

ANNUAL REPORT

2025





Data Protection Office

2025

ANNUAL REPORT

17th Edition



TABLE OF CONTENTS

MISSION AND VISION	1
OUR MISSION	1
OUR VISION	1
FOREWORD BY THE HONOURABLE MINISTER.....	2
FOREWORD BY THE COMMISSIONER	3
ADVANCING PRIVACY RIGHTS AND GOVERNANCE IN MAURITIUS	4
REPORT OF THE UN SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY	5
DATA PROTECTION OFFICE (DPO)	6
ORGANISATION STRUCTURE	7
 BUDGET FINANCIAL YEAR 2025 – 2026.....	 8
I. HUMAN RESOURCE REQUIREMENTS.....	8
a) Chart on human resources requested versus number of officers in post	8
b) Other human resources required	9
II. RUNNING COST OF THE OFFICE	9
 2025 HIGHLIGHTS.....	 10
I. 2025 PICCASO AWARDS AFRICA.....	11
II. 2025 GLOBAL TOP 50 WOMEN LEADERS	12
III. 15 TH ANNUAL CONFERENCE AND 17 TH GENERAL ASSEMBLY OF THE ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES (AFAPDP)	13
IV. WORKSHOP ON DATA PROTECTION DAY	14
V. MEMORANDUM OF UNDERSTANDING (MOU) BETWEEN DPO AND BANK OF MAURITIUS	15
VI. VISIT OF THE PRESIDENT OF THE FRENCH REPUBLIC	15
VII. MAURITIUS NATIONAL DATA STRATEGY (NDS).....	16
VIII. MOU BETWEEN DPO, COMPUTER EMERGENCY RESPONSE TEAM OF MAURITIUS (CERT-MU) AND MAURITIUS POLICE FORCE (MPF)	16
IX. AMENDMENTS TO THE DATA PROTECTION ACT FOR EU ADEQUACY	17
X. GUIDE ON ARTIFICIAL INTELLIGENCE AND DATA PRIVACY	17

ACTIVITIES IN 2025	18
I. FINANCIAL STATUS	19
(a) Revenue collected	19
II. INTERNATIONAL COOPERATION.....	19
a) Participation with international organisations	19
Organisation Internationale de la francophonie (OIF).....	19
b) Participation with regional and international organisations.....	20
1. Southern African Development Community (SADC)	20
2. Africa Digital Rights Hub (ADRH).....	21
3. Council of Europe (CoE)	22
4. Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP)	22
5. Identification for Development(ID4) Africa 2025	22
(c) Other virtual meetings	23
I. OECD.....	23
II. Sensitisation	23
III. Enforcing Data Protection.....	31
IV. IMPROVING LEGAL PROTECTION	34
(a) Supreme Court Cases:	34
(b) Intermediate Court Cases:.....	34
(c) Industrial Court Cases:	34
V. REGISTRATION OF CONTROLLERS AND PROCESSORS	34
VI. REQUESTS FOR LEGAL ADVICE	34
VII. ADVISORY /STAKEHOLDER ROLE IN PROJECTS.....	35
VIII. PERSONAL DATA BREACH NOTIFICATIONS.....	35
IX. DATA PROTECTION IMPACT ASSESSMENTS	36
X. TRANSFERS OF PERSONAL DATA ABROAD	36
XI. CERTIFICATION	36
CAPACITY BUILDING	37
PROJECTS IN THE PIPELINE	38
I. REGULATION FOR DATA PROTECTION OFFICERS	38
II. E-PRIVACY REGULATIONS	38
III. FREEDOM OF INFORMATION BILL.....	38
IV. AMENDMENTS TO THE CONSTITUTIONAL RIGHT TO PRIVACY.....	39
V. DIGITAL FORENSICS LAB	39
VI. WORKSHOP ON DATA PROTECTION DAY 2026	39
RECOMMENDATIONS	39





List of ABBREVIATIONS

01

DPO

Data Protection Office

02

DPC

Data Protection Commissioner

03

DPA

Data Protection Act 2017

04

MITCI

Ministry of Information Technology,
Communication and Innovation

MISSION AND VISION

Our **MISSION**

Safeguarding the processing of your personal data in the present age of information and communication.

Our **VISION**

A society where data protection is understood
and practiced by all.

The right to privacy and data protection is primordial to the sanctity of any modern democracy.

The adoption of clear procedures for the collection and use of personal data in a responsible, secure, fair and lawful manner, by all controllers and processors.





FOREWORD by the HONOURABLE MINISTER

Mr Avinash RAMTOHUL
Minister of Information Technology,
Communication and Innovation

If data is power, then governance is responsibility.

And in 2025, Mauritius made a deliberate choice: not just to accelerate into the digital age, but to do so with clarity, structure and principle.

This Report captures a transition from a system managing compliance to a nation architecting trust. Because what is unfolding is bigger than regulation.

Across the world, data is expanding faster than institutions can adapt. Artificial Intelligence is advancing faster than societies can fully understand. In that space between innovation and uncertainty, countries either drift or they decide.

Mauritius has decided.

The launch of the National Data Strategy in January marked a turning point. For the first time, we are treating data not as fragmented information across institutions, but as a coordinated national asset, one that must be governed with discipline, shared with purpose and protected with rigour. It is about unlocking value, but never at the cost of trust.

This is where the work reflected in this Report becomes essential. The rising number of complaints, the increasing complexity of cases, the growing demand for guidance, these are not anomalies. They are indicators of a society stepping into digital maturity. Citizens are more aware. Institutions are more exposed. Expectations are higher.

This is precisely why data protection can no longer be seen as a technical function. It is now a national priority. At the same time, Artificial Intelligence is forcing a new conversation, not just about efficiency, but about control, accountability and ethics.

Our approach has been clear : we do not wait to regulate after disruption; we prepare before it. The development of our National AI Strategy, alongside the guidelines on Artificial Intelligence and Data Privacy, reflects this anticipation. These are not reactive measures. They are forward-looking instruments designed to ensure that innovation is anchored in responsibility from the outset.

We are embedding principles where it matters most, at design stage, at deployment stage and at decision stage. But strategy alone does not deliver outcomes. The realities outlined in this Report, capacity constraints, the need for stronger enforcement mechanisms, the urgency of skills development, remind us that transformation is not linear. It requires persistence, investment and coordination across every level of government and society.

Mauritius now stands at a defining intersection. We can follow global trends or we can set our own standards. We can react to change, or we can organise it. Our initiatives reflect a country that is choosing the latter. And in a world where speed often outpaces reflection, that choice may well be our greatest strength.



FOREWORD by the COMMISSIONER

Mrs Drudeisha MADHUB
(Barrister-at-Law)
Data Protection Commissioner

2025 built many foundational blocks on the local data protection field as my office registered a record-breaking number of complaints reported to it. Given the complexity of issues relating to these cases, we stretched our existing small resources to meet the growing expectations of the public, professionals and controllers and processors.

Coupled with the increasing positive awareness on the seriousness of data privacy, presentations and trainings were delivered to many organisations including workshops and conferences hosted by this office.

Legal opinions were delivered to many controllers and processors on the nature of their obligations under the Data Protection Act to support and enhance their data protection management functions. Hearings on cases registered at the office were conducted to provide parties with the opportunity to express their grievances for fruitful resolution of disputes.

A number of projects for 2025 have been worked by my office to ensure innovation becomes the guiding objective in each and every endeavour embarked upon by this office; namely the creation of a digital forensic lab to professionalise our investigations, the finalisation of a comprehensive guide on artificial intelligence and data protection to improve data governance, the Data Protection Amendment Bill, Regulations for data protection officers, E-Privacy Regulations, Freedom of Information Bill, the National Data Strategy and Digital Rights

to be included in the Constitution which are also included in the Digital Transformation Blueprint of MITCI 2025-2029.

This Office has also strengthened the country's position on the regional and international stage. In my capacity as President of the Association Francophone des Autorités de Protection des Données Personnelles, I had the privilege of contributing to high-level discussions on artificial intelligence, digital sovereignty and the protection of fundamental rights. By hosting the Association's Annual Conference and General Assembly in 2025 and advancing a resolution proposed by my office on the ethical governance of Artificial Intelligence, we demonstrated that influence is not determined by size, but by vision, credibility and the courage to lead and shape the digital future.

The path ahead is both demanding and full of promise. Our ambition is to build a regulatory authority whose financial independence, human resources and technical capabilities match the scale of its responsibilities.

The Data Protection Office will therefore continue to stand as a vigilant regulator, a trusted adviser and a firm guardian of privacy.

I would like to extend my profound gratitude to every member of my staff for their dedication and perseverance which have contributed to the advancement of the office.

ADVANCING PRIVACY RIGHTS AND GOVERNANCE IN MAURITIUS

The right to privacy is a cornerstone of democratic societies and a fundamental human right that underpins trust in the digital age. In an increasingly data-driven economy, the protection of personal data is no longer a peripheral concern but a national imperative.

In this context, the **Budget Speech 2025–2026**, “Paragraph 30 – Eighth, we are also amending the Data Protection Act to meet EU requirements.” represents a significant step towards enhancing Mauritius’ legal framework and progressing toward EU adequacy.

The **Government Programme 2025–2029** further outlines a comprehensive set of measures to strengthen the protection and management of personal and sensitive data to foster a culture of accountability, trust and respect for individual rights. It also highlights the role of the Constitutional Review Commission in advancing privacy protections within the broader human rights framework. In particular, the Programme provides that:

Paragraph 6 (c)

“The Commission will, inter alia, examine:

... (c) Amendments to be made to Chapter 2 of the Constitution to better protect fundamental rights, including new generation rights relating to: environment, technology, health, education and other economic, social and cultural rights provided under international treaties, and also to provide for the rights of Nature; and”

Paragraph 8

“... Government will strengthen measures pertaining to the protection and management of personal and sensitive data.

The Constitutional Review Commission will consider proposals to further consolidate the constitutional right to privacy. ...”

Paragraph 9

“... A Freedom of Information Act will be introduced to provide for more transparency in relation to the decisions of public institutions. ...”

These national priorities are further supported by the **Digital Transformation Blueprint 2025–2029** which positions data protection at the heart of Mauritius’ digital future. Notably, Enabler 5 – Data Protection and Artificial Intelligence focuses on transforming data into a valuable national asset. At the same time, Enabler 2 – Legal and Regulatory Reform underscores the necessity of aligning the legal framework with technological advancements guaranteeing the protection of citizen data and reinforcing public confidence in digital services.

The Data Protection Office remains committed to supporting and operationalizing these measures through effective regulation and enforcement. As the digital ecosystem continues to expand, the office will play a pivotal role in ensuring that innovation progresses hand in hand with the protection of fundamental rights.

REPORT OF THE UN SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY

The Special Rapporteur on the Right to Privacy, in her report (A/HRC/58/58/Add.1)¹ dated 15 January 2025, commended Mauritius for having one of the most robust and comprehensive regulatory systems for privacy and data protection in alignment with the EU General Data Protection Regulation and further acknowledged Mauritius as the first country in Africa to sign and ratify the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. She also highlighted a number of areas requiring further actions.

Key challenges and recommendations identified include:

- The Data Protection Office, which is under the administration of the Ministry of Information Technology, Communication and Innovation, has independent functions but does not have independent funding.
- In 2023, owing to a lack of funding, there were only two Data Protection Officers on staff to process 423 claims.
- DPO has requested police officers to be seconded to the office as enforcement presents the greatest challenge.
- It is mandatory for organisations to have Data Protection Officers although in practice many do not.
- More resources and investment are needed to provide training sessions on data processing for professionals as the private sector is very evolved.
- While Mauritius clearly places a high value on privacy, additional measures are needed to balance innovation, security and privacy by strengthening and coordinating oversight powers.
- The Data Protection Office requires more financial resources to improve public awareness and education so that individuals are better informed on how to protect their fundamental right to privacy.
- Data is an important asset and citizens need confidence and trust in their personal data. The protection of personal data is a shared responsibility that must be balanced with the right to access and disclosure; if data is overprotected, it can inadvertently enable corruption. Thus transparency, privacy by design, privacy impact assessments and regional and international standards for data protection mechanisms are essential tools.
- It is critical to implement preventive measures to address the challenges related to digitalization which can undermine the ability to protect one's privacy.
- To ensure that the legal framework on data protection remains strong and resilient, it must align with technological developments and ensure that legal safeguards are harmonised with international norms.

¹ <https://docs.un.org/en/A/HRC/58/58/Add.1>



DATA PROTECTION OFFICE (DPO)

DPO became operational since **16 February 2009** and enforces the provisions of the Data Protection Act 2017(DPA). The DPA strengthens the control and personal autonomy of individuals over their personal data in line with the principles of the European Union General Data Protection Regulation (GDPR) and the Council of Europe(CoE) Convention 108 and 108+.

As a regulator with enforcement powers, this office has the immense responsibility and mandate to:

- | | |
|---|---|
| a | Ensure compliance with the DPA and any regulations made under it |
| b | Issue or approve such codes of practice or guidelines for the purposes of the DPA |
| c | Maintain a register of controllers and processors |
| d | Exercise control on all data processing operations and verify whether the processing of data is done in accordance with the DPA |
| e | Promote self-regulation among controllers and processors |
| f | Investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under the DPA |
| g | Take such measures as may be necessary to bring the provisions of the DPA to the knowledge of the general public |
| h | Undertake research into, and monitor developments in, data processing, and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals |
| i | Examine any proposal for automated decision making or data linkage |
| j | Cooperate with supervisory authorities of other countries, to the extent necessary for the performance of its duties under the DPA, in particular by exchanging relevant information in accordance with any other enactment |
| k | Submit an annual report to the National Assembly |

ORGANISATION STRUCTURE

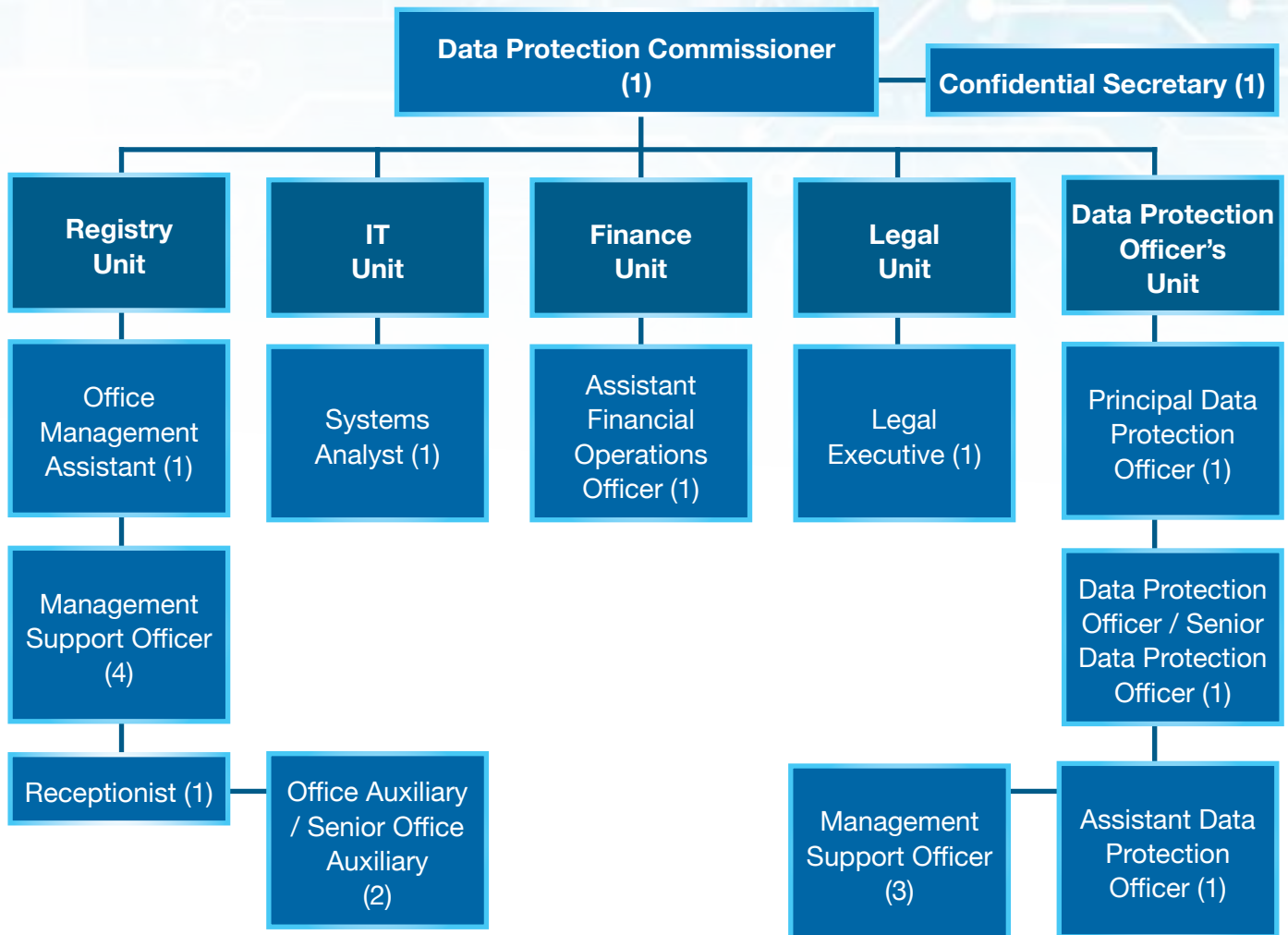


Figure 1: DPO Organisation Structure



BUDGET FINANCIAL YEAR 2025 – 2026

I. Human Resource Requirements

In 2025, the Office has continued to face significant operational challenges arising from a critical shortage of staff, which has impacted its capacity to effectively discharge its statutory mandate. The core functions of the Office, primarily undertaken by the Data Protection Officers' Unit, remain constrained by a limited workforce, with the number of officers in post being inadequate to meet the growing demands for regulatory oversight, compliance monitoring, enforcement activities, public engagement and international cooperation. This resource constraint has affected the Office's ability to deliver timely services to citizens and stakeholders across both the public and private sectors. In an effort to address these challenges and strengthen institutional capacity, the posts of Assistant Data Protection Officer and Data Protection Officer/Senior Data Protection Officer were advertised during the last quarter of 2025. However, these posts were still unfilled.

a) Chart on human resources requested versus number of officers in post

Grade	Number of posts requested in budget 2024-2025	Number of posts funded in budget	Actual number of officers in post
Data Protection Officer/ Senior Data Protection Officer	12	5	1 (4 posts vacant)
Assistant Data Protection Officer	6	3	1 (2 posts vacant)
Legal Executive	2	1	1
Principal Data Protection Officer	2	1	1
Deputy Data Protection Commissioner (Legal - new post)	1	Nil	Nil
Assistant Data Protection Commissioner (New Post) (Legal 1 and Information Technology 1)	2	Nil	Nil

b) Other human resources required

i. Police Unit

Under the provisions of the Data Protection Act, the police is collaborating with DPO by providing assistance in the investigation of complaints especially CCTV camera cases.

Furthermore, the Office continues to face constraints in strengthening legal enforcement mechanisms due to the absence of a dedicated prosecution and investigative support unit. The establishment of such a unit, including the secondment of police officers, remains essential to enhance the effectiveness of complaint handling, investigations and prosecution of offences under the Data Protection Act. The creation of this specialised unit would support the Office in ensuring that alleged violations are handled in a timely and efficient manner, facilitate evidence gathering and strengthen enforcement actions, thereby improving overall regulatory effectiveness and compliance across both the public and private sectors.

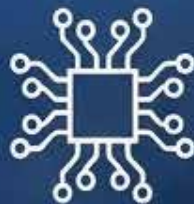
ii. Deputy Data Protection Commissioner

The establishment of the grade of Deputy Data Protection Commissioner remains essential to strengthen the leadership and operational capacity of the Office. The Deputy Data Protection Commissioner would provide strategic and administrative support to the Data Protection Commissioner and deputise to ensure continuity in decision-making, oversight and enforcement functions. However, this critical post has yet to be operationalised, as the Scheme of Service for the grade has not been prescribed to date. The absence of this position continues to impact succession planning, operational resilience and the effective discharge of the Office's expanding mandate.

II. Running cost of the office

The running cost of the office for the financial year 2025-2026 is Rs 8 million.

2025 HIGHLIGHTS



I. 2025 PICCASO Awards Africa

The 2025 PICCASO Awards Africa, held in Accra on 3 December 2025, recognised excellence and leadership in data protection, privacy and cybersecurity.

DPO was awarded the winner of the 2025 PICCASO Awards Africa

- Most Impactful Privacy Product for its innovative E-DPO Platform.



In addition, the Data Protection Commissioner served on the panel of expert judges for the 2025 PICCASO Awards Africa contributing her expertise to the evaluation and recognition of outstanding initiatives in the field.

II. 2025 Global Top 50 Women Leaders

The Women in GRC & Financial Crime Prevention (WGRCFP) recognised the Data Protection Commissioner, Mrs. Drudeisha Madhub, as one of the 2025 Global Top 50 Women Leaders in Governance, Risk, Compliance, Financial Crime and Fraud Prevention. This prestigious accolade celebrates women who are shaping international standards, driving regulatory innovation, and strengthening global financial integrity. Each honouree is recognised for her transformational leadership, unwavering commitment to integrity, and significant contributions to enhancing financial ecosystems worldwide.



WOMEN IN GOVERNANCE, RISK,
COMPLIANCE, FINANCIAL CRIME,
AND FRAUD PREVENTION

2025 GLOBAL TOP 50 WOMEN LEADERS IN GRC & FINCRIME PREVENTION -WOMENINGRCFP

 Julie Brill CHIEF PRIVACY OFFICER & DPO, MICROSOFT	 Drudeisha Madhub DATA PROTECTION COMMISSIONER, MAURITIUS
 Noopur Davis CHIEF TRUST OFFICER, COMCAST	 Immaculate Kassait DATA PROTECTION COMMISSIONER, KENYA
 Poppy Gustafsson CEO, Darktrace	 Paula Ingabire MINISTER OF ICT & INNOVATION, RWANDA
 Ayesha Khanna CEO, ADDO AI	 Rania Al-Mashat MINISTER OF INTERNATIONAL COOPERATION, EGYPT
 Nezha Hayat CHAIR, MOROCCAN CAPITAL MARKETS AUTHORITY (AMMC)	 Sanda Ojiambo EXECUTIVE DIRECTOR & CEO, UN GLOBAL COMPACT

Powered by:  THE MORGANS

www.grcfincrimewards.com
www.eu.grcfincrimewards.com
www.wgrcfp.org



III. 15th Annual Conference and 17th General Assembly of the Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)

On 24 and 25 November 2025, the Data Protection Office (DPO) hosted the 15th Annual Conference and the 17th General Assembly of AFAPDP in Mauritius. The conference was held under the theme “L’économie numérique et la protection des données: enjeux et perspectives pour les autorités francophones.” The elected president of the AFAPDP is the Data Protection Commissioner, Mrs D. Madhub.



At the conclusion of the Assembly, members adopted a resolution on the ethical governance of Artificial Intelligence proposed by this office reaffirming the importance of establishing a responsible framework that safeguards fundamental rights in the context of rapidly evolving AI technologies. Members also agreed to establish a dedicated Working Group on the role of Data Protection Officers (DPOs), with a view to enhancing expertise, fostering collaboration and promoting the harmonisation of practices across the francophone space.

IV. Workshop on Data Protection Day

In commemoration of Data Protection Day 2025, DPO organised a full-day workshop on 28 January 2025 titled “Data Protection Training”. The workshop brought together approximately 300 Data Protection Officers from both the public and private sectors in Mauritius.

During the workshop, members of the Networking Forum of Data Protection Officers shared insights through a short video highlighting the Forum’s objectives, its benefits to members and its future and impact. This was followed by the launching of a private GPT solution for the office.



The training programme was structured into four comprehensive modules:

- Part I: Understanding Data Protection
- Part II: Fulfilling Organisational Responsibilities
- Part III: Security of Processing, Compliance Audits, Data Protection Impact Assessments (DPIAs) and Personal Data Breach Management
- Part IV: Maintaining Records of Processing Operations and Rights of Data Subjects

The workshop provided participants with in-depth knowledge and practical insights into data protection practices. It further enhanced their understanding of the applicable legal framework and strengthened their capacity to effectively discharge their responsibilities as Data Protection Officers.

Each participant was awarded a certificate of completion in recognition of their commitment to promoting and strengthening data protection practices in Mauritius.

V. Memorandum of Understanding (MoU) between DPO and Bank of Mauritius

Cabinet agreed to the signing of a Memorandum of Understanding between the Data Protection Office and the Bank of Mauritius at its meeting of 25 July 2025.

The MoU was signed on 4 September 2025 formalising a strengthened partnership between DPO and Bank of Mauritius. It established a structured framework for strategic collaboration with a focus on information sharing, capacity building and mutual assistance in the discharge of respective statutory mandates.



The MoU aims to:

- Strengthen cooperation between financial supervision and data protection oversight;
- Facilitate the exchange of relevant expertise and information; and
- Provide greater clarity to regulated entities thereby promoting consistent and efficient compliance.

VI. Visit of the President of the French Republic

The Data Protection Commissioner participated in two conferences on personal data protection and artificial intelligence organised by the Embassy of France in Mauritius in the context of the official visit of the President of the French Republic, Mr Emmanuel Macron, to Mauritius in November 2025.

On this occasion, the Data Protection Commissioner also had the opportunity to interact with the President of the French Republic at Caudan in her capacity as President of the AFAPDP.

VII. Mauritius National Data Strategy (NDS)

In 2025, DPO developed the Mauritius National Data Strategy establishing a comprehensive framework to harness the power of data to drive innovation, enhance public service delivery and support economic growth. The NDS constitutes a key component of the Digital Transformation Blueprint 2025–2029.

The NDS sets out the following strategic objectives:

- Improving public sector data quality and sharing
- Promoting ethical, secure and transparent use of data
- Building a world-class data economy
- Strengthening data protection and privacy safeguards
- Preparing for a safe, trustworthy and ethical adoption of AI

To support its implementation, DPO developed the following four annexes to the NDS providing practical tools and guiding frameworks:

1. Model Data Governance Framework
2. Data Sharing Policy Template
3. Data Sharing Protocol Template
4. Data Retention Policy Template

The development of the NDS and its annexes required significant time, research and expertise to adequately reflect the broad scope of data governance which extends beyond privacy and personal data processing to encompass non-personal data. The process also incorporated recommendations and insights from international partners including the World Bank and the European Union as well as consultations with local stakeholders.

The NDS and its annexes are scheduled for official launch on 28 January 2026.

VIII. MoU between DPO, Computer Emergency Response Team of Mauritius (CERT-MU) and Mauritius Police Force (MPF)

On 19 September 2025, Cabinet approved the signing of a Memorandum of Understanding between the DPO, CERT-MU and MPF regarding the operation of a Digital Forensic Laboratory.

The primary objective of the MoU is to strengthen collaboration among the parties through the exchange of relevant technical information and expertise thereby enhancing the effective discharge of their respective regulatory and enforcement functions. The MoU further provides for enhanced cooperation in supporting investigations involving the collection, preservation and analysis of digital evidence and facilitating technical assistance and capacity building among the parties.

The MoU is expected to be signed by all parties on 28 January 2026.

IX. Amendments to the Data Protection Act for EU Adequacy

Mauritius proclaimed the Data Protection Act 2017 to align its legislation with the essential principles of the European Union General Data Protection Regulation (GDPR) and the Council of Europe Convention 108 and 108+ which represent the recognised global standards in data protection.

However, achieving adequacy extends beyond alignment with the fundamental principles of the GDPR. It requires a comprehensive assessment of a country's overall data protection ecosystem.

The European Commission evaluates third countries based on several criteria including the rule of law, respect for human rights, the relevant data protection legislation and its implementation, enforcement mechanisms, the presence of independent data protection authorities and the international obligations related to data protection. Therefore, while Mauritius has aligned its legal framework with key GDPR principles, adequacy would constitute a formal recognition by the European Commission that the data protection ecosystem of Mauritius offers a level of protection equivalent to the European Union (EU) and European Economic Area (EEA).

In 2025, DPO updated the draft Bill following continued consultations with the European Commission and the Ministry of Information Technology, Communication and Innovation. The updated draft was subsequently submitted to the State Law Office for legal review and several consultative meetings were held between the State Law Office and DPO.

Once the draft Bill would be finalised, it would be submitted to the European Commission for consideration prior to its introduction to Parliament which is anticipated in 2026.

X. Guide on Artificial Intelligence and Data Privacy

In 2025, DPO developed a Guide on Artificial Intelligence and Data Privacy to address emerging challenges at the intersection of data protection and artificial intelligence. The guide establishes clear frameworks and technical benchmarks to support organisations in implementing the principle of "Privacy by Design" within AI systems ensuring that technological advancement remains both ethically grounded and legally compliant.

By addressing the complex interplay between AI governance, ethical considerations and regulatory requirements, the guide aims to strengthen oversight and safeguard fundamental rights in an increasingly automated digital economy.

The guide is expected to be launched in 2026.

2025 ACTIVITIES



I. Financial Status

(a) Revenue collected

DPO collected a total revenue of Rs 3,504,700 for registration of controllers and processors in 2025.



In 2025, revenue was lower than in 2024 because the higher revenue in 2023 came from the renewal of registration for controllers and processors who registered anew under the Data Protection (Fees) Regulations 2020. Subsequently, their registration certificates expired after three years and they renewed in 2023.

II. International Cooperation

The DPO participates in numerous international privacy networks such as Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP), Global Privacy Enforcement Network (GPEN), Common Thread Network (CTN), Global Privacy Assembly (GPA), Council of Europe, Southern African Development Community (SADC) and the United Nations, amongst others. Such participation enables the office to exchange information, undertake and support specific activities and share knowledge with best practices.

a) Participation with international organisations

Organisation Internationale de la francophonie (OIF)

The Data Protection Office continued its active engagement with the Francophone community to address the shared challenges of the digital age. From 05 to 06 July 2025, the OIF hosted its annual conference in Geneva, Switzerland. Under the overarching theme “Forum Francophone de la gouvernance du Numérique et de l’IA,” the forum brought together delegates from member states to harmonize perspectives on digital sovereignty and the ethical deployment of Artificial Intelligence.

The Data Protection Commissioner participated online as a distinguished panelist to discuss the critical topic «Gouverner les données: entre souveraineté, éthique et sécurité à l’ère de l’interconnexion ». During this session, the Commissioner addressed the complex interplay between national data sovereignty and the reality of global digital interconnection.

b) Participation with regional and international organisations

1. Southern African Development Community (SADC)

I. Putting Mobile Phone Data (MPD) to Work for Statistics SADC Regional Workshop:

An officer of the DPO participated in a regional workshop organized by SADC, with support from the World Bank Group on Mobile Phone Data in Johannesburg from 19 - 22 May 2025. The workshop was part of the implementation of the SADC Digital Transformation Strategy (DTS) and the SADC Big Data Framework and was designed to support initiatives that leverage data collected through MPD for official statistical purposes.



II. Capacity building on data governance and policy based on the AU data policy framework and validation

An officer from the Data Protection Office attended the Capacity Building on Data Governance and Policy workshop, held from 22nd to 26th September 2025 in Madagascar. This workshop focused on the African Union (AU) Data Policy Framework and included the validation of the revised SADC E-Commerce/E-Transaction Model Law. The event was a crucial platform for enhancing regional capacity on data governance, protection and policy harmonization, with participation from 82 delegates across nearly all SADC Member States. It provided in-depth sessions on data governance principles, institutional and regulatory frameworks, emerging data issues such as AI and case studies from Member States.



2. Africa Digital Rights Hub (ADRH)

The Data Protection Africa Summit 2025, organized by the ADRH took place in Ghana, from 01 December to 04 December 2025. The event focused on 'Defining Africa's Digital Future: From Consumerism to Partnership'. The Data Protection Commissioner was invited as speaker to deliver a talk on 'Behavioural data, AI & Digital Sovereignty in Africa'.

The ADRH in partnership with PICCASO also hosted the PICCASO Awards Africa at the Data Protection Africa Summit 2025 and the Data Protection Commissioner was invited as judge for the PICCASO Awards.

The Data Protection Office (DPO) represented by Mrs Drudeisha Madhub has been awarded the winner of the PICCASO Awards Africa 2025 - Most Impactful Privacy Product for its E-DPO Platform.



3. Council of Europe (CoE)

On 15 May 2025, the Data Protection Commissioner participated virtually as an expert panelist at the Privacy Symposium 2025. The Commissioner contributed to a dedicated session titled “Accompagner la conformité pour créer, entreprendre et innover en français”. During the discussion, the Commissioner highlighted the critical role of data protection frameworks not as barriers, but as essential catalysts for digital trust and business development. The session provided a valuable platform to exchange best practices on how regulatory compliance can successfully drive technological innovation and entrepreneurship within the Francophone ecosystem, further reinforcing the Commissioner’s commitment to international collaboration under the auspices of the Council of Europe.

4. Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP)

The Data Protection Office continued its commitment to international cooperation and the development of harmonized data standards by participating in the 8th Edition of the NADPA-RAPDP Conference and AGM 2025. Hosted by Nigeria from 6th to 8th May 2025, the conference brought together regulators, policymakers and industry experts from across the continent to address the evolving landscape of digital privacy in Africa.

The Data Protection Commissioner represented the office virtually, contributing expert insights as a guest speaker on two high-level panels focused on the intersection of emerging technology and regulatory frameworks.

5. Identification for Development(ID4) Africa 2025

The Data Protection Office played a central role in the ID4 Africa 2025 Annual General Meeting, held in Addis Ababa, Ethiopia, from 20 to 23 May 2025. This movement remains the premier continental forum for digital identity, providing a critical space for the intersection of legal identity systems and robust data privacy frameworks. The Data Protection Commissioner, accompanied by an officer represented the Office through high-level moderation and technical contributions.

The Office’s participation was marked by a focus on practical regulatory tools and the governance of digital identity risks:

- **A-Z of DPIAs: A Joint Workshop for Identity and Data Protection Authorities** The Commissioner served as Moderator for this specialized workshop. The session provided a comprehensive guide to conducting Data Protection Impact Assessments (DPIAs) specifically tailored for large-scale identity systems. It fostered direct dialogue between identity providers and regulators to ensure that privacy is “baked into” the design of national digital ID infrastructures.
- **Digital Identity: Data Risks & Governance (Workshop 2).** The discussions highlighted evolving governance models that secure personal data while ensuring inclusive access to digital services.

(c) Other virtual meetings

I. OECD

In line with our commitment to international best practices and global policy development, the Data Protection Office maintained an active presence within the OECD's digital governance initiatives throughout 2025. One officer of the Data Protection Officer's Unit participated in key specialized forums to represent the Office's interests and contribute to global standards on data flows and consent:

13 January 2025	Plenary meeting of the OECD DFFT Community	Discussions centered on operationalizing Data Free Flow with Trust (DFFT), specifically focusing on building interoperability between different regulatory regimes to facilitate secure global data transfers
18 March 2025	OECD Roundtable on Scoping emerging consent practices in the digital ecosystem	An intensive technical session exploring the evolution of user consent in the digital ecosystem. Topics included addressing "consent fatigue," dark patterns, and the shift toward more automated or delegated consent mechanisms.

• Webinars

APLA-Association of Privacy Lawyers in Africa's

The Data Protection Commissioner intervened as a keynote speaker in a webinar organized by Association of Privacy Lawyers in Africa's (APLA) on Powerful Women in Privacy, with the theme "Accelerate Action" on the 15th March 2025. The Data Protection Commissioner shared her insights on how to accelerate action in the field of privacy and data protection and shared her extensive experience in driving meaningful change in this critical area.

II. Sensitisation

One amongst the functions of this office is to take such measures as may be necessary to bring the provisions of the DPA to the knowledge of the general public. Many sensitization activities were carried out during 2025.

a. Press Communiqués/Interviews

• Communiqué to the Public, Data Protection office – Registration of controllers and processors

This office has issued a communiqué regarding the registration /renewal of controller and processor.



COMMUNIQUE TO THE PUBLIC
DATA PROTECTION OFFICE
(Registration of controllers/processors)

1. All public and private organisations, sociétés, partnerships, professionals such as doctors, lawyers, engineers, architects, notaries and sole traders such as jewellers, bookmakers and any other entity processing and collecting personal data of living individuals, are required to register themselves as a controller with the Data Protection Office. The list is non-exhaustive and includes all categories of professionals and businesses.
2. A processor is a person who, or an organisation which, processes personal data on behalf of a controller. An example of processor is an organisation which prepares the payroll of employees of other organisations as defined in the contract between the processor and the controller.
3. Section 14 of the Data Protection Act 2017 (DPA) makes it mandatory for controllers/processors to register with the Data Protection Office.
4. Under Section 22(2)(e) of the DPA, a controller must designate an officer responsible for data protection compliance.
5. The application form for registration or renewal of registration a controller/processor may be downloaded on the website <http://dataprotection.govmu.org>. **Only** online applications are accepted.
6. Please consult the user manual on our website to assist controllers/processors and citizens on registration, complaints and eforms processes.
7. The Data Protection (Fees) Regulations 2020, which came into force on 01 August 2020, provides for the registration of controllers and processors and related fees payable. Failure to register, to renew and to designate a data protection officer are offences which are, on conviction, liable to a fine not exceeding Rs 200,000 and to imprisonment for a term not exceeding 5 years under Section 43 of the DPA.
8. Should you have any queries related to registration, complaints and eforms, please contact us by phone (4600251) or email (registrydpo@govmu.org).

The Data Protection Commissioner
Data Protection Office
This 24th February 2025

- **Communique to the Public, Data Protection office – Post containing passport details on social media**

The DPO issued a communiqué to remind the public of the risks and criminal consequences associated with the unauthorised publication of personal data on social media.

COMMUNIQUÉ
Data Protection Office

It has come to the attention of the Data Protection Office (DPO) that a post is currently circulating on social media containing the passport details of two students in relation to the jet ski incident in Dubai.

The DPO is issuing this urgent communiqué to remind the public of the risks and criminal consequences associated with the unauthorised publication of personal data on social media.

1. Passport Information is Personal Data

Passport documents contain personal data including an individual's photograph, name, date of birth and other identifiers. The disclosure of such information without authorisation can expose individuals to privacy breaches, identity theft and other serious risks.

2. Unauthorised Disclosure Is a Criminal Offence

The publication of personal data on social media is regulated by the **Cybersecurity and Cybercrime Act** and the **Data Protection Act**.

Under **Section 28 of the Data Protection Act**, the consent of the data subject is required prior to any publication of their personal data on social media or any other platform.

3. Penalties

Any breach of the Data Protection Act is an offence and upon conviction is liable to:

- a fine not exceeding 200, 000 rupees and to
- imprisonment for a term not exceeding 5 years.

The Data Protection Office urges the public to exercise responsibility and refrain from sharing or forwarding any personal data without the necessary consent.

4. Deletion of the Post

Individuals who have posted or shared the content containing the personal data of the two students are required to remove it without delay.

09 December 2025

• **Radio One Intervention**

On the 2nd March 2025, the Data Protection Commissioner took part in a live session at Radio One, discussing the topic "Data Protection: Companies Urged to Comply." The Commissioner emphasized that businesses handling customers' personal data must register with the Data Protection Office. This registration enables authorities to monitor the use of this data and ensure compliance with legal standards. The Data Protection Commissioner urged professionals, businesses and merchants to complete their registration online through the Data Protection Commission's website. The Data Protection Commissioner also highlighted that many companies have yet to comply with the law, leaving them at risk of fines of up to 200000 rupees.

- **BDO IT Consulting Data Privacy Day 2025 Newsletter**

On the occasion of Data Privacy Day 2025, the Data Protection Office contributed to a newsletter published by BDO IT Consulting. The newsletter focused on the theme “Building Trust Through Transparency and Security” and aimed to raise awareness and promote best practices in data protection throughout Mauritius.

7

Data Protection Day 2025: Building Trust Through Transparency and Security
BDO IT Consulting | Newsletter 2025

Section 3: Mauritius Data Protection Focus

Insights from the Data Protection Commissioner

To gain a deeper understanding of Mauritius's commitment to data protection, **Mrs. D. Madhub**, the **Data Protection Commissioner** provided her insights to shed light on the proactive steps organisations can take to prevent breaches and the key priorities of the Data Protection Office for 2025.



Mrs. Drudelsha Madhub
Data Protection Commissioner

Question 1

What proactive measures do you recommend organisations implement to prevent data breaches?

Answer 1

Organisations can minimise data breach risks by focusing on:

► **Access Control & Data Classification:**

Organisations must categorise data based on sensitivity and enforce strict access controls, ensuring that only authorised individuals can access sensitive data. Implementing role-based access and multi-factor authentication further strengthens security.

► **Encryption & Regular Audits:**

Encrypting sensitive data both in transit and at rest is paramount. Regular security audits and vulnerability assessments help proactively identify and address potential weaknesses.

► **Employee Training & Incident Response:**

Training employees to recognise cyber threats, such as phishing and establishing a comprehensive incident response plan ensures quick and effective action during a breach.

► **Monitoring & Backups:**

Monitoring network activity and user access in real-time helps detect suspicious behaviour, while secure, encrypted backups protect data from loss or ransomware attacks.

► **Third-Party Risk Management**

Organisations should assess the security practices of third-party vendors and ensure compliance with relevant data protection laws, reducing legal and reputational risks.

Section 3: Mauritius Data Protection Focus (Cont'd)

Insights from the Data Protection Commissioner

To gain a deeper understanding of Mauritius's commitment to data protection, **Mrs. D. Madhub**, the **Data Protection Commissioner** provided her insights to shed light on the proactive steps organisations can take to prevent breaches and the key priorities of the Data Protection Office for 2025.

Question 2

Looking ahead to 2025, what are the key priorities for the Data Protection Office?

Answer 2

Our 2025 focus is twofold:

► Strengthened Enforcement & Compliance

We are stepping up enforcement actions of the Data Protection Act 2017. This will involve more frequent audits and site visits to assess compliance. We are also establishing a dedicated prosecution unit to handle serious breaches ensuring organizations are held accountable for their data protection practices.

► Enhanced Capacity & Global Collaboration

We have streamlined complaint handling procedures to ensure timely responses and keeping complainants informed of the progress of their cases. We are committed to improving our internal capacity through an upgrade of our Forensic Lab, equipping us with the latest technology to investigate data breaches effectively. Investing in training programs for Data Protection Officers remains a priority. We also continue to actively engage with international privacy networks like the AFAPDP, RAPDP, CPEN, and others to share best practices and stay abreast of global developments. (For more information on DPO initiatives and the Data Protection Officer Networking Forum, visit:

<https://dataprotection.govmu.org/Documents/Networking%20forum%20for%20data%20Protection%20Officers%2026072023.pdf>



Key Takeaways:

- Proactive data security measures are essential for maintaining public trust and complying with evolving regulations.
- The Data Protection Office is prioritising enforcement and accountability to strengthen data protection in Mauritius.
- Collaboration and training are key to building a robust data protection framework and culture.



- **The Postal and Telecommunication Regulatory Authority of Zimbabwe (POTRAZ) Solidarity Message to Commemorate Data Privacy Symposium from 28 – 30 January 2025**

The Data Protection Commissioner partnered with the Postal and Telecommunication Regulatory Authority of Zimbabwe (POTRAZ) by delivering a pre-recorded solidarity message, which was featured during POTRAZ's second Data Privacy Symposium from 28th to the 30th of January 2025 in celebration of the Data Privacy Week. The symposium was held under the theme: 'Bridging the gap between technology, policy, law and practice: Towards strengthening data protection in Zimbabwe'.

- **Guidelines on usage of ChatGPT for Government bodies**

The Data Protection Office has developed a guide on the usage of ChatGPT for government bodies to ensure responsible and secure implementation. The guide provides several key recommendations to safeguard personal data and restrict access to sensitive information that should be considered when using ChatGPT.

- **Participation in DITEX 2025**

From 16-18 May 2025, the Data Protection Office actively participated in the DITEX (Defi Information and Technology Exhibition) event organized by the Defi Media Group at the Swami Vivekananda International Convention Centre (SVICC). Officers from the Data Protection office delivered insightful talks tailored for school students and the general public, effectively raising awareness and providing crucial information regarding the Data Protection Act 2017.

(b) Raising awareness with businesses

- **Strategic Initiatives of MloD**

- i. The Data Protection Commissioner intervened as the guest speaker in a workshop organized by the Mauritius Institute of Directors (MloD) focusing on "Future-Ready Data Protection: Trends, Tools, and Techniques" on 21 January 2025 to mark Data Protection Day. The event focused on the evolving landscape of data protection, emerging trends, the latest tools and best practices in the field.

This Workshop aimed to provide participants with the knowledge and insights necessary to stay ahead of the evolving challenges in data protection and privacy. The Data Protection Commissioner addressed these challenges, offering perspectives on how organizations can be better prepared for the future of data protection.



- ii. The MLoD in collaboration with Dili Trust organised a half day session on the theme “Enhancing board dynamics through AI: Opportunities and challenges” on the 15th May 2025. During the event, the Data Protection Commissioner was invited to participate as a panelist. The event explored how artificial intelligence can enhance decision-making at board level while addressing potential risks and governance concerns. It provided a platform for discussing the balance between innovation and responsible AI adoption.
- iii. The Data Protection Commissioner participated as a guest speaker for the event organised by The Pod under the theme “Laundering/Counter Terrorism Financing” held on 16th June 2025. The session focused on strengthening awareness and compliance with AML/CFT regulations. It provided insights into regulatory frameworks, risk mitigation and the importance of data protection in combating financial crimes.
- iv. The Data Protection Commissioner participated as a keynote speaker in a session organized by the MLoD under the theme “Future Ready Data Protection: Trends, Tools and Techniques” held on 3rd September 2025. The event aimed to explore advanced strategies and practical approaches to strengthening data protection frameworks. It provided valuable insights into adapting to evolving regulatory and technological environments.

- **Conference on General Data Protection Regulation (GDPR) and Data Protection Act 2017 (DPA) by CCIFM**

The Data Protection Commissioner intervened as a guest speaker in a conference on 23rd January 2025 to commemorate Data Protection Day organized by Chambre de Commerce et d'Industrie France Maurice (CCIFM). The event centered on the theme of the General Data Protection Regulation (GDPR) and the Data Protection Act 2017 (DPA). The Data Protection Commissioner discussed about the Data Protection Office of Mauritius (DPO), its functions, overview of the DPA, Mapping between DPA and GDPR, Transfer of personal data abroad and achievements of the DPO.



- **The Institutional Expert Services (IES) summit in Mauritius**

The IES Summit was held on the 30th of April 2025 at Hennessy Park Hotel where the Data Protection Commissioner participated as panelist to discuss the topic on “Ethical and Legal Dimensions of AI: Where do we draw the line?” The session explored the balance between innovation and regulation in the use of artificial intelligence and discussions were focused on ethical concerns, legal boundaries and the need for responsible AI governance to ensure compliance with data protection principles.

c) Training

• Data Protection Day Training on Data Protection

The Data Protection Office organized a full-day event on 28 January 2025 in commemoration of the Data Protection Day at Mahatma Gandhi Institute. The workshop, titled “Data Protection Training” trained 300 Data Protection Officers (DPOs) from both public and private organizations across Mauritius.

The training covered the following essential topics Understanding Data Protection, Fulfilling organizational responsibilities, Security of Processing, Compliance Audits, Data Protection Impact Assessments (DPIAs), Personal Data Breach Management, Maintaining Record of processing operations and Rights of Data Subjects.

The workshop provided in-depth knowledge and practical insights into advanced practices for safeguarding personal data. Participants gained a comprehensive understanding of data protection laws and their responsibilities as DPOs. The workshop fostered sensitization, knowledge-sharing and collaboration among professionals working in the data protection field.

• Internal Capacity Building: The Law and its Implications

On 04 July 2025, two officers from the Data Protection Office conducted an intensive in-house training session for approximately 30 participants. Under the theme “The Law and its Implications,” the workshop was designed to deepen the staff’s technical understanding of the Data Protection Act and its practical application. The session focused on bridging the gap between legislative requirements and effective data protection practices, ensuring that operational activities remain fully compliant with evolving regulatory standards.

• Regional Training: Knowledge Sharing with the Madagascar Data Protection Authority

On 26 November 2025, the Data Protection Office hosted a specialized training session for a delegation from the Madagascar Data Protection Authority. Facilitated by two senior officers, the program focused on the comprehensive legal framework of the Mauritius Data Protection Act. The primary objective was to facilitate a high-level exchange of expertise and to impart an in-depth understanding of our legislative landscape, thereby strengthening regional alignment in data protection standards.

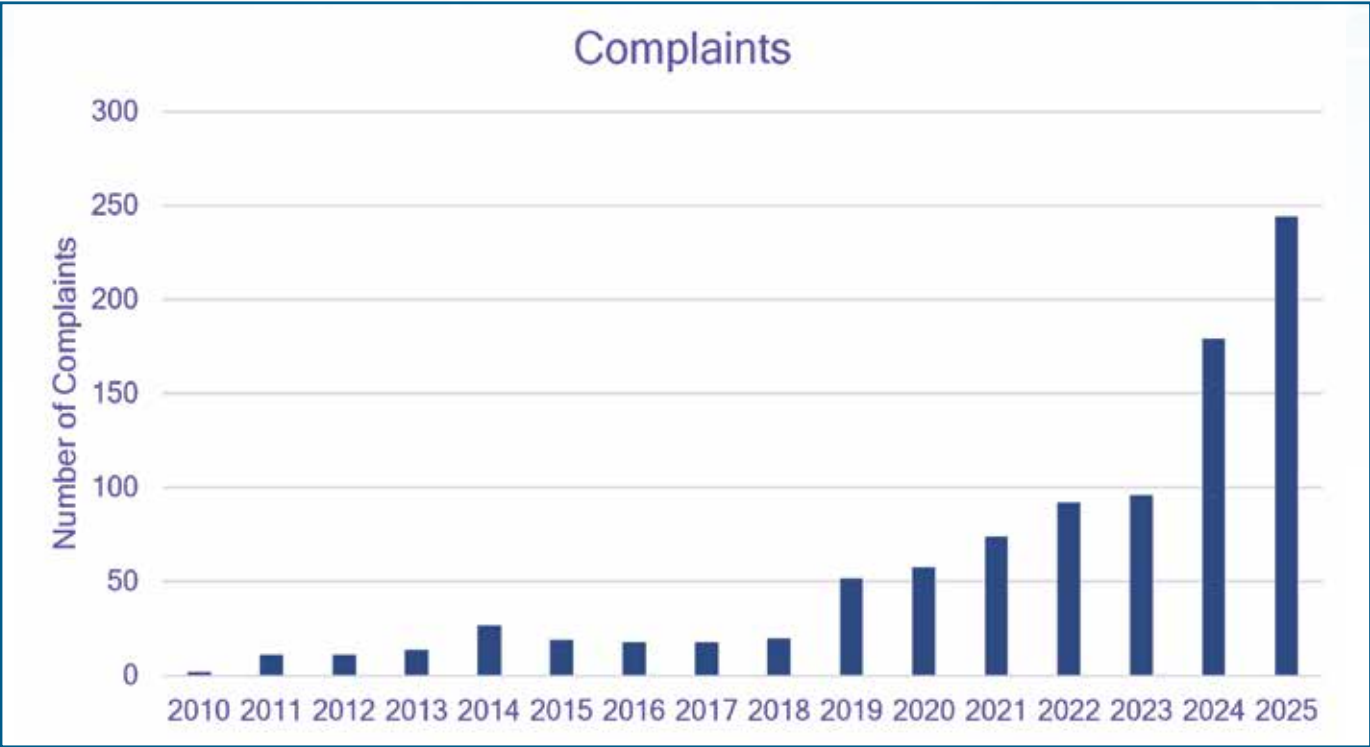
III. Enforcing Data Protection

• Investigation on Complaints

During the period January to December 2025, the DPO received **two hundred forty-four (244)** new complaints regarding investigations on the below subjects among others:

- Unauthorised use of CCTV camera
- Unlawful disclosure of personal data
- Fingerprint
- Access to data subject

The diagram below illustrates the total number of complaints received during the past years.

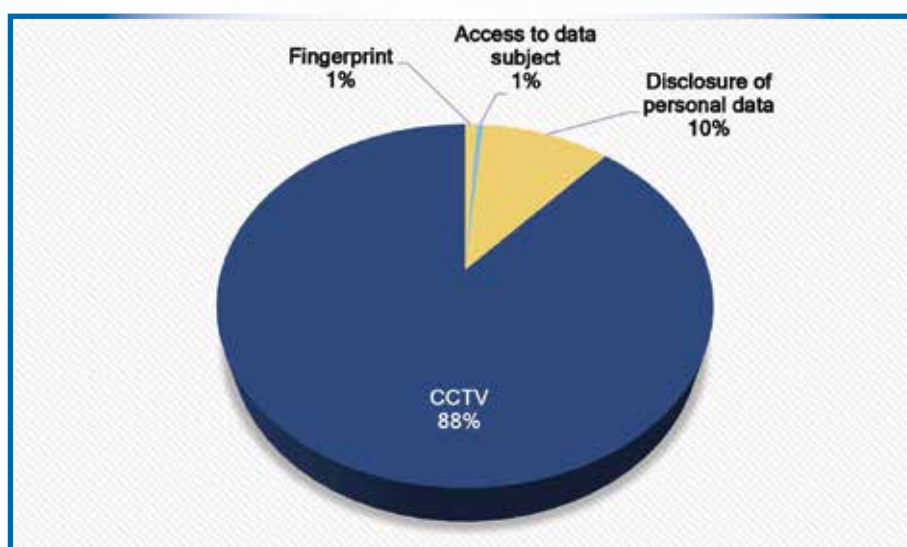


- Enquiries conducted by DPO in 2025

Categories	Details
Closed Cases Involving CCTV Cameras (87 cases)	These cases concerned the use of CCTV cameras by private individuals primarily relating to alleged invasions of privacy. In all these cases, the office sought the assistance of the Police to conduct site inspections. The inspections confirmed that the cameras were either: • Capturing images within the respondents’ own premises or • Reorienting cameras following intervention by the office and the police As a result, the eighty-seven (87) cases were closed. The enquiries were resolved to the satisfaction of the parties involved.
Ongoing Cases Involving CCTV Cameras (99 cases)	Ninety-nine (99) CCTV-related cases were processed and were ongoing in 2025. These cases require further inspections such as: • Determining whether cameras capture areas beyond the respondents’ premises and • Checking the positioning of the cameras. DPO solicited Police assistance for site inspections and evidence collection. The resolution of these enquiries remained ongoing in 2025 due to the need for detailed verifications, non-collaboration of parties involved and in some cases, the complexity of ongoing disputes on properties or court proceedings between neighbours.

CCTV Cases in Workplaces (2 cases)	In 2025, DPO received two (2) complaints regarding the use of CCTV cameras in workplaces, with staff raising concerns that their privacy was being infringed and that they were under constant monitoring:- • One of the cases were closed following advices provided to the workplace by the office. • One case remained ongoing as further information was being gathered.
Unlawful Disclosure of Personal Data (37 cases, 34 ongoing, 3 closed)	In 2025, the Data Protection Office investigated several cases involving the unlawful disclosure of personal data, ranging from unauthorized sharing of information by employees and colleagues to the misuse of emails and biometric data. In response to these complaints, the DPO conducted thorough investigations and following a careful examination of the evidence and the implementation of appropriate security measures by the concerned parties, three (3) were successfully resolved and closed to the satisfaction of the complainants, while others remained ongoing and were being monitored to ensure ongoing compliance.
Right of access to CCTV footage (1 case)	In 2025, a case was lodged involving a verbal altercation. The complainant alleged that an individual, acting outside of his purview, intervened in a private matter and instructed another party to refuse the receipt of a physical envelope. In accordance with the Data Protection Act, the Office reviewed the circumstances surrounding the potential processing of personal data during this interaction. Following an investigation of the incident, it was determined that the matter primarily concerned a behavioral dispute rather than a breach of data processing principles. The case was subsequently closed as no evidence of unauthorized storage or recording of personal data was found to exist during the encounter.
Right of access to data subject (1 case)	In 2025, a case was registered involving a dispute over the unauthorized retention of user profile access and company equipment. Following an intervention by the CCID to recover the physical hardware, DPO was engaged to facilitate the recovery of the digital accounts. The case highlights the importance of maintaining administrative control over recovery credentials when delegating data entry tasks to third parties. The case was subsequently closed after the Office provided a determination on the respondent's obligations to balance statutory confidentiality with the transparency requirements of the Data Protection Act.

Out of the total number of cases, one hundred eighty-four (184) cases (representing 88%) pertained to CCTV as depicted below.



The duration of any investigation which is on a case to case basis depends on the complexity of the case and collaboration/response of all concerned parties including complainant and respondent.

d) Complaints Closed

The office closed thirty-nine (39) complaints in 2025.

IV. Improving Legal Protection

By virtue of section 51 of the DPA, any person aggrieved by a decision of the Commissioner under the DPA may, within 21 days from the date when the decision is made known to that person, appeal to the Tribunal.

- (a) **Supreme Court Cases:** The DPO represented by the State Law Office, was involved in two (2) Supreme Court cases, where this officer was co-defendant/respondent. Both cases were set aside.
- (b) **Intermediate Court Cases:** The DPO appeared as a witness in two (2) CCTV-related cases for which complaints were filed at this office. Both cases are ongoing.
- (c) **Industrial Court Cases:** The DPO appeared as a witness in one CCTV – related case for which complaint was filed at this office. The case was set aside.

V. Registration of Controllers and Processors

Under the Data Protection (Fees) Regulations 2020, the cumulative number of registered controllers and processors from 01 August 2020 to 31 December 2025 reached 23505 and 2005 respectively. 2894 registration certificates were issued in 2025. The office has also attended a voluminous amount of phone calls and emails on registration of controllers and processors.

VI. Requests for Legal Advice

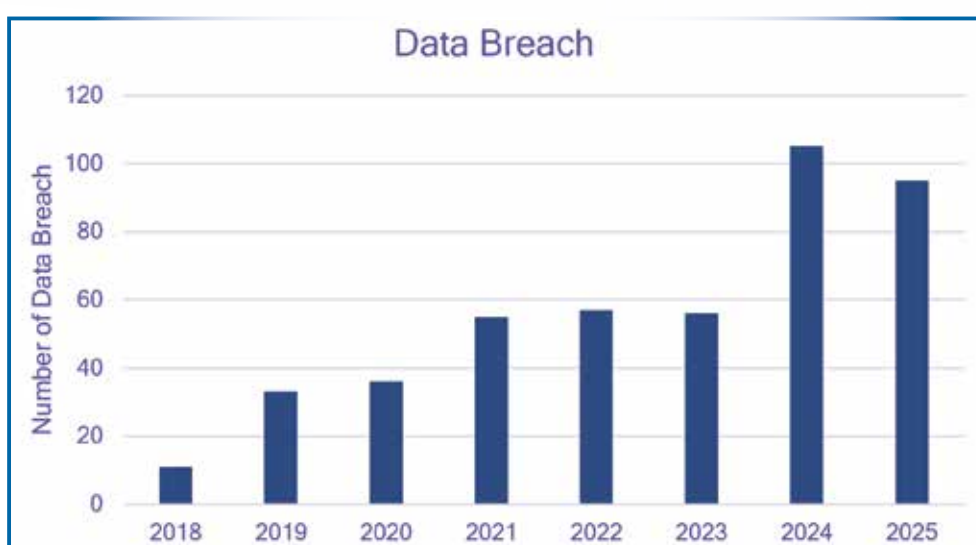
In 2025, the office received around four hundred and fifty five (450) written requests for legal advice on the interpretation of the DPA.

VII. Advisory /Stakeholder Role in Projects

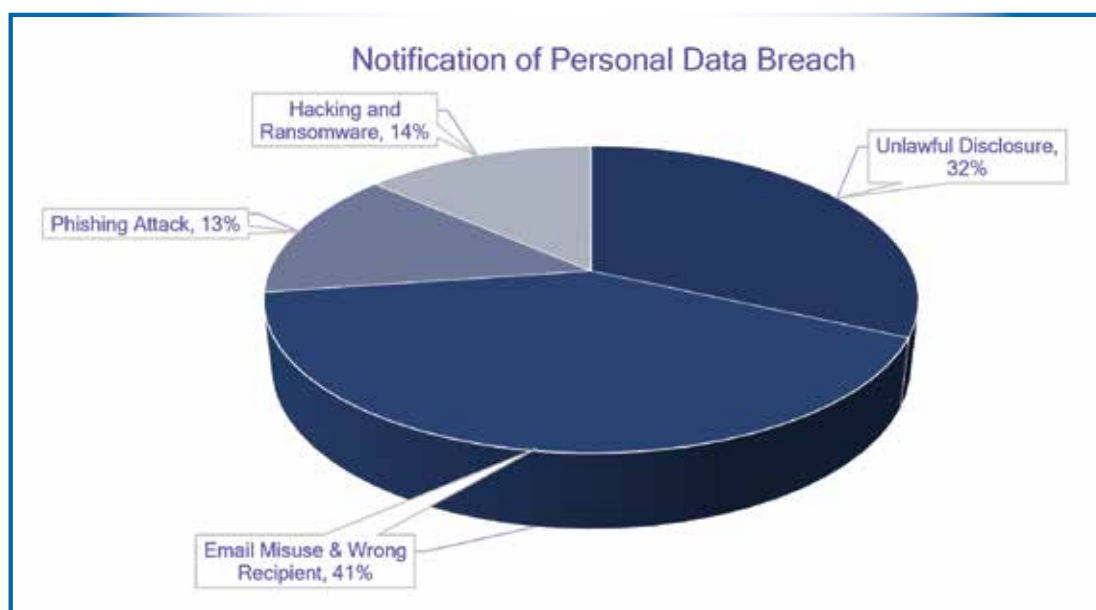
In 2025, the Data Protection Office further solidified its role as a strategic institutional stakeholder, providing critical regulatory oversight and formal recommendations for high-impact projects across both the public and private sectors. Integrating “Privacy by Design” into the national digital architecture, the office actively engaged in the governance of emerging technologies, including Artificial Intelligence (AI) implementations, mobile application ecosystems and complex web-based systems. Through its continued representation on various Steering Committees and the rigorous review of Data Protection Impact Assessments (DPIAs), the DPO ensures that innovation in the digital economy remains strictly aligned with the compliance mandates of the Data Protection Act.

VIII. Personal Data Breach Notifications

In 2025, ninety five (95) personal data breaches have been reported to this office.



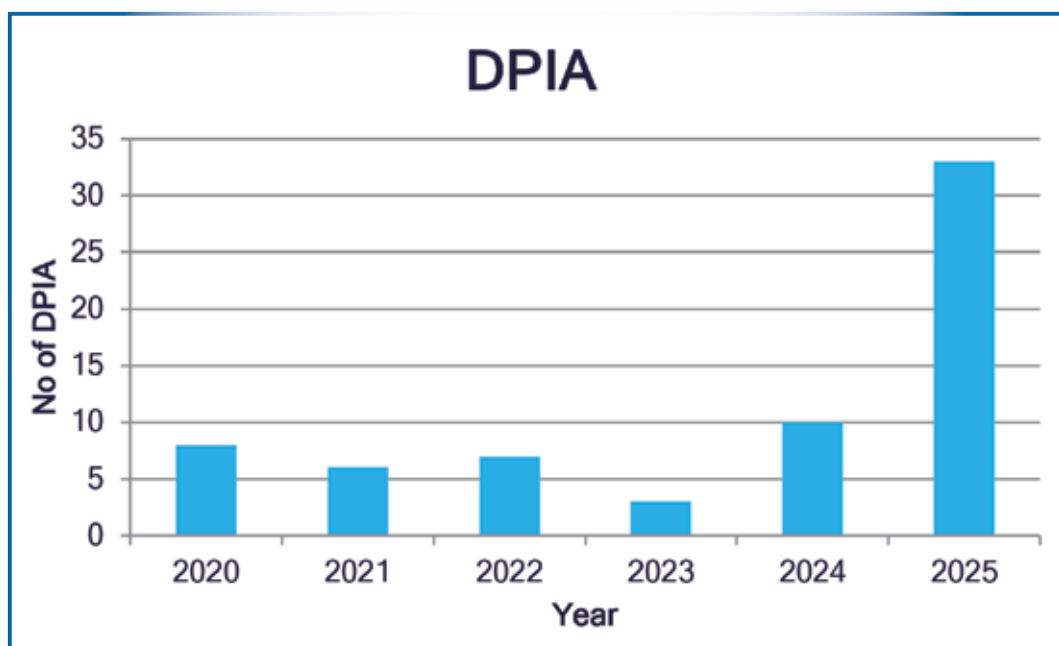
An analysis of the type of breaches received showed that unlawful disclosure and email misuse including sending email to wrong recipients remain the main causes of breaches reported. The following pie chart categorises the types of data breaches notified in 2025.



IX. Data Protection Impact Assessments

Organisations must carry out a data protection impact assessment for high risk processing operations. This assessment is a comprehensive analysis of privacy aspects of a proposed project with respect to the rights and freedoms of individuals. It also incorporates a risk evaluation approach to minimise privacy infringements to individuals.

In 2025, the office has received **thirty three (33)** data protection impact assessments submitted by organisations.



X. Transfers of Personal Data Abroad

The DPC authorised One hundred (100) requests for transfer of personal data outside Mauritius with proof of appropriate safeguards under section 36 of the DPA. One (1) applications for transfers were rejected due to insufficient safeguards mentioned on the forms.

XI. Certification

The Data Protection Office issues certification under section 48(1) of the Data Protection Act 2017 (DPA). A certification is–

- (a) voluntary;
- (b) issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions where the relevant requirements continue to be met;
- (c) withdrawn where the requirements for the certification are no longer met.

In 2025, the Office initiated the review of certifications; however, due to acute staff shortages and other pressing deadlines, these reviews have not yet been completed.

CAPACITY BUILDING

In 2025, officers of the DPO attended the following capacity building sessions:

Course	Date	Training Institution
Operation & Process Management Training Programme for Support Staff	12,19 May, 05 June	CSCM
First Aid	03,04,05,06,07,10 March	CSCM
Safety and Health in the Workplace for OMAs	18-Mar	MPSAIR
Training Programme on Change Management	13-Mar	CSCM
Training Programme on Change Management	14-Mar	CSCM
Training Programme on Change Management	19-Mar	CSCM
Training Programme on Change Management	19-Mar	CSCM
Managing Risk at the Workplace	10-Apr	MPSAIR
Foundation course for newly recruited MSO	26,28,30 May and 03, 05 June	CSCM
Foundation course for newly recruited MSO	26,28,30 May and 03, 05 June	CSCM
Training Programme on Mobile ID	6 half days on Tues and Thurs starting 27 May	CISD
Foundation course for newly recruited MSO	02, 06, 10, 11, 12 June	CSCM
Training on PostgreQSL	17, 18, 19, 20 June	CISD
Safety and Health in the Workplace	16-Sep	MPSAIR
Safety and Health in the Workplace	26-Sep	MPSAIR
Safety and Health in the Workplace	16-Oct	MPSAIR



I. Regulation for Data Protection Officers

In order to strengthen our data protection framework, the Data Protection Office will introduce a new regulation on Data Protection Officers (DPOs) to address critical gaps in the Data Protection Act 2017. While the DPA mandates the designation of a DPO, it lacks a proper definition, clear qualifications and detailed functions for the role, all of which are provided for in the new regulation. The core objective is to enhance the professional standing and responsibilities of DPOs across public and private sectors, thereby improving organizational discipline and ensuring a higher level of data protection expertise.

II. e-Privacy regulations

This office is working on an e-Privacy regulation to harmonize national provisions and ensure a high level of protection for fundamental rights within the electronic communications sector. This framework will strictly enforce the confidentiality of communications by prohibiting the unauthorized interception, surveillance or storage of traffic data without explicit user consent, except where legally authorized. Furthermore, the Regulation will establish rigorous standards for data processing security and breach notifications while providing essential safeguards against unsolicited direct marketing. By ensuring that information storage on personal equipment will only be permitted following clear, informed consent, this initiative will guarantee that processing across public networks remains secure and private.

III. Freedom of Information Bill

The Freedom of Information Bill will represent a landmark legislative project in the 2025 pipeline, designed to safeguard the rights of Mauritian citizens to access information held by both public and private bodies. Based on the Commonwealth Model Freedom of Information Bill and the United Nations Model Freedom of Information Law, the bill will aim to increase national transparency and accountability by guaranteeing the right of everyone to access official documents.

IV. Amendments to the Constitutional Right to Privacy

In alignment with the Government Programme 2025–2029, this office will support the strengthening of fundamental rights by modernizing Mauritius’s legal framework to include enhanced protection for the right to privacy and robust data management. Central to this reform, a Constitutional Review Commission will be established to address current constitutional limitations and align national provisions with international standards.

V. Digital Forensics Lab

A Digital Forensic Laboratory serves another important initiative of this office, aimed at significantly enhancing the technical capacity to investigate data breaches and cyber-compliance incidents. The laboratory will serve as a critical infrastructure for the forensic acquisition and analysis of digital evidence ensuring that investigations are conducted with high evidentiary standards while strictly upholding data protection principles.

VI. Workshop on Data Protection Day 2026

The Data Protection Office has formally engaged with its parent Ministry regarding the organization of a workshop to commemorate Data Protection Day on 28 January 2026.

RECOMMENDATIONS

1. Staffing Capacity

The recruitment process for the posts already advertised by the Public Service Commission, including key operational grades, should be expedited and concretised to enhance the Office’s staffing capacity. This will enable the Office to better meet the increasing demands for compliance monitoring, enforcement, advisory services and international cooperation.

2. Amendments to the DPA

The proposed amendments to the Data Protection Act should be enacted at the earliest to support Mauritius’ continued efforts towards achieving EU adequacy to strengthen the legal and regulatory framework governing data protection.

3. Reinforcing Enforcement Capacity

Strengthening enforcement capacity will enhance the Office’s ability to investigate complaints, address violations effectively and ensure improved compliance across both the public and private sectors.

DATA PROTECTION OFFICE

Email: dpo@govmu.org

Website: <http://dataprotection.govmu.org>

<https://www.linkedin.com/in/data-protection-office-dpo579354360/>

Tel: 4600251

Fax: 4897341

Address: 5th Floor, Sicom Tower, Wall Street, Ebene

