means any operation or sets of operations which is performed on Personal Data or on sets of Personal Data whether or not by automated means, such as:

- (a) collection, recording, organisation, structuring;
- (b) storage, adaptation or alteration;
- (c) retrieval, consultation or use;
- (d) disclosure by transmission, dissemination, or otherwise making available;
- or
- (e) alignment or combination, restriction, erasure or destruction.

**“Register of Data Controllers and Data Processors”** means the list of registered Entities maintained and published by the Office of the Data Protection Commissioner.

**“Regulations”** means the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 that takes effect from 14 July 2022.

**“Revenue”** means the total income of profit-making Data Controllers or Data Processors for the year immediately preceding the year of registration.

**“Sensitive Personal Data”** means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the Data Subject.

**“Turnover”** means the utilized annual budget of non-profit making Data Controllers or Data Processors for the year immediately preceding the year of registration.

## **1. SCOPE AND PURPOSE OF GUIDELINES**

The Act provides a statutory obligation for all Entities, including individuals, that process Personal Data to register with the Data Commissioner, subject to the thresholds set in place by the data commissioner on mandatory registration. The Act further places an obligation on the data commissioner to maintain a register of Entities registered as either Data Controllers or Data Processors.

Pursuant to section 18 of the Act and, particularly, sub-section (2), and section 71 of the Act, the Cabinet Secretary caused to be developed and, subsequently, gazettement the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 that will take effect from **14 July 2022**. The Regulations details the requirements of Registration including the Entities that must register, and must meet their mandatory registration obligations, and those that are exempt due to being found to be below the threshold. The Regulations also set out the treatment of government Ministries, Departments, Agencies and Counties (MDACs) and non-for-profit Entities, and religious institutions.

This guidance was developed to assist Entities in ascertaining if they are Data Controllers or Data Processors, and understand their obligations with respect to mandatory registration. This Guidance Note considers:

- The Data Protection Act, 2019
- The Data Protection (Registration of Data Controller and Data Processors) Regulations, 2021
- The Data Protection and Privacy Policy, 2018; and
- International Best Practice.

## **2. TYPES OF ENTITIES**

The Act and Regulations define two types of Entities that process Personal Data, namely: Data Controllers and Data Processors. The Act and Regulations give similar obligations to the Data Controller and Data Processor, with only slight variations such as in instances of notification of data breaches.

An Entity can register as both a Data Controller and a Data Processor with regards to any Processing operation. Where an Entity registers as both, they will be required to pay the fee for an application as Data Controller and an application as a Data Processor.

### **2.1. DATA CONTROLLERS**

The Act defines a Data Controller as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing of Personal Data.

Data Controllers must comply and demonstrate compliance with, all the data protection principles and meet all obligations under the Act and all regulations therein. Data Controllers are also responsible for the compliance of Data Processors contracted to process Personal Data on their behalf.

The Office may take enforcement action against a Data Controller when there is a breach of its obligations. This may be occasioned by a complaint from a Data Subject, following an audit of the Data Controller or following an investigation on the Office's own initiative.

Data Controllers established or resident in Kenya and Data Controllers outside Kenya that process the Personal Data of individuals located in Kenya (not just citizens or residents) must register with the Office.

### **2.1.1. Checklist: Are you a Data Controller?**

- You decide to collect or process the Personal Data.
- You decide what the purpose or outcome of the Processing was to be.
- You decide what Personal Data should be collected.
- You decide which individuals to collect Personal Data about.
- You obtain a commercial gain or other benefit from the Processing, except for any payment for services from another controller.
- You are Processing the Personal Data as a result of a contract between you and the Data Subject.
- The Data Subjects are your employees.
- You make decisions about the individuals concerned as part of or as a result of the Processing.
- You exercise professional judgement in the Processing of the Personal Data.
- You have a direct relationship with the Data Subjects.
- You have complete autonomy as to how the Personal Data is processed.
- You have appointed the processors to process the Personal Data on your behalf.

## 2.2. DATA PROCESSORS

The Act defines a Data Processor as a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

There must be a contract between the Data Processor and the Data Controller that clearly defines this relationship. The Data Processor has no decision-making power on the Personal Data that they are Processing. **An employee of an Entity is not a Data Processor for the purposes of the Act.**

### 2.2.1. Checklist: Are you a Data Processor?

- You have a contract to handle Personal Data on behalf of another Entity.
- You are following instructions from someone else regarding the Processing of Personal Data.
- You do not decide to collect Personal Data from individuals.
- You do not decide what Personal Data should be collected from individuals.
- You do not decide the lawful basis for the use of that data.
- You do not decide what purpose or purposes the data will be used for.
- You do not decide whether to disclose the data, or to whom.
- You do not decide how long to retain the data.
- You may make some decisions on how data is processed, but implement these decisions under a contract with another Entity.

## 3. MANDATORY REGISTRATION

The Act states that subject to prescribed mandatory registration thresholds or exemptions, no person shall act as a Data Controller or Data Processor unless registered with the Data Commissioner. Therefore, all Data Controller and Data Processors **MUST** register unless an Entity **can clearly identify that they fall within an exemption.**

There are three tiers of fees that are prescribed in the Regulations and are dependant on a number of considerations including:

- Annual Turnover/ Revenue
- Number of employees
- Whether your Entity is a public Entity

- Whether your organisation is a non-profit making Entity or religious institution.

The fees payable for registration are between Kshs. 4,000/- to Kshs. 40,000/-.

There are a number of Entities (“**non-exempt mandatory registration Entities**”) that are must comply with their mandatory registration obligation despite their annual Turnover/ Revenue or number of employees. These Entities are listed below:

Any Entities Processing Personal Data for activities, or in the following sectors, **regardless of their annual Turnover/Revenue or number of employees:**

- political canvassing,
- crime prevention,
- gambling,
- education,
- health administration and provision of patient care,
- hospitality,
- property management,
- financial services,
- telecommunications,
- direct marketing,
- transports, and
- Entities Processing of genetic data

The fees payable by these Entities, if their annual Turnover/ Revenue is less than Five Million Kenyan Shillings (Kshs. 5,000,000/-) and they have less than ten (10) employees, will be Kshs. 4,000/-.

### **3.1. PRIVATE SECTOR**

All Entities within the private sector that:

- are resident in Kenya; or located outside Kenya;
- process Personal Data of persons located in Kenya (including citizens, residents and visitors); and
- have an annual Turnover or Revenue of Kshs. 5 million and above or more than 10 employees;

unless, the Entity is a **non-exempt mandatory registration Entity**, are required to register.

Non-exempt mandatory registration Entities must register regardless of their annual Turnover/ Revenue and/or number of employees.

<b>Category</b>	<b>Registration fee in Kshs. per Data Controller/Processor (payable Once)</b>	<b>Renewal fee in Kshs. per Data Controller/Processor (after every 2 years)</b>
<b>Micro and Small Data Controllers /Processors</b> - with between 1 and 50 employees <b>and</b> an annual Turnover/ Revenue of a maximum of Kshs. 5Million	4,000/-	2,000/-
<b>Medium Data Controllers /Processors</b> - with between 51 and 99 employees <b>and</b> an annual Turnover/ Revenue of between Kshs. 5,000,001(Five million and one shilling) and maximum of Kshs. 50,000,000 (Fifty million)	16,000/-	9,000/-
<b>Large Data Controllers /Processors</b> - with more than 99 employees <b>and</b> an annual Turnover/ Revenue of more than Kshs. 50 Million	40,000/-	25,000/-

To graduate to the next tier an Entity must meet both requirements.

For example, if an Entity has an annual Turnover/ Revenue of more than 5 million but has 10 employees, the Entity will be required to register as a Micro and Small Data Controller/ Processor and will pay Kshs. 4,000/-.



### 3.2. GOVERNMENT ENTITIES (MDACs)

The Regulations provide that State departments or County departments shall register and pay the fees on behalf of their respective Entities. These Entities must be 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.

*For example, the State Department of Broadcasting and Telecommunications in the Ministry of ICT, Innovation and Youth Affairs has a number of directorates and agencies under it, that are not deemed to be State Corporations by virtue of the State Corporations Act, 2012. In submitting the registration application, the State Department of Broadcasting and Telecommunications will need to identify and list all public Entities that operate under it and submit one application that will cater for the State Department and the public agencies under it. However, any Entity that is a state corporation, such as KBC (for example) will need to make its own application.*

The single registration fee of Kshs. 4,000/- and renewal fee of Kshs. 2,000/- to be paid by the State department or County department will cater for all specified Entities registered or under the concerned state department or county department.

A State Corporation or a County Corporation will be required to register as a Data Controller or a Data Processor in respect of their Processing activity.

<b>Category</b>	<b>Registration fee in Kshs. per Data Controller/Processor (payable Once)</b>	<b>Renewal fee in Kshs. per Data Controller/Processor (after every 2 years)</b>
<b>Public Entities</b> -offering government functions (Regardless of number of employees or Revenue/ Turnover)	4,000/-	2,000/-

### 3.3. CHARITIES AND RELIGIOUS INSTITUTIONS

The Act provides that a standard registration fee of Kshs. 4,000/- and renewal fee of Kshs. 2,000/- will be payable by non-profit making Data Controller or Data Processors. Non-profit making Data Controllers and Data Processors are Entities whose core mandate **excludes the generation of profit** and includes non-governmental

organizations, charitable and religious institutions, multi-lateral agencies or civil society organizations.

<b>Category</b>	<b>Registration fee in Kshs. per Data Controller/Processor (payable Once)</b>	<b>Renewal fee in Kshs. per Data Controller/Processor (after every 2 years)</b>
<b>Charities and Religious Entities</b> – servicing or offering charitable or religious functions (Regardless of Revenue/ Turnover)	4,000/-	2,000/-

#### **4. EXEMPTIONS**

The Regulations provide some exemptions from the mandatory registration. The table below illustrates which organisations must register with the ODPC, and those which may be exempted.

Data Controllers and Data Processors (not Processing Personal Data for one of the above activities or in one of the above sectors) <ul style="list-style-type: none"> <li>- with an annual Turnover or annual Revenue below KES 5 million; <b>AND</b></li> <li>- less than 10 employees.</li> </ul>	<b>EXEMPT</b>
Any Entities Processing Personal Data for activities, or in the following sectors, <b>regardless of their annual Turnover/ Revenue or number of employees:</b> <ul style="list-style-type: none"> <li>• political canvassing,</li> <li>• crime prevention,</li> <li>• gambling,</li> <li>• education,</li> <li>• health administration and provision of patient care,</li> <li>• hospitality,</li> <li>• property management,</li> <li>• financial services,</li> <li>• telecommunications,</li> <li>• direct marketing,</li> <li>• transports, and</li> <li>• Entities Processing of genetic data</li> </ul>	<b>NO EXEMPTION</b>

Where an Entity does not meet **BOTH** of the requirements, the **Entity will not be exempt and must register**. For example, if the Entity has an annual Turnover of more than five million but less than 10 employees, the Entity will be required to pay Kshs. 4000/-. If the Entity has more than 10 employees and less than 5 million in annual Turnover or Revenue, the Entity will be required to register as a micro and small Data Controller or Data Processor.

## **5. HOW TO REGISTER AND OTHER CONSIDERATIONS**

### **STEP 1: IDENTIFY IF YOU ARE A DATA CONTROLLER OR DATA PROCESSER (OR BOTH)**

If you are a Data Controller and a Data Processor, you will be required to register twice as a Data Controller and a Data Processor. **These are two separate applications that incur two separate fees.**

- **Data Controller**

A public and private organization, not for profit Entities or individual Processing or dealing with Personal Data of individuals that are located in Kenya, and determine the purpose of Processing that Personal Data are required to register as Data Controllers. This could be for internal purposes such as HR & Payroll or as part of an Entities core business such as provision of professional services.

- **Data Processor**

A processor is a public and private organization, not for profit Entities or individual Processing Personal Data on behalf of a Data Controller. There must be a **contract between the processor and the controller that clearly defines this relationship**. The processor has no decision-making power on the Personal Data that it is Processing and is bound by the terms of engagement in the contract.



# DATA PROTECTION

Know your rights

- × Right to access
- × Right to be forgotten
- × Right to object
- × Right to portability
- × Right to be forgotten
- × Right to be forgotten

## REGISTER ACCOUNT



### PRE-REGISTRATION PROCESS

Welcome to ODPC registration process. If this is your first time registration please select the first option, if you had earlier started registration but did not complete the process due to internet problems, power or other circumstances, select the second option.

- First time registration
- Resuming registration

### REGISTRATION REPRESENTATIVE

<p>Name *</p> <input type="text" value="Representative Name"/>	<p>Phone Number *</p> <input type="text" value="Representative phone number"/>
<p>Email Address *</p> <input type="text" value="Email Address"/>	<p>Institution *</p> <input type="text" value="Institution"/>
<p>Relation to institution * ⓘ</p> <input type="text" value="Indicate self if appropriate, or your role or relation to the institution."/>	

## STEP 2: PROVIDE BASIC INFORMATION

- Provide details of your Entity including uploading your Entity's establishment documents. If you are an individual Processing Personal Data, your establishment document will be your National ID or Passport.
- If you have a Data Protection Officer, you can provide contact details of the appointed data protection Office. This could be a Data Protection Officer that acts for many Entities, including a group of companies; or a Data Protection Officer that acts only for your Entity.
- If you have not appointed a Data Protection Officer, you can provide a contact person of an individual the Office can liaise with, should the Office need to.
- Alternatively, you may wish to leave the Data Protection Officer section blank.

The screenshot shows the 'BASIC DETAILS' section of the DPC registration form. The form is titled 'Account submitted' and includes the following fields:

- Institution/Individual Name \***: Company/institution Name
- Postal Address \***: Postal Address
- Country \***: Kenya (dropdown), National (dropdown)
- Telephone Number \***: Telephone Number
- State or County Department \***: County Department (dropdown)
- Legal Establishment \***: Select your legal establishment (dropdown)
- Establishment Document \***: Choose File (No file chosen)

Below the main form, there is a section for **Data Protection Officer(Optional)** with a note: 'Fill this section if your institution has a dedicated data protection officer.' The field for 'Name of the officer' is visible at the bottom.

### STEP 3: IDENTIFY THE CLASSES AND CATEGORIES PERSONAL DATA PROCESSED

- For 'description of Personal Data', you should provide only the kinds/ types of Personal Data you process. For example, if an organization collects names and identification numbers of clients, you should write only the **classes of information** processed, which are "names" and "ID numbers". **Do not write the actual names and telephone numbers of all your clients.**
- For 'category of Data Subjects', you should list the categories of individuals which relate to the list of data that you have stated. For example, employees, customers, shareholders, directors, suppliers, students, participants are categories of individuals.
- For 'purpose of Processing', you should state the reasons for the Processing. For example, payroll, invoicing, know your client, due diligence, etc.

The screenshot displays a web interface for 'REGISTER ACCOUNT'. At the top, a progress bar shows eight steps: Verification, Basic Details, Personal Data (highlighted in blue), Sanitize Personal Data, Transfer of Data, Measures of Protection of Personal Data, Employees and Turnover, and Login Options. Below the progress bar, a green message states: 'Basic details saved successfully. Since this is a first time registration, a resume code has been generated and sent to your email address.' The 'PERSONAL DATA' section contains three input fields: 'Category' with a dropdown menu (example: 'e.g. employee, client, student, supplier, shareholder, etc.'), 'Description' with a text area (example: 'description of personal data to be processed e.g. name, address, identification number'), and 'Purpose' with a text area (example: 'purpose of processing e.g. for payroll, invoicing, Know Your Client (KYC)'). A 'Add Personal Data Group' button is located to the right of the Category field. At the bottom right, there are 'Previous' and 'Next' buttons.

## STEP 4: LIST THE SENSITIVE PERSONAL DATA PROCESSED

- Please tick the box applicable or not applicable.
- If applicable, state the purposes for which you are Processing the relevant sensitive Personal Data.
- If not applicable, please proceed to the next step.

The screenshot shows a web form titled 'SENSITIVE PERSONAL DATA' with a progress bar at the top. The progress bar includes steps: Verification, Basic Details, Personal Data, Sensitive Personal Data (current step), Transfer of Data, Measures of Protection of Personal Data, Employees and Trustees, and Login Credentials. The form contains a message 'Personal details saved successfully' and a question: 'Do you handle any sensitive data. If yes, Please tick yes, and then describe the purpose.' Below this are radio buttons for 'Yes' and 'No'. A table lists categories of sensitive data with corresponding 'Purpose' input fields:

Category	Purpose
Race or ethnic origin	Describe the purpose
Property Details (including financials)	Describe the purpose
Religious, philosophical residence and beliefs	Describe the purpose
Marital (include spouse and children details)	Describe the purpose

## STEP 5: TRANSFER OF PERSONAL DATA OUTSIDE KENYA

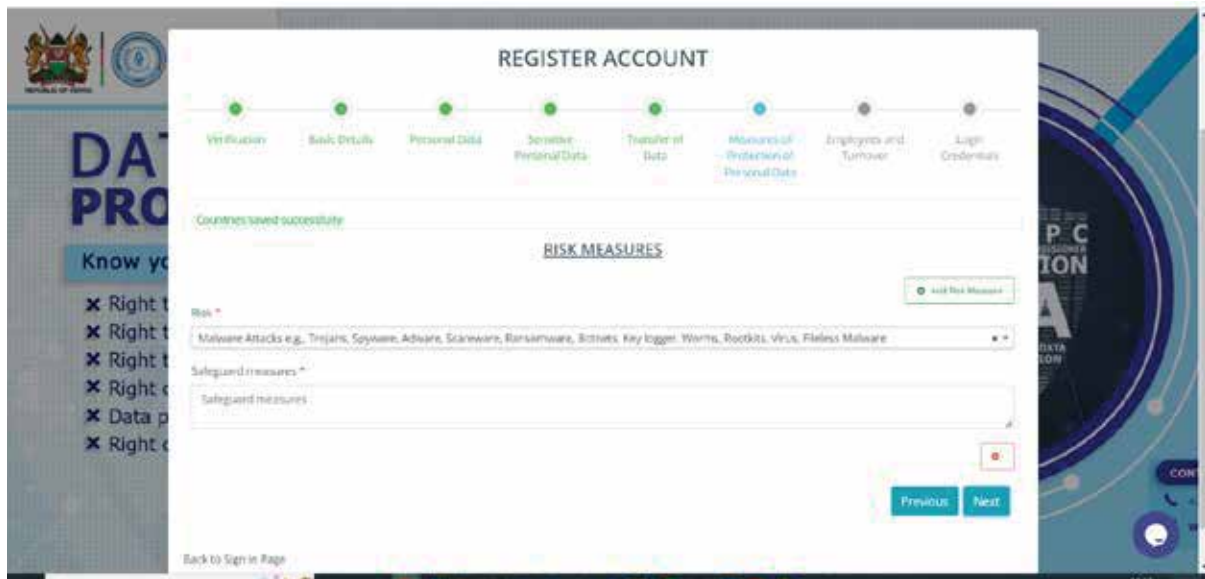
- If you transfer Personal Data outside Kenya, use the drop-down function to select all the countries where your Entity transfers or will transfer Personal Data to.
- If not applicable, please proceed to the next step.

The screenshot shows a web browser window displaying the 'REGISTER ACCOUNT' form for the Office of the Data Protection Commissioner, Republic of Kenya. The form is titled 'REGISTER ACCOUNT' and has a progress bar with eight steps: Verification, Basic Details, Personal Data, Sensitive Personal Data, Transfer of Data (current step), Measures of Protection of Personal Data, Employees and Turnover, and Login Credentials. A green message states 'Sensitive details saved successfully'. The 'TRANSFER OF DATA' section asks 'Does your data reside outside Kenya. If yes please list the countries.' with radio buttons for 'No' and 'Yes'. Below this is a 'List of Countries:' label and a text input field with the placeholder 'Select your countries'. 'Previous' and 'Next' buttons are at the bottom right, and a 'Back to Sign in Page' link is at the bottom left.



## STEP 6: RISKS AND SAFEGUARDS FOR PROTECTION OF PERSONAL DATA

- You should list the risk(s) to Personal Data, for example, unauthorized access, unlawful disclosure, theft amongst others.
- You should also describe the safeguards and security measures in place to protect the Personal Data. For example, physical access control, fine grained access control, visitors' log book, privacy notice, information security policy (firewall, antivirus amongst others), email policy amongst others.



The screenshot displays a web form titled "REGISTER ACCOUNT" with a progress bar at the top. The progress bar includes steps: "Verify Email", "Basic Details", "Personal Data", "Sensitive Personal Data", "Transfer of Data", "Measures of Protection of Personal Data" (which is the current step), "Employee and Turnover", and "Login Credentials". Below the progress bar, a message states "Countries saved successfully". The main section is titled "RISK MEASURES" and contains a form with the following fields:

- Risk \***: A dropdown menu with the selected option "Malware Attacks e.g., Trojans, Spyware, Adware, Scanware, Botsware, Botnets, Keylogger, Worms, Rootkits, Virus, Fileless Malware".
- Safeguard measures \***: A text input field with the placeholder text "Safeguard measures".

At the bottom right of the form, there are "Previous" and "Next" buttons. A "Back to Sign in Page" link is located at the bottom left of the form area.

## STEP 7: IDENTIFICATION OF PAYMENT TIER

- Please tick the tier to which your Entity belongs: either micro/small, medium or large Entity. This will assist in generating an invoice.
- If you are a government Entity or non-profit making Entity, your fee is calculated automatically.
- If you have an annual Turnover/ Revenue of less than Kshs. 5 million **and** less than 10 employees, you must identify which non-exempt mandatory registration Entity your Entity belongs to.
- If your Entity does not engage in any of the activities on the non-exempt mandatory registration Entity list, you can proceed to cancel your application.

**REGISTER ACCOUNT**

Verification Basic Details Personal Data Sensitive Personal Data Transfer of Data Measures of Protection of Personal Data Employees and Turnover Login Credentials

Risk measures saved successfully

**EMPLOYEES AND TURNOVER**

Since you have selected a Government institution category, You are not required to specify the number of employees or turnover.

I confirm that the reported information is correct and I understand and hereby accept the responsibility of Data Protection Act & Regulations

Previous Next

Back to Sign In Page

## STEP 8: PAYMENT OF REGISTRATION FEE

- A pdf form of your application will be made available to download at this stage.
- The registration fee payable will be calculated based on the information provided and an invoice issued.
- Payment can be made by:
  - i. Mobile money
  - ii. Credit Card
  - iii. Cheque
  - iv. Cash deposit to the relevant bank.

The screenshot shows a web interface for paying a registration fee. At the top, a message reads: "Please follow the instructions below and pay the registration fee of KSh. 1.00 in order to complete your application. Once you complete your payment, your application will be submitted automatically for approval." Below this, a section titled "PLEASE FOLLOW the steps below" contains a list of instructions: 1. Go to M-PESA on your phone, 2. Select Pay Bill option, 3. Enter Business no, 4. Enter Amount as KSh. 10000, 5. Enter the Account No. 100, 6. Enter your M-PESA PIN and send. A red "Manual Pay" button is visible. Below the instructions, there are sections for "Bank" and "Cheque" with plus signs. At the bottom right, there is a green "Done" button with a checkmark and a circular arrow icon.

## STEP 9: REGISTRATION CERTIFICATE

- The Office issues a registration certificate to an applicant for registration as a Data Controller or a Data Processor who meets the requirements for registration within fourteen days (14) days from the date of receipt of the registration application and payment.
- The registration certificate will be valid for a period of two years unless revoked or varied.

## **6. CANCELLATION OR VARIATION OF REGISTRATION CERTIFICATE**

The office may vary the certificate of registration where a data controller or data processor applies for the variation.

The Office may cancel the registration certificate before its date of expiry if the registration certificate holder:

- (i) applies for the cancellation
- (ii) has submitted false or misleading information;
- (iii) fails to comply with requirements of this law or terms and conditions specified in the certificate.

## **7. CHANGE IN PARTICULARS**

Where there is a change in any of the particulars in your application, your Entity must, within 14 days of the date of the change, notify the Office in writing or electronically of the nature of the change through [registration@odpc.go.ke](mailto:registration@odpc.go.ke).

## **8. OFFENCES**

A Data Controller or a Data Processor who:

- (a) processes Personal Data without registering in accordance with the Regulations;
- (b) provides false or misleading information for the purpose of registration; or fails to renew a certificate of registration and continues to process Personal Data after the expiry of the certificate, commits an Offence.



**OFFICE OF THE DATA PROTECTION COMMISSIONER**

P.O. BOX 30920-00100

NAIROBI

[info@odpc.go.ke](mailto:info@odpc.go.ke) | [www.odpc.go.ke](http://www.odpc.go.ke)