مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

Data Protection Officer Categories

Personal Data Protection Center

www.pdpc.gov.eg

Establishing a Professional Hierarchy for Data Protection Officers in Egypt

This document outlines the structured hierarchy for Data Protection Officers (DPOs) in Egypt, categorized into three distinct levels: Category A, Category B, and Category C. It details the qualifications, experience, certifications, and examination requirements for each category, ensuring a clear progression path and maintaining high standards in data protection practices. This framework aims to support the development of skilled DPOs and enhance data protection compliance across various sectors.

Table of Contents

I. General and Specific Requirements for DPO Categories 3

II. Shared Data Protection Officer (DPO) 7

III. Reassessment and Renewal of DPO Accreditation 7

IV. Voluntary Category Change During Accreditation Cycle 10

I. General and Specific Requirements for DPO Categories

<table>
<tr><th colspan="2">General Requirements (Applicable to All Categories)</th></tr>
<tr><td colspan="2">i. <u>Qualifications and Relevant Experience:</u> The applicant must possess appropriate academic qualifications or recognized professional certifications, in addition to having practical experience in fields relevant to personal data protection, in accordance with the standards approved by the Board of Directors of PDPC.
ii. <u>Successful Completion of Official Examinations:</u> The applicant must successfully pass the official examinations administered or accredited by PDPC, commensurate with the nature and scale of personal data processing activities for which registration is sought.
iii. <u>Good Standing and Integrity:</u> The applicant must not have been previously convicted of any offence involving moral turpitude or dishonesty.</td></tr>
<tr><th>Specific Requirements by Category</th><th>Sector Examples</th></tr>
<tr><td colspan="2"><u>Category A – Lead DPO</u>
More than 2,000,000 records (no maximum limit)</td></tr>
<tr><td>A candidate must meet one of the following two criteria:

1. Professional Experience Pathway:
○ A minimum of 3 to 5 years of proven experience in the field of data protection, privacy management, or a closely related discipline.

OR
2. Certification Pathway:
○ The applicant shall be certified by a recognized international organisation in the field of personal data protection, privacy, information security, or cybersecurity, including but not limited to:
• International Association of Privacy Professionals (IAPP)
• ISC2
• PECB</td><td>- Telecom companies and mobile network operators
- Major private hospitals, healthcare networks, and diagnostic centers
- Technology companies with large user platforms and cloud services
- Ride-hailing and transportation apps (e.g., Careem, Uber)
- Digital wallets, fintech startups, and payment processing platforms (non-bank)
- Large e-commerce platforms and marketplaces (e.g., Jumia)
- Data analytics firms managing big data and advanced consumer profiling
- Cloud service providers and data centers
- Social media platforms, content-sharing, and community apps</td></tr>
</table>

• **ISO-accredited or equivalently recognized certification bodies** ○ The applicant must hold **at least two (2) relevant professional certifications** in data protection, information security, or cybersecurity, **or** demonstrate completion of **no less than fifty (50) documented training credit hours** in areas touching upon, supporting, or intersecting with data protection, information security, cybersecurity, risk management, governance, compliance, or related digital, legal, or technical domains, issued or accredited by recognized professional bodies, academic institutions, or accredited training providers. In both cases, the candidate must successfully pass **PDPC's customised Lead DPO exam** with a score of **more than 80%.**	- National and multinational retail chain stores with CRM and loyalty programs - Large insurance companies - Large travel and hospitality aggregators (online booking, ticketing) - Telecommunications infrastructure providers and ISPs - Online education platforms with extensive user databases - Large-scale logistics and supply chain companies - Financial technology platforms offering credit scoring, loans, or insurance products - Healthtech companies managing patient records and telemedicine platforms - Large hospitality chains and hotel groups with extensive guest data - Energy sector companies managing consumer data - Large-scale marketing technology platforms and ad tech companies - Major entertainment event organizers and ticketing platforms - Customer service centers (call centers, support desks)
<u>Category B – Advanced DPO</u> **Up to 2,000,000 records**	
A candidate must meet **one** of the following two criteria**:** **2. Professional Experience Pathway:** ○ A minimum of **2 to 3 years of experience** in data protection or a relevant field, such as legal compliance, information security, IT governance, or internal audit.	- Large private clinics, diagnostic labs, and specialized medical centers - Private schools and universities - HR and recruitment firms handling employee records - Medium-sized e-commerce platforms

OR **2. Certification Pathway:** ○ The applicant shall be **certified by a recognized international organisation** in the field of personal data protection, privacy, information security, or cybersecurity, including but not limited to: • **International Association of Privacy Professionals (IAPP)** • **ISC2** • **PECB** • **ISO-accredited or equivalently recognized certification bodies** ○ The applicant must hold **at least one (1) relevant professional certification** in data protection, information security, or cybersecurity, **or** demonstrate completion of **no less than thirty (30) documented training credit hours** in areas touching upon, supporting, or intersecting with data protection, information security, cybersecurity, risk management, governance, compliance, or related digital, legal, or technical domains, issued or accredited by recognized professional bodies, academic institutions, or accredited training providers. In both cases, the candidate must pass **the PDPC's customised Advanced DPO exam** with a score of **more than 70%.**	- Delivery & logistics companies operating at city or municipal level - Property management firms overseeing large residential/commercial complexes - Medium-scale fintech firms (non-banking digital wallets, payment gateways) - Private transportation companies (bus operators, shuttle services) - Medium to large travel agencies and tourism operators - Private universities and language schools - Hospitality chains (small hotel groups, guest houses) - Insurance companies - Data analytics firms handling aggregated personal data - Private security companies managing access control and surveillance data - Medium-sized tech startups with user data platforms - Fitness chains and sports clubs with member health data
<u>Category C – Entry-Level DPO</u> **Up to 100,000 records**	
A candidate must meet **all** of the following criteria: ○ **Experience:** • **Between 0 to 1 year of experience in data protection or a related field.** ○ **Certification:** • **Not required** at this level. ○ **Exam Requirement:**	- Retail stores (non-chain) - Cafés & restaurants - Real estate agencies - Small e-commerce shops - Salons & spas - Fitness centers & gyms - Photography studios

• Must pass the **PDPC's customised Entry-Level DPO exam** with a score of **more than 60%.**	- Tutoring centers / training institutes/ language institutes - Event planning companies - Home services (cleaning, maintenance) - Small travel agencies - Local courier and delivery services - Local car repair shops and garages - Small-scale NGO offices or community groups (non-sensitive data) - Small manufacturing workshops - Local printing and publishing houses - Small-scale agricultural businesses and cooperatives - Local retail pharmacies (that do not save/retain sensitive health data) - Community sports clubs and associations - Small-scale import-export traders - Daycare centers and nurseries - Event equipment rental services - Independent consultancy firms (design, IT, marketing) managing customer databases - Small retail markets (e.g., textile, hardware)

Important Note:

Final categorisation of DPOs shall be subject to the **discretion of PDPC**, based on a comprehensive evaluation of the applicant's **qualifications, professional background, documented training, certifications, and practical experience**. For this purpose, the PDPC may conduct a **formal assessment interview** to evaluate the applicant's technical competence, legal understanding, applied knowledge, and professional judgment relevant to the assigned category.

PDPC reserves the right to **assign or reassign applicants** to the appropriate category where justified, and to **approve justified exceptions** to the standard criteria on a case-by-case basis, in line with the overarching objective of ensuring effective and responsible data protection oversight.

II. Shared Data Protection Officer (DPO)

Without prejudice to the provisions of the Personal Data Protection Law No. 151 of 2020 and its Executive Regulation, an organisation may appoint a **shared DPO**, provided that such arrangement is established through a **clear and binding contractual agreement** defining the scope of services, responsibilities, and accountability of the DPO. In all cases, the shared DPO shall perform their duties with **full independence**, shall not receive instructions regarding the exercise of their statutory functions, and shall **report directly to the highest administrative or executive level** within each concerned organisation. The appointment of a shared DPO shall be subject to the **prior review and acceptance of PDPC**, which retains the right to assess the adequacy of the arrangement and to reject or require modification thereof where necessary to ensure effective and independent data protection oversight.

III. Reassessment and Renewal of DPO Accreditation

To ensure sustained alignment with national data protection objectives, the PDPC adopts a strategic reassessment framework applicable to all registered DPOs. This framework reinforces accountability, promotes continuous professional development, and enables PDPC to proactively respond to emerging risks and evolving sectoral demands.

A. Purpose of Reassessment

The periodic reassessment process is designed to:

- Ensure that accredited DPOs continue to demonstrate **competence, integrity, and readiness** in managing data protection obligations.
- Adapt to **technological developments**, sectoral changes, and updates in **regulatory and legislative frameworks**.
- Promote a **culture of continuous learning and professional excellence** in the field of data protection.
- Strengthen the **alignment** between DPO capabilities and the scale, complexity, and sensitivity of data processing operations.

B. Reassessment Cycle

All accredited DPOs shall undergo a comprehensive reassessment **every three (3) years** from the date of initial accreditation or last renewal. PDPC may also initiate reassessment at any time based on sectoral developments, individual performance concerns, or organisational changes.

C. Components of Reassessment

1. **Capability Review**

- Evaluation of the DPO's **continued effectiveness** in fulfilling regulatory and organisational responsibilities.
- Alignment of the DPO's **role and scope** with the category assigned (A, B, or C).

2. Professional Development and Learning

- The reassessment process prioritizes **demonstrable professional experience** in data protection roles during the accreditation period.
- Where relevant experience is **insufficient, interrupted, or not clearly verifiable**, the DPO must demonstrate **active engagement in professional development**, including:
  - Participation in **PDPC-accredited** or **recognized training programs**
  - Continuing education relevant to data protection law, or data governance
  - Familiarity with **emerging regulatory and technological issues**, such as
    - ✓ AI and automated decision-making
    - ✓ Cross-border data transfers
    - ✓ Data breach response and incident management
    - ✓ Privacy-by-design and accountability models

3. Regulatory Engagement and Conduct

- PDPC shall conduct an internal **review of the DPO's file** maintained by PDPC, which includes records of the DPO's **regulatory performance** throughout the accreditation period.

- This assessment shall cover:
  – The DPO's **compliance history** and adherence to data protection obligations.
  – **Responsiveness and cooperation** with PDPC communications, requests, or supervisory inquiries.
  – The DPO's level of **proactive engagement** with regulatory updates, guidance documents, and capacity-building initiatives issued by PDPC.
  – Any **complaints, breach notifications, or formal enforcement actions** that have involved or implicated the DPO.

4. **Sectoral Relevance and Role Evolution**

- Review of changes in the **DPO's industry context**, organisation size, and nature of data handled.
- Revalidation of the **category assignment** to ensure strategic fit with the entity's data risk profile.

5. **Ethical and Legal Standing**

- Confirmation that the DPO remains in **good standing**, with no disqualifying legal, ethical, or disciplinary findings.

D. Reassessment Outcomes

Based on the reassessment, PDPC may take one or more of the following actions:

- **Renew accreditation** for a further three-year term.
- **Recommend upskilling or targeted training** where gaps are identified.
- **Adjust the DPO's category assignment** based on updated privacy management responsibilities or risk exposure.
- **Revoke or suspend accreditation** in cases of significant non-compliance or loss of eligibility.

Important Note: The final decision regarding category placement, reassignment, or exceptions shall remain at the sole discretion of PDPC, based on a holistic review of the DPO's profile and the broader regulatory priorities **and shall be issued within a period not exceeding fifteen (15) working days from the date of receipt of the complete reassessment submission**.

IV. Voluntary Category Change During Accreditation Cycle

A DPO may submit a request to upgrade or change their assigned category at any time during the three-year accreditation period. Such requests shall be reviewed by PDPC based on the following principles:

1. Eligibility for Re-Categorisation

- A DPO may be considered for re-categorisation during the active accreditation cycle upon submission of a formal request and subject to the approval of PDPC. To be eligible, the DPO must demonstrate clear and verifiable evidence of alignment with the **criteria of the target category**, as set forth in the official accreditation framework, **including**:
    - ✓ Demonstrated **expansion in the scale, complexity, or sensitivity** of personal data processing activities under the DPO's responsibility;
    - ✓ Acquisition of relevant **professional certifications**, **academic qualifications**, or completion of recognized **specialized training**;
    - ✓ Documented **practical experience** in data protection that meets or exceeds the threshold defined for the target category;
    - ✓ Maintenance of a **compliance record free of major violations**, with a proven track record of professional integrity and effective regulatory engagement.

2. Documentation and Supporting Evidence

- The DPO must submit a formal request for re-categorisation, accompanied by comprehensive documentation that clearly substantiates their eligibility for the higher category. The submission must include, at a minimum:
    - ✓ An updated **professional dossier** detailing current responsibilities, role evolution, and scope of data processing activities;
    - ✓ Verified copies of any **new academic qualifications**, **professional certifications**, or **training programs** completed since initial accreditation (if requested by PDPC);
    - ✓ Official evidence from the employing entity confirming the **volume, nature, and sensitivity of personal data** currently handled by the DPO;
    - ✓ Any additional supporting material that may assist PDPC in conducting a holistic evaluation of the DPO's qualifications and readiness for category advancement.

PDPC retains full discretion to assess the sufficiency of the submitted evidence and may request additional information as part of the evaluation process.

3. Assessment Process

- Upon receipt of a re-categorisation request, PDPC shall initiate a comprehensive review to evaluate the applicant's suitability for the proposed category. This process includes, but is not limited to, the following steps:

  ✓ **Verification of Submitted Documentation:** PDPC will rigorously examine all supporting materials submitted to substantiate eligibility, ensuring their authenticity, relevance, and completeness.

  ✓ **Competency Evaluation:** The applicant may be required to undergo additional assessments, including PDPC's customised examination relevant to the requested category, to validate their knowledge and capabilities.

  ✓ **Review of Regulatory Compliance:** PDPC will assess the DPO's historical compliance record, including responsiveness to regulatory inquiries, involvement in any breaches or complaints, and overall adherence to data protection standards.

  ✓ **Final Determination:** Based on the outcomes of the above steps, PDPC will render a decision regarding the re-categorisation request. The decision will be communicated in writing to the applicant, with the effective date of any category change clearly specified.

4. Decision and Notification

- The final decision will rest with PDPC based on merit and documented qualifications, and shall be issued within a period not exceeding fifteen (15) working days from the date of receipt of the complete submission.
- If approved, the new category assignment will take effect immediately, with the **three-year cycle resetting from the date of reclassification**.

Important Note: PDPC reserves the right to deny re-categorisation requests if the DPO fails to meet the full requirements, or if there are pending compliance concerns.