DESIGNATION AND CERTIFICATION OF DATA PROTECTION OFFICERS (DPOs)

The Data Protection Office has received a number of queries concerning the implementation of the Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026. This document provides guidance in response to queries received.

1. THE GENERAL RULE

Designation of Data Protection Officer

Under the Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026, the general rule is that a controller must designate a Data Protection Officer from a staff member of the organisation. The designated DPO is responsible for carrying out the duties stipulated under Regulation 4.

The designation of **more than one** Data Protection Officer (DPO) is optional and is not a mandatory requirement.

The controller must update the details of designated DPO(s) through the e-DPO Portal, using its administrator account, at the following link:

https://dpo.govmu.org/dpoPortal/login.jsf

Controllers are also encouraged to consult the "DPO Portal User Guide", in particular the section entitled "8. Register Data Protection Officer" available at:

https://dataprotection.govmu.org/Documents/2026/DPO%20Portal%20User%20Guide_V8-1.pdf

Certification

Certification relates to the knowledge, training and competence required of the person designated as DPO. The DPO is expected to possess the appropriate knowledge and ability to perform the duties prescribed under the Regulations. Existing Data Protection Officers or individuals holding international certifications such as PECB Certified Data Protection Officer, CIPP/E, CIPM or CIPT will still be required to complete the certification programme conducted by the Data Protection Office for the purposes of the Regulations. While such international certifications may demonstrate relevant knowledge and experience in the field of data protection and privacy, they do not replace the certification issued by the Data Protection Office for the purposes of Regulation 5(d)(ii).

Data Protection Officers who have also previously completed any data protection training or obtained any certificate issued by this office are still required to complete the certification programme prescribed under the Regulations.

The certification programme consists of:

- completion of an online training covering the principal provisions of the Data Protection Act and related requirements;
- physical attendance at training sessions delivered by trainers of the Data Protection Office;
- successful completion of a written examination; and
- issuance of a certificate by the Data Protection Office upon successful completion of the required training and examination.

The Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026 will come into force on 1 January 2027. Prior to that date, the Data Protection Office will issue a separate communiqué setting out the arrangements and modalities for the certification programme including registration, the training schedule, course fees, assessment and certification requirements. The communiqué will also indicate when registrations will open. Training sessions requiring physical attendance are expected to be organised in batches from 2027 onwards.

2. PROPORTIONATE CASE-BY-CASE REGIME

The case-by-case regime is strictly limited to organisations whose staffing or operational circumstances place them within one of the limited cases identified below. It is **not** an alternative regime available by choice to the general rule.

An organisation should approach the Data Protection Office for a case-by-case assessment only if it falls within one of the following limited cases:

- companies having no employees;
- Global Business Companies, Authorised Companies or investment holding companies having no employees;
- sole traders;
- micro or small organisations having only one or two directors and very limited personnel and no suitable staff to undertake the DPO role;
- organisations whose employees mainly perform field-based, manual or general-worker duties and which have no staff member whose responsibilities and organisational position make that person reasonably suitable to undertake the DPO role.

WHO SHOULD APPROACH THE OFFICE?

Only organisations falling within one of the limited cases listed above should request a case-by-case assessment from the Data Protection Office. The request should include the relevant information as set out in section 3 below for the office to consider the organisation's circumstances.

WHICH REGIME APPLIES TO ME?

THE KEY QUESTION **Does my organisation fall within one of the limited cases identified in Section 2 above?**	
↓ NO ↓	↓ YES ↓
NO – GENERAL RULE APPLIES Designate one or more DPOs from staff members and comply with the certification requirements. Do not submit a case-by-case request.	**YES – CASE-BY-CASE REGIME APPLIES** Approach the Data Protection Office for assessment and provide the relevant facts and supporting evidence. The Data Protection Office will assess the circumstances and advise on the appropriate designation, training and compliance arrangement.

3. INFORMATION TO BE SUBMITTED FOR A CASE-BY-CASE ASSESSMENT

Only an organisation that falls within one of the limited cases in Section 2 above should submit information and supporting evidence to the Data Protection Office for an assessment as follows:

1	the nature of the business and its activities
2	the number of employees or other staff members and the functions they perform
3	the directors, owners, partners or other persons responsible for managing the organisation
4	the categories and approximate volume of personal data processed
5	the number and categories of customers or other data subjects concerned
6	whether sensitive or higher-risk personal data are processed
7	the systems and applications used to process or store personal data
8	whether any processing activities are carried out in Mauritius or in connection with persons in Mauritius
9	where relevant, the role of a management company, administrator, service provider or other person involved in the organisation's day-to-day administration or personal data processing
10	any other relevant circumstances that may be determined by the Data Protection Office

SUPPORTING EVIDENCE AND VERIFICATION

The organisation must provide documentary evidence in support of the information submitted. The information may also be subject to verification, including an inspection, where considered appropriate.

4. ALTERNATIVE CAPACITY-BUILDING ARRANGEMENTS

Where, following a case-by-case assessment, the Data Protection Office determines that an alternative capacity-building arrangement is appropriate, the person concerned will not be required to undergo the same certification programme that applies under the general rule.

The capacity-building arrangement may include:

- ❖ a practical data protection workshop;

- a short capacity-building programme; or
- any other form of training determined by the Data Protection Office.

The purpose is to ensure that the person concerned acquires an appropriate practical understanding of the responsibilities arising under the Data Protection Act and the Regulations while taking into account the organisation's size, structure, resources and activities. More details regarding the capacity-building arrangement will be published on the DPO website in due course.

Following satisfactory participation, the person may be issued with a certificate of participation or other evidence confirming completion of the capacity-building arrangement determined by the Data Protection Office.

5. MANAGEMENT COMPANIES AND COMPANIES ADMINISTERED BY THEM

Management companies should distinguish between their own obligations and the obligations of each company or entity that they administer.

A Management Company should follow the normal designation and certification regime for the appointment of its own Data Protection Officer. It should not seek a case-by-case assessment merely because it administers other entities.

The Data Protection Officer of a Management Company does not automatically become the Data Protection Officer of the entities managed by that Management Company.

Managed Entity with Employees	Managed Entity with No Employees
A managed entity that has its own staff members should, as a general rule, designate a Data Protection Officer from among its staff and comply with the normal certification requirements.	A managed entity that has no employees or staff members from whom a Data Protection Officer can be designated should contact the Data Protection Office for a case-by-case assessment. For administrative convenience, a Management Company may submit to the Data Protection Office a consolidated list of managed entities having no employees and having substantially similar structural or operational circumstances for the relevant assessment. The Data Protection Office will thereafter advise on the appropriate designation and compliance arrangement.

6. DPO CONTACT DETAILS WHEN THERE ARE NO PHYSICAL PREMISES AND WEBSITE

Where an organisation does not have physical premises and does not operate a website, it should still ensure that the contact details of its DPO are accessible to data subjects through an appropriate alternative means.

Depending on the circumstances, this may include:

- official correspondence or communications addressed to data subjects;
- forms, agreements or other documents through which personal data are collected; or
- an official online platform or other electronic communication channel used by the organisation.

7. CAN A DATA PROTECTION OFFICER BE A FOREIGNER?

The Regulations do not require the Data Protection Officer to be resident in Mauritius but the Data Protection Officer must be an employee of the organisation. However, the designated officer must be accessible and able to effectively carry out the statutory functions under the Regulations.

8. KEY MESSAGES TO REMEMBER

1	The Regulations do not create any exemption for controllers regarding the designation and certification of Data Protection Officer(s).
2	Designation of a Data Protection Officer and certification are separate requirements.
3	First ask whether the organisation falls within one of the limited cases identified in Section 2.
4	If it does **not** fall within the defined limited cases, the general rule applies and **no** case-by-case request should be submitted.
5	If it falls within the defined limited cases, the organisation should approach the Data Protection Office for assessment. Any alternative capacity-building arrangement applies only after the office has assessed the case and advised accordingly.
6	The Data Protection Officer of a Management Company does not automatically become the Data Protection Officer of the entities managed by that Management Company.

Date of issue: August 2026