



**Prime Minister's Office**  
Data Protection Office

Volume 2

# **Registration Classification & Guidance Notes for Application of Data Controllers & Data Processors**



# **Registration Classification & Guidance Notes for Application of Data Controllers & Data Processors**

Volume 2

**Mrs Drudeisha MADHUB,**

*Data Protection Commissioner*

***Contact Details***

Tel No.: 201 3604

E-mail: [pmo-dpo@mail.gov.mu](mailto:pmo-dpo@mail.gov.mu)

Website: <http://dataprotection.gov.mu>



# TABLE OF CONTENTS

	Page
1. What is Registration?	5
2. Who are required to register?	5
3. Multiple/separate registrations	5
4. Public Register	6
5. Status of applicant while the application for registration is pending	6
6. How do I renew my registration?	6
8. Refusing your application for Registration	6-7
9. Completing the Registration Application Form	7-13
10. Fees	14



# REGISTRATION

DATA PROTECTION ACT 2004  
SECTION 31

## 1. What is Registration?

Under the Data Protection Act, data controllers and data processors who control or process the contents and use of personal data must register details with the Data Protection Commissioner.

Registration is a simple process which entails submitting the form to the Data Protection Commissioner setting out the type of personal data you keep on computer, for what purpose/purposes you keep it and to whom the information is disclosed, so that these practices can be made available to the public for viewing (Public Register). The form is available on the website <http://dataprotection.gov.mu>.

## 2. Who are required to register?

Under Section 33 of the Data Protection Act 2004, certain categories of data controllers are required to register provided that the personal data is held by them in an automated or non-automated form, that is, a structured set of information forming part of a relevant filing system.

## 3. Multiple/separate registrations - Section 34(2)

If you keep personal data for two or more purposes, then you are required to apply for a separate registration for each of those purposes, for instance, personal data relating to employees and the activities of organisation represent two categories requiring separate registrations. Separate registrations allow you to reflect the clear distinctions between different databases in your organisation, in terms of the nature and uses of the personal data involved, the assignment of control over and responsibility for the databases, and the legal compliance arrangements.

If you wish to make an application for a separate registration, use a separate registration form.



#### **4. Public Register**

The register of data controllers and processors is a public register intended to bring transparency to the processing of personal data. All register entries are now available on this office's website <http://dataprotection.gov.mu>

#### **5. Status of applicant while the application for registration is pending**

Under Section 33 of the Data Protection Act, it is an offence to keep personal data as a data controller or data processor unless you are registered.

#### **6. How do I renew my registration?**

The registration period is for one year. You are required under the Act and the Data Protection Regulations 2009 to renew your registration annually and apply for renewal within three months before the date of expiry of your registration. The appropriate fee should be included with your signed application for continuance.

#### **7. Failure to Renew**

If you fail to renew, you will commit an offence and you will be liable to a fine not exceeding Rs 200, 000.- and to imprisonment for a term not exceeding 5 years and your details will be removed from the public register.

#### **8. Refusing your application for Registration**

Under Section 34 of the Data Protection Act, the Commissioner is required to accept an application for registration unless she reasonably believes that the details submitted by the applicant are insufficient, that other information requested has not been furnished or is insufficient, or that the applicant does not provide adequate safeguards for the protection of the privacy of individuals concerned or that the applicant is not a fit and proper person. If the Commissioner's office has queries regarding the details submitted, the applicant will be contacted to give him the opportunity to resolve the matter.



If sensitive data is held by the data controller or data processor, then the Commissioner will not accept the application unless she is satisfied that appropriate safeguards for the protection of the privacy of the individuals concerned will be provided.

If your application is rejected, you will be informed in writing of the reasons for refusal and you also have a right to appeal against such a refusal to the ICT Appeal Tribunal within 21 days of the date the decision of the Commissioner is made known to you.

## **9. Completing the Registration Application Form**

Although the registration application form is largely self-explanatory, the following notes indicate the level of detail required to enable your application to be speedily processed. Please note that the suggested answers to particular sections of the form are provided for illustrative purposes only, and you will need to amend and/or supplement them to fit the particular circumstances of your organisation.

You should also note that not all of the details which you provide in your application form will be made available as part of the public register. Only the responses to sections 1 to 7 and 9 (inclusive) form part of the public register; the other details are required for the purposes of the office of the Data Protection Commissioner, and will be treated as confidential. For clarity, each section below includes an indication of whether the information under that section forms part of the public register.

# FORM DPO I

## Section 1: Name & Address

**This information forms part of the public register**

You should give the registered name of the company or person carrying on business. In the case of a partnership, you should give its name and list each of the partners. Foreign companies who have a presence in Mauritius and who are required to register must put the Mauritian address in Section 1.

**Note:** You must keep this office informed in writing of any change of address within **15** days of the change in address. Failure to do so is an **offence** under sections 35(3) and 35 A (3) of the Act. You must also notify this office in writing of the nature and date of any change in particulars to your registration form within 14 days of the change. Failure to do so is an offence under section 35 B of the Data Protection Act.

## Section 2: Compliance Person

**This information forms part of the public register**

You should give the name and/or job status of the individual in your organisation who will supervise the application of the Act within your firm, i.e, the person to whom this Office will address correspondence relating to your application and the person to whom members of the public will address any applications for access to their personal data under section 41 of the Act. It is sufficient to identify the contact person by title or position, e.g. "Finance Officer", "Secretary", "Senior, Executive Officer", "Director", or "Manager" etc. if you wish.

## Section 3: Description

**This information forms part of the public register**

This section is divided into 'Use of Personal Data' and 'Description of Personal Data'. You are required to identify the various uses, i.e. distinct areas or aspects of your work, for which personal data are held and to detail the types of personal data kept in respect of each use. Where the personal data held is what would normally be associated with that use, then it can be described briefly like "contact details" or "income details". If the data held would not normally be associated with that use, then that data should be described in detail, for example, Political

Membership, Racial Origin, etc. Personal data held for uses which are ancillary to your primary purpose, such as personnel and payroll data, should be recorded separately in the left hand column.

Below are two illustrative lists of:-

- (i) uses, services, schemes or areas where it is expected that personal data would be held i.e. appropriate to the left hand column of the form;
- (ii) brief descriptions of data that might be held in respect of those uses, schemes or areas i.e. appropriate to the right hand column of the form.

The lists below contain **examples** of what might appear in the two columns. Complete the form using your own knowledge of your business/organisation describing the personal data you process. In the table below, the personal data descriptions on the right are not matched to the "uses" on the left. When filling out the form you should match the information in both columns.

Use of Personal Data	Description of Personal Data
Savings & Loans	Contact Details
Insurance & Pensions	Income Details
Finance & Investment	Occupation
Human Resources	Property owned
Payment Services	Employment status
Training	Financial details/circumstances
Customer/Client/Patient Records	CV/Qualifications
Appointment Systems	Disability Information
Planning Application	Personal data in respect of
Grants	case/transaction/proceedings being undertaken
Banking Services	
Security	Medical history
Volunteers/Voluntary Workers	Amount of debt and circumstances
Library Services	Next of Kin
	Marital Status
	Transaction Details
	Employment records

**Keeping personal data of any description other than that specified in the register entry may involve the commission of an offence under sections 35 and 35A of the Act.**

## Section 4: Sensitive Data

### This information forms part of the public register

'Sensitive data' means any data of the types listed in section 2 of the Data Protection Act i.e. racial or ethnic origin, political opinions or adherence, religious beliefs or other beliefs of similar nature, physical or mental health, membership to trade unions, sexual preferences or practices, or the commission or alleged commission of an offence or criminal convictions. This section must be completed where such sensitive types of **personal data** are held. If the nature of your business is such that you may potentially hold all categories of sensitive **personal data** at some point, then it is advisable to select all categories.

Under heading (ii) of this section, you should state for which of the services/schemes or areas listed under section 3, the sensitive data are held.

## Security Measures

You should also indicate the measures you have taken to protect the privacy of the individuals about whom you keep sensitive data. You should note, in this regard, your legal obligation to use security measures that are appropriate to the sensitivity of the **personal data** in question. You should also note that the Commissioner is precluded under section 34(3) of the Data Protection Act from accepting an application unless she is satisfied that adequate safeguards are in place.

**Example:** Minimum security arrangements would normally include the following -

**Physical Safeguards** - 'Access to computers is restricted to authorised personnel only, premises alarmed and secure when not occupied'.

**Technical Safeguards** - 'Access to computer system is password-protected, PC workstation is subject to password-protected lock-out after period of inactivity, anti-virus software is in use, a firewall is used to protect systems connected to the internet.' [Note: for especially sensitive data, it is also advisable to use additional technical safeguards, such as routine encryption of files and multi-level access control.



## **Section 5: Purpose(s) for which you keep or use personal data:-**

### **This information forms part of the public register**

You should provide a general, but comprehensive, statement of the purposes for which you carry on your business, trade or profession. Here are some examples:

Administration/provision of health services

Administration/provision of life, pension and disability insurance and related services

Administration/provision of local authority services

Provision of banking and related services

Provision of medical care

Provision of dental care

Provision of legal services

The general statement of purposes must be sufficiently comprehensive to cover all the purposes for which the business is carried on since your statement of purposes will be copied into the register and it is an offence to keep or use personal data for any purpose not described in a register entry (sections 35 (1) (e) & 35 A).

The requirement to set out publicly your purpose for holding personal data makes an important contribution towards meeting your second data protection principle set out in the First Schedule of the Data Protection Act to obtain and process personal data 'only for any specified and lawful purpose'.

If the purpose for which personal data are processed is unrelated, then a separate application must be made for the unrelated purpose. For instance, employees and non-employees personal data represent two unrelated purposes.

## **Section 6: Disclosures**

### **This information forms part of the public register**

Section 29 of the Act requires inter alia that any disclosure of the data must be compatible with your specified purpose for holding the data. You should list in this section any third parties or recipients to whom you make such disclosures. You should note that the inclusion of a particular disclosure in your registration does not, of itself, make disclosure to that person legitimate.

In case of doubt, it is advisable to list the disclosure in any event.

**Example:** Possible disclosures are given below for illustrative purposes.

Use of Personal Data	Recipients
Savings & Loans Insurance & Pensions Finance & Investment Human Resources Payment Services Training Customer/Client Records Appointment Systems Planning Application Grants Banking Services Security Volunteers/Voluntary Workers Library Services	National Councils and Boards Local Authorities Government Departments Parastatal Bodies Banks and Insurance companies Other financial institutions, etc.
<p><i>Note: Knowingly to disclose <b>personal data</b> to a person who is not described in the entry, other than a person to whom a disclosure of such data may be made in the circumstances specified in section 52 of the Act, may involve an <b>offence</b> under section 29 of the Act.</i></p>	

You do not need to include transmissions of **personal data** to your employees or agents, to the extent that such transmissions are necessary to enable them to carry out their duties. Such transmissions do not fall within the definition of 'disclosures' under the Act. Similarly, you do not need to list disclosures which are permitted under Section 52 of the Act, that is, disclosures which are:

- required under any enactment or court order.
- necessary for the purpose of legal proceedings.
- necessary for the purpose of obtaining legal advice.
- necessary for the purpose of exercising legal rights.

## Section 7: Transfers abroad

This information forms part of the public register

This section relates only to **personal data** when transferred abroad.

**Example:** A possible transfer of personal data is given below for illustrative purposes

<i>Application: personnel / payroll / administration</i>		
<i>Country</i>	<i>Description of Data</i>	<i>Purpose of transfer</i>
France	Staff name, personnel/payroll number, salary details	Payroll administration

**Note:** Transferring **personal data**, directly or indirectly, to a place outside Mauritius other than one named or described in the entry may involve an **offence** under sections 35 and 35 A of the Act.

## Section 8: Public Information

This information **DOES NOT** form part of the public register

For example, the electoral register, a judgment from our courts, birth and marriage certificates, etc.

## Section 9: Fees

This information **DOES NOT** form part of the public register

Payment of the relevant fee must accompany the application.

**Payment should be made by cash or cheque or adjustment. Crossed cheques should be made payable to the "Government of Mauritius". Foreign cheques will not be accepted due to the clearing charges involved.**



## Current fees:

### 1. Data controller registration fee:

Having not more than 25 employees	1,000
Having more than 25 employees	2,000
In all other cases	800

### 2. Data controller renewal fee:

Having not more than 25 employees	750
Having more than 25 employees	1,750
In all other cases	550







