Data Protection Office

ANNUAL REPORT 2024

16th Edition

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DPO	Data Protection Office
DPC	Data Protection Commissioner
DPA	Data Protection Act 2017
MITCI	Ministry of Information Technology, Communication and Innovation

MISSION AND VISION STATEMENTS

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

To create a shift in the mindset of the Mauritian population on data privacy concerns, requires an unflinching commitment from government to honour its obligations under the DPA and international obligations under the African Union's Malabo Convention on Cyber Security and Personal Data Protection, the Southern African Development Community Model Law on Data Protection, The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Protocol Amending Convention 108, the European Union General Data Protection Regulation (EU GDPR) and the United Nations resolutions and guidelines on data protection.

Whilst technology is evolving at rocket speed and is controlling the global data ecosystem from infrastructure to architecture and management, the data life cycle is being threatened by vulnerabilities and ethical and privacy concerns and further punctuated by risks caused by unsafe AI applications.

To become a respected democracy requires a profound respect for fundamental human rights including the right to privacy and data protection. As the data protection regulator, I bear the enormous task to investigate offences under the Data Protection Act, a function which requires prosecution of offenders. Without the required resources, this function has been seriously impeded and led to enforcement actions being delayed by this office. It is imperative that we are properly equipped with appropriate expertise to avoid public criticism and perform our prosecutorial functions in a diligent and effective manner.

A revised data protection guide for the financial sector has been finalized by this office and is awaiting publication by the parent Ministry for raising awareness on the safeguards and mechanisms for protection of financial data.

The draft report of the UN Special Rapporteur on Privacy after her visit effected in November 2023 in Mauritius and which will be presented to the UN General Assembly in March 2025, depicts the journey and the achievements of this office and has assessed Mauritius to be the leader in data privacy in the region although challenges relating to the commitment of the country in achieving the robust standards provided under the Data Protection Act have been identified.

Phone tapping which occurred through covert mass surveillance has alarmed the population and was executed by the previous regime under the national security exemption in section 44 (4) (a) and (b) of the Data Protection Act.

This office has offered its timely collaboration to the Commissioner of Police for a thorough enquiry to be conducted in the matter and is awaiting a response from the latter. National security has defined legal parameters under the Constitution of Mauritius and is not an absolute prerogative, although enshrined in law, namely section 44 of the Data Protection Act.

Recommendations for amendments to be brought to the Data Protection Act have been submitted to the Parent Ministry for their consideration to remove such an exemption provision from our Data Protection Act and other substantive proposals for the EU Adequacy project to align the Mauritian data protection framework with the EU GDPR.

Mrs Drudeisha MADHUB (Barrister-at-Law)

Data Protection Commissioner

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

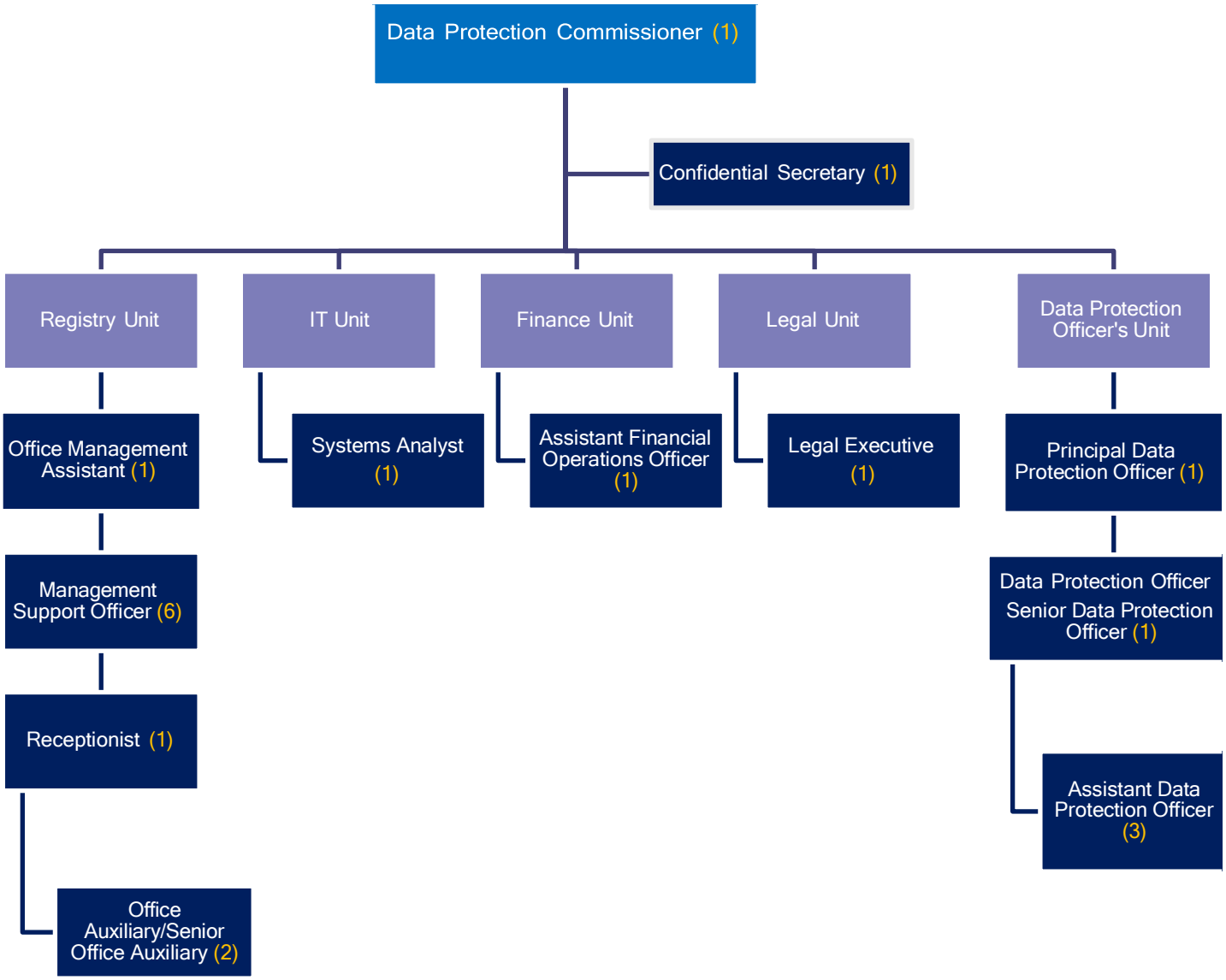


Figure 1: DPO Organisation Structure

I. Human Resource Requirements

Over the years, the office has consistently faced significant challenges due to the critical shortage of departmental staff, which has hindered its ability to effectively fulfill its mandate. The core implementation of the office's functions, carried out by the Data Protection Officer's unit, is severely constrained by a very limited workforce. The actual number of officers in post is largely inadequate and this shortage makes it extremely difficult to provide the necessary services to all citizens of Mauritius, implement compliance and enforcement across the public and private sectors and engage in international cooperation.

For instance, the grade of Data Protection Officers/Senior Data Protection Officers has registered a staff leaving rate of 85.7% over the years and replacement has not yet been completed. The percentage of staff leaving is namely related to better salary opportunities in public and private sectors.

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**
Assistant Data Protection Officer	**6**	**3**	**3** (joined in September 2024)
Legal Executive	**2**	**1**	**1** (joined in September 2024)
Principal Data Protection Officer	**2**	**1**	**1**
Deputy Data Protection Commissioner (Legal - new post)	**1**	**Nil**	**Nil**
Assistant Data Protection	**2**	**Nil**	**Nil**

Commissioner (new post)	(Legal:1 and Information Technology:1)		

b) Other human resources required

i. Police Unit

Sections 6 (Investigation of complaints), 7 (Power to require information), 8 (Preservation order), 9 (Enforcement notice), 10 (Power to seek assistance), 11 (Power of entry and search) and 53 (Prosecution and jurisdiction) of the DPA are police duties. DPO requires assistance from the police to ensure effective criminal law enforcement under the DPA. The DPC has powers to delegate any investigating or enforcement powers to the police as provided under section 13 of the DPA. The police is thus collaborating with DPO by providing assistance in the investigation of complaints especially CCTV camera cases.

Furthermore, to enhance legal enforcement, it is essential to urgently establish a dedicated prosecution unit with seconded police officers to ensure the smooth operations of this office. This unit will be tasked with managing complaints and overseeing prosecutions related to violations, ensuring that all legal processes are followed thoroughly and efficiently.

ii. Deputy Data Protection Commissioner

The grade of Deputy Data Protection Commissioner is essential to provide assistance to the DPC and to deputise for the Data Protection Commissioner, as and when required. The scheme of service has not yet been prescribed.

II. Running cost of the office

The running cost of the office for the financial year 2024-2025 is Rs 5.6 million.

I. Workshop on "Data Protection for the Youth"

The Data Protection Office organised a half-day workshop themed 'Data Protection for the Youth' on 18th July 2024. Around 400 participants mostly educators from primary, secondary and tertiary level and students attended the workshop.

As part of the office's mandate to promote awareness on data protection, the Data Protection Office developed an informative video titled "*The Guardians of Privacy: Empowering Youth in the Digital Age*" which was launched during the workshop. The video is available on the link: https://dataprotection.govmu.org/SitePages/SliderReadMore.aspx?IDS=76

The video aimed to educate young people on the importance of data protection, online privacy and responsible digital behaviour. It focused on the following key points:

- Understanding the significance of personal data.
- Recognising potential online threats and risks.
- Practicing responsible and ethical use of digital platforms.
- Educating on the legal aspects of data protection.

The video was distributed to participants of the workshop as part of the office ongoing efforts to promote digital literacy and safeguard personal data.

II. European Union Adequacy

Since 2022, extensive discussions, consultative meetings and information exchanges between the Data Protection Office and the European Commission have been carried out to develop the necessary legal framework for Mauritius to achieve adequacy.

The rationale for Mauritius EU adequacy of Mauritius are:

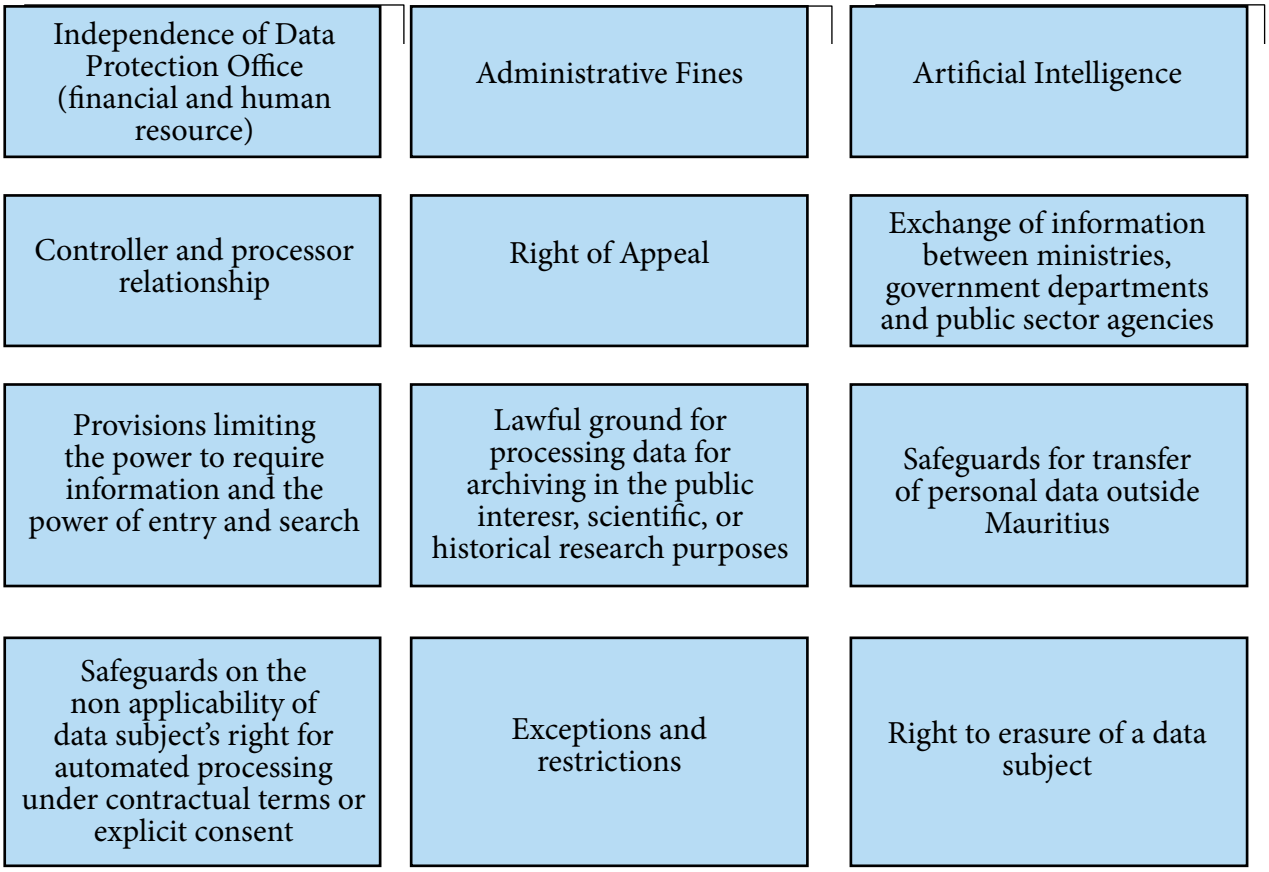
- Firstly, Mauritius data protection law will receive recognition from EU as providing protection equivalent to the global benchmark for privacy and data protection, namely the General Data Protection Regulation.
- Secondly, adequacy will facilitate cross-border data transfers from the EU to Mauritius without any further safeguard being necessary.
- Thirdly, achieving adequacy will give Mauritius a competitive edge over other countries in the region and globally that do not meet EU's stringent data protection requirements, positioning it as a regional leader in data protection.
- Fourthly, there have been instances where companies were compelled to cease operations in Mauritius due to the lack of EU recognition.

The benefits of Mauritius achieving EU adequacy are long term, offering both financial advantages and non-financial gains.

- From a financial perspective, Mauritius will attract increased foreign direct investment from Europe since businesses prioritise data security and regulatory compliance in their operations. Additionally, adequacy will simplify market entry for Mauritian companies in Europe, boosting economic growth, creating jobs and opening new trade opportunities. It will also facilitate seamless data transfers between Mauritius and EU member states. Mauritius will thus become more attractive as an international financial and business hub to EU-based companies, particularly in sectors that depend on data processing such as financial services, artificial intelligence, fintech, business outsourcing, e-commerce and ICT.
- On the non-financial side, EU adequacy will enhance Mauritius's international reputation and build consumer trust. Seeking adequacy also highlights Mauritius's commitment to protecting the privacy rights of its citizens. Furthermore, in today's era where data breaches and misuse of data are frequent, demonstrating a robust data protection framework is a strong signal and deterrent to multinational companies that are seriously involved in ensuring compliance with data protection laws.

A draft Data Protection Bill as recommended by the European Commission has been submitted to the Ministry of Information Technology, Communication and Innovation for

consideration. The draft Bill includes several amendments to the DPA covering aspects such as:



III. Guide On Data Protection in the Mauritian Financial Sector

In 2024, the office finalised a guide titled "Data Protection in the Mauritian Financial Sector" which delved into the critical importance of data protection in the financial sector amidst data breaches and cyber threats, which could have financially devastating and reputationally catastrophic consequences. The guide imparts knowledge, best practices and insights on data protection for institutions in the financial sector. It aims to provide guidance on the processing of personal data performed by financial entities to ensure compliance with data protection principles under the Data Protection Act of Mauritius. The guide was drafted after consultation with relevant stakeholders in the financial sector. The office is awaiting approval of its parent Ministry for the printing of the guide.

IV. President of Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)

On 28 October 2024, AFAPDP held its 16th General Assembly in the city of Saint-Helier, at the invitation of the Jersey Data Protection Authority. Thirteen member authorities participated in this significant meeting, rich in discussions and important decisions for the future of the association.

A historic election: first President and first representative of the Indian Ocean at the head of the AFAPDP

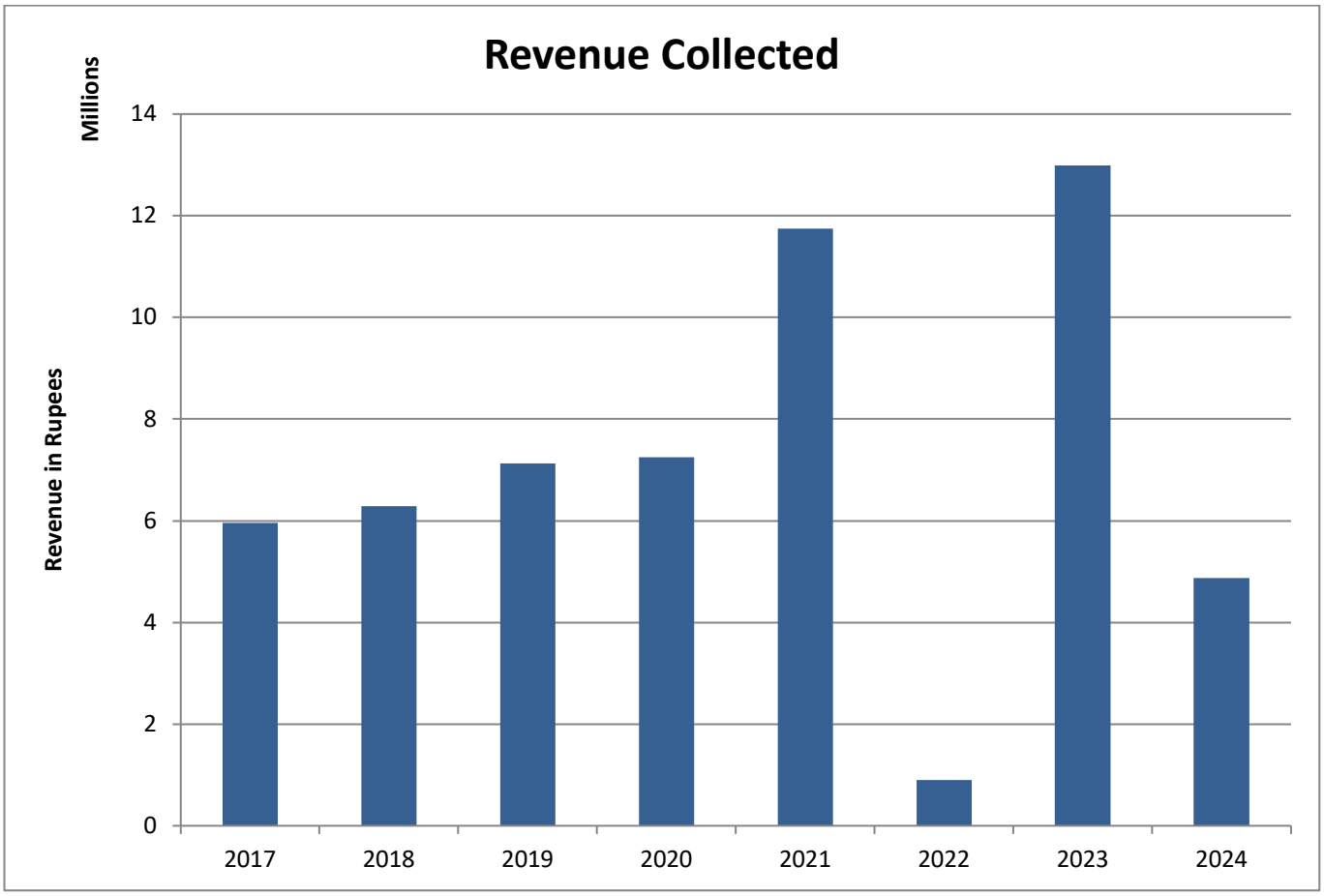
This meeting was marked by a great first: the election of Mrs. Drudeisha Madhub, Data Protection Commissioner of the Republic of Mauritius, as President of the AFAPDP. Her election was a historic moment for the Association since she became the first woman to hold this position, as well as the first representative from the Indian Ocean region to sit on the Association's Bureau.

Her leadership promised to contribute significantly to the collective efforts of AFAPDP to meet contemporary challenges in terms of personal data protection and fundamental rights in the French-speaking world.

I. Financial Status

(a) Revenue collected

DPO collected a total revenue of Rs 4,873,400 for registration of controllers and processors in 2024.



In 2024, revenue was lower than in 2023 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 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

i. African Union (AU) Commission

The Ministry of Information Technology, Communication and Innovation agreed to participate in the Technical Assistance Program coordinated by the African Union Commission, in close collaboration with Regional Economic Communities (RECs), to support the implementation of the AU Data Policy Framework. The Data Protection Commissioner participated in an online meeting organised by the AU Commission on 5 April 2024, along with other stakeholders, to discuss the specific needs of Mauritius and to agree on the way forward regarding the support that will be provided in terms of developing data policies and regulations, as well as building data capabilities.

On 28 August 2024, the office further participated in an online meeting on "Technical Assistance Program on data Policy & Governance".

ii. Council of Europe (CoE)

The Council of Europe invited the Data Protection Commissioner to participate online as panelist in CPDP 2024 held on 22nd May 2024 to discuss the topic 'Council of Europe Model Contractual Clauses (CoE MCC)'.

On 10 June 2024, the DPC participated online as a panelist in the 'Privacy Symposium 2024' organised by CoE in Venice on the theme 'Convention 108+ A Wind of Change'.

On 06 May 2024, the DPC participated in the online meeting "Working Group on Article 11 (GT-Art.11)''.

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

The Office of the Data Protection Commissioner of the Republic of Kenya hosted the NADPA - RAPDP Conference & AGM from 7th to 9th May 2024. The Data

Protection Commissioner participated online as speaker on the panel "Towards building a safe and trusted digital space for children".

iv. OECD

Upon invitation from OECD, the DPC participated as panelist on the topic "Privacy considerations in Open Banking and Open Finance" on 21 June 2024 during the Digital Finance in Africa Roundtable that was held in Mauritius.

In October 2024, the Data Protection Office completed the OECD survey for evaluating OECD current position and guiding their future engagement with the global community.

The DPC also participated in the following online meeting with OECD:

18 April 15h30-17H00	OECD "Expert Community on Data Free Flow with Trust (DFFT)" - First meeting - Discussion on possible cooperation

v. World Bank

The Data Protection Office completed the Business Regulation and Enforcement Toolkit for Digital Markets (BRET-D) Data Market Module questionnaire from World Bank. The self-assessment tool was designed to help emerging markets and developing economies identify the minimum package of regulations, institutional arrangements and enforcement actions needed to build trustworthy and safe digital markets. The data market module aimed to help authorities identify gaps and prioritize actions. The work was built on the World Bank's experience working over the years with multiple countries on data policies by taking into account good practices commonly recognised in different international and regional organisations, as well as free trade agreements. The data will help build a harmonized global database, which will facilitate country analysis and regional comparisons using a market institutional approach.

In this context, the DPC attended an online meeting with World Bank as follows:

Date	**Topic**	**Organisation**
8 April 15h00-17H30	Présentation de l'initiative BRET-D sur les nouveaux marchés de données	Digital Market Regulation World Bank

(b) Other virtual meetings

During 2024, the DPO participated in numerous prestigious international virtual meetings with the active participation of the DPC who shared the Mauritius data protection experience and journey. Her interviews, presentations and valuable insights have been deeply appreciated by foreign counterparts. Officers from the Data Protection Officer's unit have done substantial research on topics discussed on the international forefronts and have assisted the DPC in the preparation of materials and briefs for the DPC's interviews and presentations. The DPC participated in the below virtual meetings in 2024:

- **Second edition of the Massive Open Online Course (MOOC) on the right to privacy in the digital age in Africa**

  On 24 June 2024, the Data Protection Commissioner participated as panelist in the webinar for the launch of the second edition of the Massive Open Online Course (MOOC) on the right to privacy in the digital age in Africa. The session was themed "Stakeholders' role in data privacy in Africa."

- **DS-I Africa: Engaging Policy Makers Webinar**

  On 19 August 2024, the DPC participated as a speaker in the DS-I Africa webinar on "Engaging Policymakers in Health Research." This session was part of DS-I Africa's ongoing efforts to support the development of a thriving African data science community. The DPC addressed the following topics:

  a) Effective communication with data protection officers:
     - Tips for building a strong working relationship with data protection officers.
     - How to effectively communicate research needs and concerns regarding data privacy.

  b) Engagement strategies for policymakers and stakeholders:
     - Approaches to advocating for research-friendly data protection policies.
     - Building partnerships with policymakers to facilitate the integration of research findings into health policies while ensuring data protection.

- **Data Protection Africa Summit 2024**

  The DPC participated virtually in the Data Protection Africa Summit 2024, organized by the Africa Digital Rights Hub (ADRH), a not-for-profit think tank based in Accra, Ghana, dedicated to advancing research and advocacy on digital rights across the African continent.

  Held in Kampala, Uganda, from 2nd to 5th December 2024, the Summit was themed "Data Protection Compliance: A Catalyst for Africa's Digital Transformation." It aimed to shape policies, explore financing options and identify pathways to leverage technology and innovation for delivering critical infrastructure and services, driving Africa's economic transformation and sustainability.

  The DPC delivered a keynote address on "Privacy Enforcement in the Digital Age: Challenges, Solutions & Strategic Partnerships."

- **Webinars**

  Officers from the Data Protection Officer's unit attended the following webinars:

Date	Topic	Organisation
01-Oct-24	Public Awareness and Promoting Compliance	AFAPDP
3-Oct-24	EDTECH AI in education sector	CNIL Digital Education Working Group and UNICEF
12-Nov-24	Network Meeting	Global PETs
12-Nov-24	Que retenir des nouvelles recommendations de la CNIL	CNIL
26-Nov-24	Comment déployer un système d'IA générative : les premières préconisations de la CNIL	CNIL
3-Dec-24	Applications mobiles : Comment prendre en compte les nouvelles recommandations de la CNIL lors de développements techniques	CNIL

III. Participation in surveys

In 2024, the office participated in the following surveys:

- The office provided inputs to the Human Rights Division of the Ministry of Foreign Affairs, Regional Integration and International Trade concerning the advanced questions posed by Germany for the Universal Periodic Review Report 2023.

- SADC Financial Consumer Protection Guidelines Dashboard Baseline Assessment Survey Questionnaire

  The Data Protection Office submitted inputs on privacy and data protection to the Ministry of Foreign Affairs for the survey on Financial Consumer Protection(FCP) among SADC Member States, conducted by SADC Secretariat. The purpose of the survey was to gather information for the creation of a dashboard to track the implementation progress of the Financial Consumer Protection guidelines. It will also help in assessing the extent to which Member States have aligned their legal and regulatory frameworks and practices with the FCP guidelines. The ultimate goal of the dashboard is to achieve greater financial inclusion and regional financial integration based on sound consumer protection.

- DPA Public Sector Approach - Mauritius Data Protection Office

  The International team of the UK Information Commissioner's Office (ICO) requested inputs from this office. In June 2022, the ICO revised its approach to working with public sector organisations and started a two-year trial approach. The ICO then conducted a review of the two-year trial period, which included an international benchmarking element. As part of this international benchmarking exercise, the ICO requested contextual information to understand this office approach to imposing penalties on public authorities.

- SADC CCBG Regional Initiatives on e-KYC and Consumer Education Survey

  The CCBG's Payments Systems Subcommittee (PSS), in partnership with FinMark Trust (FMT), requested the Data Protection Office to provide inputs on a questionnaire developed in line with the Strategic Focus Areas (SFAs) outlined in the PSS's 2023-2026 Strategy aimed at fostering financial integrity and enhancing financial inclusion in the SADC region.

The questionnaire will enable FMT to better understand the current payments environment in Mauritius and to conduct baseline assessments of existing frameworks as well as feasibility studies for proposed harmonised frameworks.
The Data Protection Office completed the questionnaire in September 2024.

- Survey on Edtech

  The Data Protection Office submitted inputs to the survey developed jointly by the Digital Education Working Group (DEWG) and UNICEF on EdTech. The survey focused on data protection authorities' relationships with ministries and schools on these issues whilst exploring the various practices and approaches with EdTech. The questionnaire aimed at

  - Establishing a landscape review in terms of the data governance issue of EdTech in schools, particularly with regard to the various roles of the stakeholders involved;
  - Sharing examples about data protection authorities experiences in the development of case studies, such as sandboxes, codes for children, school charters, EdTech guidelines, amongst others;
  - Starting a process of evaluation of the 2018 GPA Resolution on eLearning platforms.

IV. 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 sensitisation activities were carried out during 2024.

(a) Press Communiqués/Interviews

- **Press Interviews**

At the request of BDO IT Consulting, the Data Protection Commissioner submitted an article titled 'Navigating the Intersection of AI and Data Protection' for the Data Privacy Newsletter 2024.

In conversation with

Drudeisha Madhub

Data Protection Commissioner at Data Protection Office Mauritius

Question 1

Describe how the Data Protection Office (DPO) drove operational change by educating organizations in Mauritius about data protection laws. What are the initiatives undertaken by the DPO to influence the understanding and implementation of a Data Protection Framework?

Mauritius data privacy framework has been recognized by UN as a leading example in the region. The Privacy Symposium of Africa hosted by this office in November 2023 showcased the success of the data privacy framework Mauritius has implemented so far.

Master Classes at the PSA were delivered to participants with a deeper understanding of the latest developments and best practices in the field of privacy and data protection. They were led by experienced privacy professionals and experts, and provided participants with hands-on training and practical knowledge on a range of privacy-related topics. The Privacy Scorecard Report provided an overview of the privacy and data protection regimes in Uganda, Kenya, and Mauritius. The panel discussions were an important part of the event, as they provided a platform for participants to engage in thoughtful and insightful discussions on the latest developments and challenges in the field of privacy and data protection.

The office undertakes a panoply of compliance and enforcement activities to ensure an effective application of the DPA as can be demonstrated by some statistics below:

Registration of controllers	Registration of processors	Registration revenue (2022)	Complaints	Investigation findings delivered	Appeals against decisions of Data Protection Commissioner
19,071	1013	Rs 2,736,500	450	73	7 (5 upheld)

Cases won at the Supreme Court of Mauritius	Authorisations for data transfer	Notifications for personal data breaches	Data Impact Assessment analysed	Request for data protection certificate	Certification Awarded
2	345	150	19	6	1 private company

- Regular interventions are made by the Data Protection Commissioner (DPC) in press interviews, conferences, seminars and international online meetings
- The office 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 and the United Nations, amongst others
- The Data Protection Office has implemented a new system, e-DPO, which is an Integrated System that enables Controllers and Processors to do their registration online on the website of the Data Protection Office. The e-service is available 24/7 and provides for:
  - Online registration and renewal of controllers and processors with e-payment facility,
  - Online search of registered controllers and processors
  - Online lodging of complaints and submission of forms (personal data breach notification form, data protection impact assessment form, transfer of data form, certification form and compliance audit form).
- A self-learning training toolkit has been produced and is available on our website. The toolkit explains the basics of the Data Protection Act 2017.
- The office has trained around 250 data protection officers through in-house training.
- This office has published 19 guides on data protection which are available on our website.
- Around 400 requests for legal advice are addressed each year to assist controllers and processors in the implementation of the DPA.
- The Data Protection Commissioner has launched a networking forum of data protection officers to promote knowledge sharing, collaboration and cooperation, learning opportunities and professional development.

Data Privacy Newsletter 2024

Africa Data Protection report

The Data Protection Commissioner was interviewed on the following questions for an article in the May report of Africa Data Protection:

a) How does the Data Protection Act 2017 compare with international data protection standards?

b) What are the main challenges your authority is facing in protecting the data of Mauritian citizens?

c) What are the specific fields where data protection is particularly critical in Mauritius, and what actions is your authority taking on these issues?

d) The Malabo Convention on Cybersecurity and Data Protection became effective in June 2023, nine years after its adoption by the African Union in 2014. How will you implement it?

e) Several discussions on artificial intelligence (AI) are ongoing in Africa. How is your authority dealing with ethical concerns related to the use of AI?

(b) Raising awareness with businesses

- **Ethics and Data Privacy Workshop**

  The Mauritius Institute of Directors (MIoD), in collaboration with the Data Protection Office, organised a workshop on Ethics and Data Privacy on 29 January 2024. The workshop coincided with the Data Privacy Day 2024, emphasizing its relevance in the current business environment.

  The Data Protection Commissioner presented an insightful session on "An Ethical Approach to Data Privacy," offering a nuanced understanding of current data protection challenges and strategies. This was augmented by an exclusive preview of the DPO Guide on Data Protection for the Financial Sector, setting new benchmarks for data handling in the industry.

  The collaboration effectively fostered a platform for learning and dialogue for the attendees, highlighting the necessity for organisations to adeptly manage customer data while upholding ethical standards.

- **BDO IT Consulting Ltd - 'Navigating Data Privacy in the Era of AI'**

  The Data Protection Commissioner participated as a keynote speaker in the workshop organised by BDO IT Consulting Ltd, which had the theme 'Navigating Data Privacy in the Era of AI' on 1st March 2024. Additionally, the Data Protection Commissioner contributed as a panelist in the panel discussion on the question "Given the rapid advancements in AI technology, how can regulatory bodies effectively balance the need for innovation with the imperative to protect individuals' data privacy rights?"

- **Celebration of Independence Day at Ebene State Secondary School (SSS)**

  The Data Protection Commissioner attended the Flag Raising Ceremony as Guest of Honour at Ebene SSS boys on the occasion of the Independence Day of Mauritius. The DPC addressed the students on the importance of education, digital education for students, data protection for youngsters and the dangers of social media to young people.

- **Workshop organised by Junior Chamber International (JCI)**

  The Data Protection Commissioner recorded a video explaining the importance of data protection for NGOs, which was disseminated in a workshop organised by Junior Chamber International (JCI) Port Louis on 17 August 2024. The office also provided answers to data protection queries from JCI Port Louis.

- **Annual IIA Mauritius Conference**

  The DPC participated as speaker on the topic "Data Protection Audits – An essential component of compliance" at the Annual IIA Mauritius Conference on 11th October 2024. The theme of the conference was "Forging Forward, Charting new frontiers."

- **Data Privacy and Information Security in the modern digital era of AI**

  Kredence Capacity Building Ltd hosted a forum on Data Privacy and Information Security in the modern digital era of AI on 22nd October. An officer from the Data Protection Officer's unit participated as speaker on the topic ""Continued Enforcement of Privacy Regulations".

- **Sensitization programme to commemorate the Human Rights Day**

  The Human Rights Division in collaboration with the Office of the Ombudsperson for Children organized an Awareness Programme focused on 'Child Safety Online on 11th December 2024. During this event, the legal executive from DPO delivered a presentation on 'Data protection and digital privacy for children'.

(c) Training

- **In-house training**
  - The Data Protection Officer's unit and the Data Protection Commissioner conducted an in-house training for approximately 30 participants on 25 April, 24 October and 26 November 2024.

(d) Guidelines

- **Insurance sector**

In 2024, the Data Protection Commissioner issued crucial guidelines aimed at strengthening data protection practices within the insurance sector. These guidelines focused on the registration of insurance salespersons as processors and the establishment of data processing agreements between insurance companies and insurance salespersons. The primary goals were to ensure the secure handling of personal data by salespersons and reinforce the industry's commitment to client privacy.

The main points of the guidelines were:

a) Registration as Processors

All insurance salespersons engaged in processing personal data on behalf of insurance companies must be registered as processors with the Data Protection Office. A registration certificate is valid for a period of 3 years. The

registration certificate must be renewed not later than 3 months before the date of its expiry.

The registration/renewal form must be submitted online on the link https://dpo.govmu.org/dpoPortal/login.jsf

b) Data Processing Agreements

Insurance companies must establish a data processing agreement with each insurance salesperson before any data processing activities commence. This agreement must include, but is not limited to, the following data protection clauses:

i. Purpose Limitation: Data must only be processed for the specific purpose(s) agreed upon by the insurance company and the insurance salesperson and must not be used for any other purposes without prior consent from the insurance company.
ii. Data Security Measures: The salesperson must implement appropriate technical and organisational measures to protect data under his/her custody.
iii. Access Control: The data processing agreement must define strict access controls to client data.
iv. Data Breach Notification: Salespersons are obligated to notify the insurance company of any personal data breach without undue delay and provide sufficient details for the company to comply with its reporting obligations to the Data Protection Office.
v. Confidentiality Obligations and unauthorised disclosure: Salespersons must be bound by confidentiality obligations regarding the handling of personal data ensuring that personal data is not disclosed to unauthorised individuals.
vi. Return or Deletion of Data: Upon termination of the agreement, all personal data must be returned or deleted in compliance with data retention policies with the insurance company.

c) Access to client's data

The insurance company must establish clear processes/procedures for controlling the disclosure of clients' personal data or previous policies to insurance salespersons. The insurance company must ensure that all its staff are adequately trained to follow these processes/procedures.

- **Cameras in schools**

In 2024, this office conducted a survey with several secondary schools regarding the use of CCTV cameras.

The use of CCTV cameras at the workplace is generally guided by the following key considerations:

1. Collection of Personal Data (section 23 of DPA):

When cameras collect personal data, employers must inform employees about various aspects of data collection, including the purpose(s), recipients, the voluntary or mandatory nature of the data collection, the retention period amongst others. Employees must also be made aware of their rights including their right of access and rectification.

2. Lawful Processing (section 28 of DPA):

Employers must have a valid reason for using cameras. Consent is not always required if the use of cameras is necessary for purposes such as contract performance, legal obligations, public interest or legitimate interests of the employer.

3. Conditions for Camera Use:

In furtherance of section 28 (vii) of the DPA, the use of cameras must meet three conditions:

- A legitimate interest to justify the processing.
- The use of cameras must be necessary to achieve the legitimate interest.
- The interest must prevail over the rights and interests of the data subject.

A Data Protection Impact Assessment (DPIA) must be conducted if the processing is likely to pose a high risk to individuals' rights and freedoms.

4. Camera Coverage:

CCTV should not be used in areas where privacy is expected such as bathrooms or changing rooms. Cameras should only capture footage within company premises and for the specific purpose defined.

5. Retention and Security (sections 27 and 31 of DPA):

Footage should only be used for the defined purpose(s) and once the purpose(s) has lapsed, the data must be destroyed unless retained for other legal obligations. Security measures must be in place to protect the data.

6. Data Subject Access Requests (section 37 of DPA):

Individuals whose images are captured have the right to request access to their data and obtain a copy of the footage. They can also inquire about the purpose(s), recipients and retention of the data.

7. Checklist for Camera Use:

Employers should assess the following:

- Purpose: Define the reasons for installing CCTV.
- Lawfulness: Identify the lawful basis for processing.
- Necessity: Ensure CCTV is the necessary solution.
- Proportionality: Ensure CCTV usage is proportionate.
- Security: Implement adequate security measures.
- Retention: Define the retention period for footage.
- Transparency: Inform employees about the monitoring.

Based on the findings of the survey, the Data Protection Commissioner issued the following recommendations for CCTV camera placement in schools:

School Spaces	Positioning
Classrooms	Cameras should be positioned to cover the entire classroom but avoid focusing on specific individuals unnecessarily.
School Yard	Cameras should be placed in a way that maximizes coverage of the yard.
School Entrance	Cameras should be positioned to capture individuals entering and leaving the school premises.
Staffroom	It is not deemed necessary but may be positioned at the entrance to capture only individuals entering and leaving the staffroom and not on staff.
Library	Cameras should cover entrances, exits and general library areas and avoid focusing on specific individuals unnecessarily.

Specialist Rooms (e.g., Laboratories, computer lab)	Cameras should be focused on key areas where safety is a concern, avoiding unnecessary surveillance of individuals.

A Code of Practice was issued on March 2010 by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force and is available for consultation on the office website. The key aspects of the guidelines focus on:

a) Initiation of a CCTV System

b) Siting Standards

c) Processing of CCTV Images

d) Disclosure of Images to Third Parties

e) Access by Data Subjects.

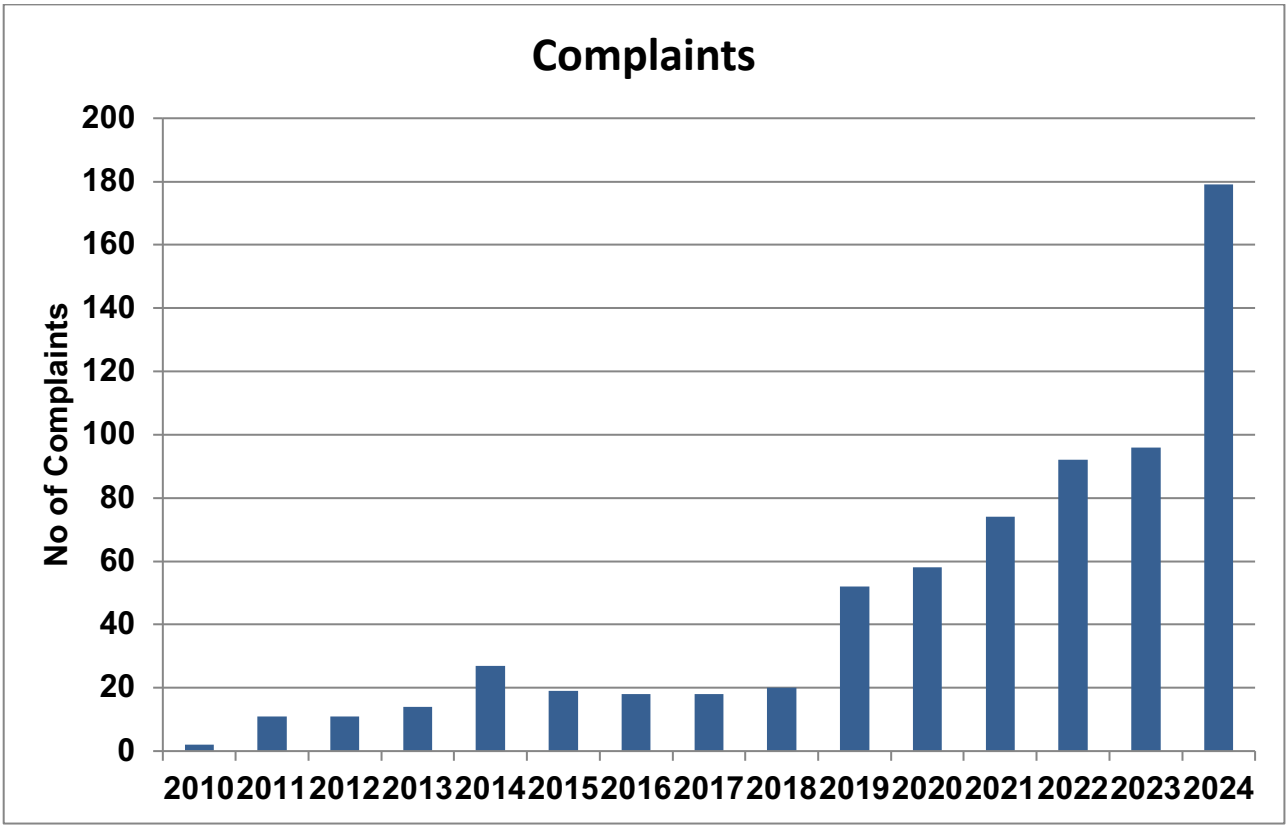
V. Enforcing Data Protection

(a) Investigation on Complaints

During the period January to December 2024, the DPO received **hundred and seventy nine (179)** new complaints regarding investigations on the below subjects among others:

- Unauthorised use of CCTV camera
- Unlawful disclosure of personal data
- Fingerprint
- Marketing

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



Out of the total number of cases, **hundred and fifty eight (158)** cases (representing 88 %) pertained to CCTV as depicted below.

- **Enquiries conducted by DPO in 2024**

Categories	Details
Closed Cases Involving CCTV Cameras (39 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 • Reoriented following intervention by the office and the Police.

	As a result, the thirty-nine (39) cases were closed. The enquiries were resolved to the satisfaction of the parties involved.
Ongoing Cases Involving CCTV Cameras (104 cases)	Hundred and four (104) CCTV-related cases were processed and were ongoing in 2024. 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 2024 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 (4 cases)	In 2024, DPO received four (4) 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:- • Two of the cases were closed following Police inspections of the workplaces. • One case remained ongoing as further information was being gathered. • For one case, officers from the DPO carried out an on-site investigation to assess the positioning of the cameras and their impact on employees' privacy. As a remedial measure, the Data Protection Commissioner convened a hearing at the office to resolve the matter to the satisfaction of all parties. During the hearing, the DPC emphasized that CCTV camera must be repositioned, informed this office of the corrective

	measures taken and that CCTV should only be placed in areas where it is strictly necessary.
Unlawful Disclosure of Personal Data (17 cases, 14 ongoing, 3 closed)	In 2024, DPO registered seventeen (17) cases concerning the unlawful disclosure of personal data. The reported matters included: • **Unauthorized sharing of customer information with third parties by employees (6 cases) –** In response to these complaints, the DPO conducted thorough investigations and requested detailed clarifications on the respondent's internal data protection policies, procedures and safeguards in place. DPO cross-examined the respondents on their compliance with data protection obligations which was evaluated and the complainant was informed to give his/her views on the measures implemented by the respondent. • **Disclosure of personal information to colleagues in the workplace (5 cases)** – In response to these complaints, DPO issued formal letters to the organizations, referencing the relevant provisions of the Data Protection Act and requesting their statements on the matter. Some have provided their statements which are being analysed. • **Unauthorized use of employee's email (2 cases)** – This office investigated the incidents and requested explanations from the organizations on how the unauthorized access occurred. • **Sensitive financial records shared without consent (1 case)** – DPO required the respondents to submit detailed reports outlining the circumstances under which the disclosure occurred. It was a case of misfiling

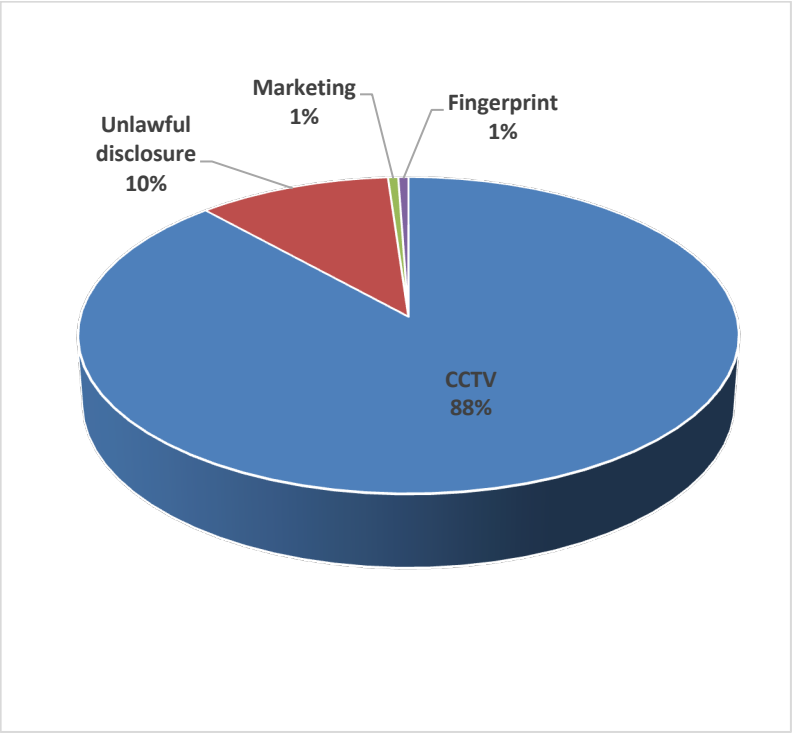
	by one of their employees. Appropriate security measures have been implemented to avoid such re-occurrence. Complainant was informed and the complaint was closed. • **Use of biometric data for attendance (e.g., fingerprints, facial recognition) without consent (2 cases) –** DPO checked if consent was obtained and provided legal advice to ensure proper safeguards were established. Organizations were reminded that biometric data is highly sensitive and requires clear consent before being collected or used. Enquiries are still ongoing. • **Unlawful interception and access of private conversations (1 case) –** DPO carried out site inspections at different organisations, carry out security audits and have meetings with them to clarify on our enquiries with a list of questions. Police assistance was requested to conduct further enquiries with related facts gathered during our preliminary enquiries. Out of the seventeen (17) cases: • Three (3) cases were closed after careful examination of the evidence, collection of statements and review of supporting records. Complainants were informed of the closure of the complaint to their satisfaction. • The remaining fourteen (14) cases remain under investigation, with DPO actively monitoring progress and engaging the concerned parties to ensure compliance with the Data Protection Act.

Right of access to CCTV footage (1 case)	In 2024, one case was registered concerning a request for access to CCTV footage in commercial area. In accordance with Section 39(1) of the Data Protection Act, DPO issued a letter to the respondent, instructing them to provide the complainant with a copy of the requested footage. The respondent replied, stating that they did not process any data. To confirm this statement, DPO officers conducted an on-site visit. The case was subsequently closed as it was confirmed that the respondent did not process any data and that no recordings or storage of personal data existed.

- **Inspections conducted by DPO**

During 2024, assistance from the police was solicited to conduct sixty-five (65) site visit inspections including the recording of statements from involved parties. The findings of the site visits and statements were then submitted to DPO for assessment and further actions.

In addition to site visits conducted for complaint investigations, DPO carried out four (4) compliance inspections under the DPA which was subject to the availability of human resources and other work commitments.



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.

(b) Complaints Closed

The office closed **thirty-nine (39)** complaints in 2024.

VI. 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 **three (3)** Supreme Court cases, where this office was a co-defendant and third party.

One case was withdrawn and the other two cases are ongoing.

(b) Intermediate Court Cases

The DPO appeared as a witness in **two(2)** CCTV-related cases for which complaints were filed at this office.

VII. 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 2024 reached **21219** and **1157** respectively. 3076 registration certificates were issued in 2024. The office has also attended a voluminous amount of phone calls and emails on registration of controllers and processors.

VIII. Requests for Legal Advice

In 2024, the office received around **two hundred (200)** written requests for legal advice on the interpretation of the DPA.

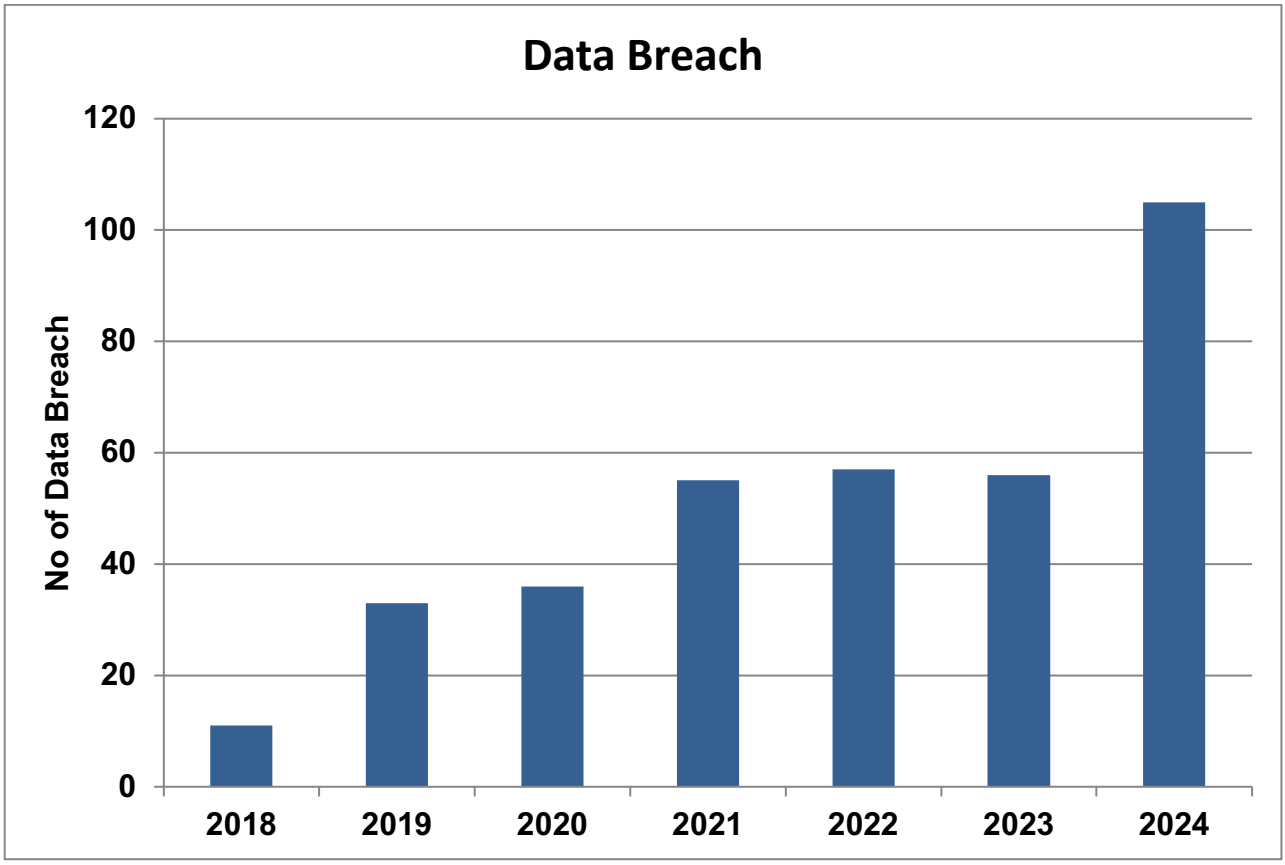
IX. Advisory /Stakeholder Role in Projects

DPO is a stakeholder in projects which involve the processing of personal data. In 2024, the office has provided recommendations on many projects from both the public and private sectors.

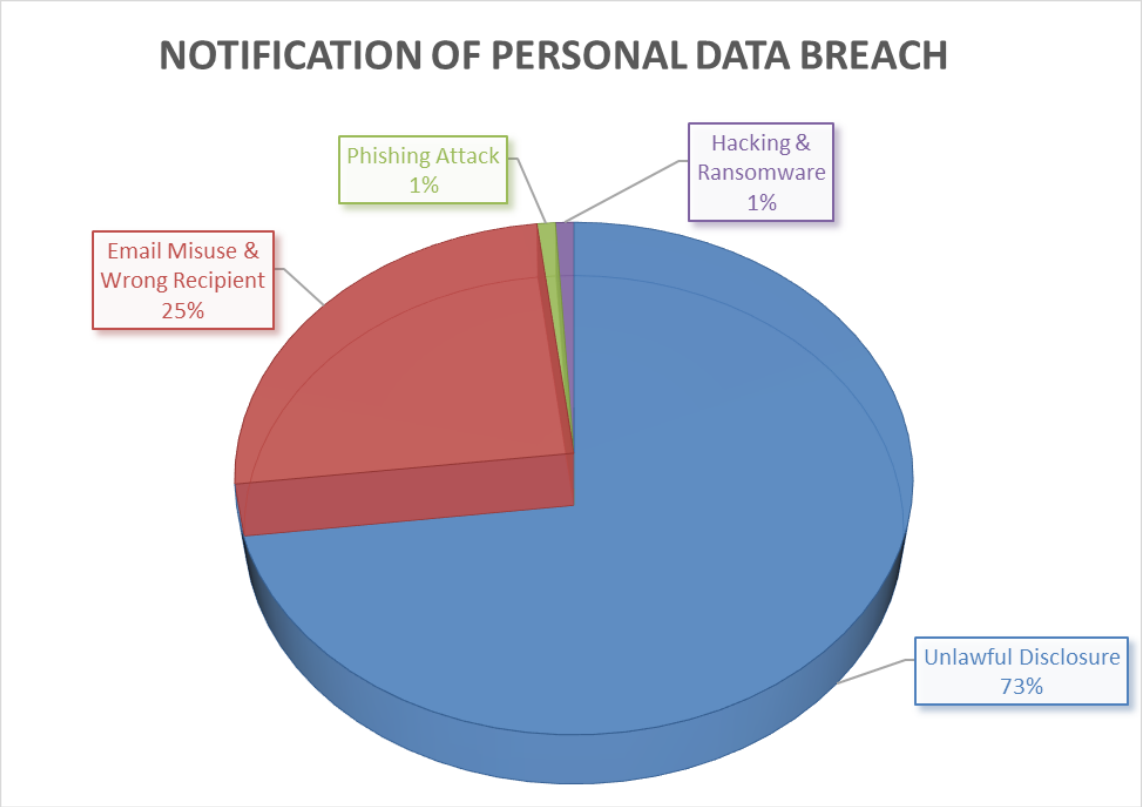
DPO is a representative in many Steering Committees such as the InfoHighway and MoKloud High Level Management Meeting.

X. Personal Data Breach Notifications

In 2024, **hundred and five (105)** personal data breaches have been reported to this office.



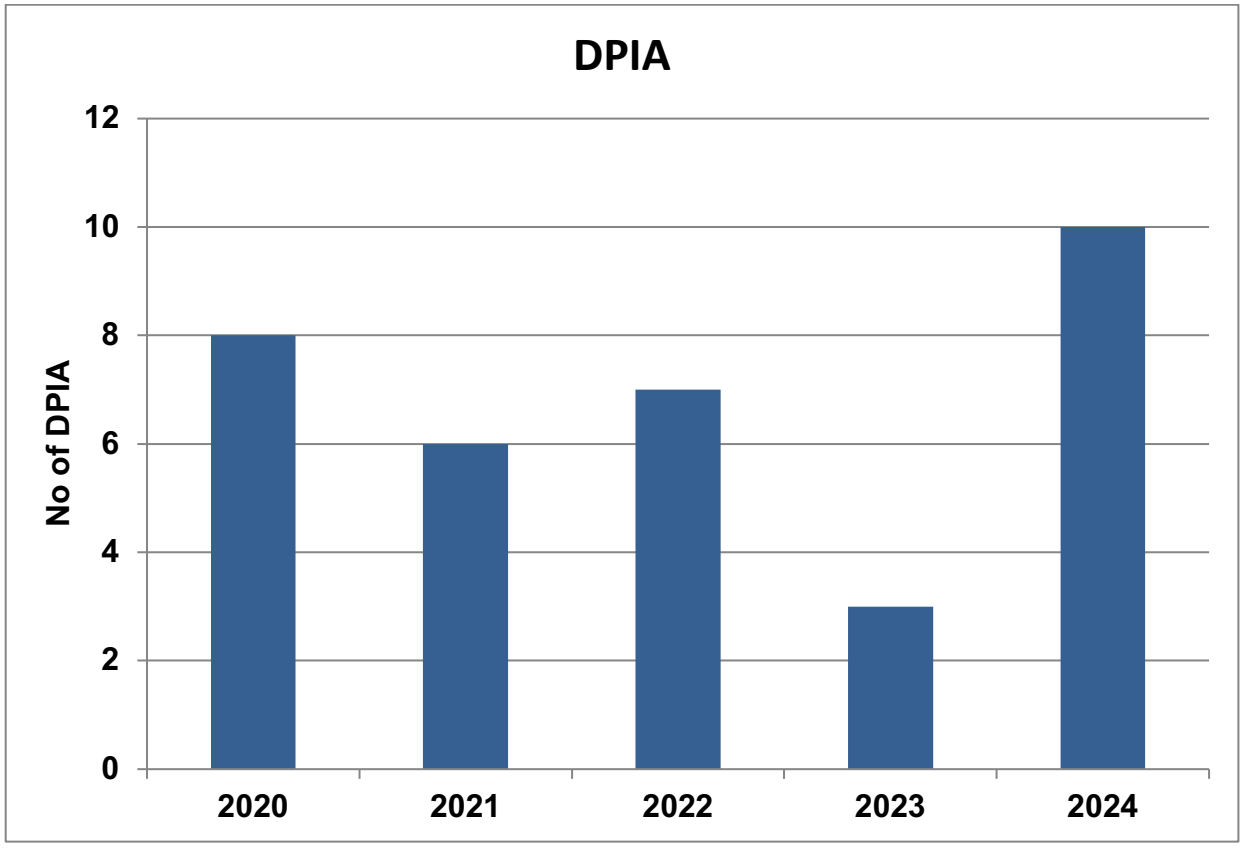
An analysis of the type of breaches received showed that unlawful disclosure and email misuse including sending email to wrong recipients remain the main causes of breaches reported. The following pie chart categorises the types of data breaches notified in 2024.



XI. 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 2024, the office has received **ten (10)** data protection impact assessments submitted by organisations.



In 2024, the office has studied and analysed **seven (7)** data protection impact assessments carried out by organisations.

XII. Transfers of Personal Data Abroad

The DPC authorised **hundred and twelve (112)** requests for transfer of personal data outside Mauritius with proof of appropriate safeguards under section 36 of the DPA. **Twelve (12)** applications for transfers were rejected due to insufficient safeguards mentioned on the forms.

XIII. 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.

The following processes are carried out by this office after submission of the completed certification form from an organisation:

(i) Analysis of all evidences submitted as per the certification form.

(ii) Meetings and exchanges with the parties involved.

(iii) Any corrective actions proposed/required to be completed within an agreed specified time frame.

(iv) submission by the organisation of a report of corrective actions taken.

(v) Any onsite verification/s required for final certification.

In 2024, the office reviewed the certification forms of four organizations and held a meeting with the data protection officers. However, the organisations withdrew their applications for certification.

XIV. Networking Forum of Data Protection Officers

The Networking Forum of Data Protection Officers performs the following roles:

a) Knowledge Sharing – providing a forum for Data Protection Officers to share their experiences, challenges and insights on the implementation of regulations and evolving best practices in data protection within their organisation.

b) Collaboration and Cooperation – data protection is a shared responsibility and collaboration between Data Protection Officers is crucial. The Networking Forum allows Data Protection Officers to collaborate on common issues, share resources and work together to address challenges collectively. This cooperation enhances the effectiveness of their data protection efforts and facilitates a coordinated approach to ensure compliance with data protection laws and regulations.

c) Learning Opportunities – the Networking Forum can facilitate the organisation of workshops, seminars and training sessions on various aspects of data protection. These events can feature expert speakers, industry professionals and legal advisors who can provide valuable insights and guidance to Data Protection Officers.

d) Professional Development – the Networking Forum plays a crucial role in fostering professional growth and development. By connecting with peers, Data Protection Officers can expand their professional network, establish relationships with experts in the field and gain access to career advancement opportunities. The forum can also

facilitate mentorship programs and mentoring circles where experienced Data Protection Officers can guide and support those who are new to the role.

In December 2024, the Data Protection Commissioner chaired a meeting with members of the networking forum to discuss forthcoming activities in 2025 and also celebrated the first anniversary of the forum.

CAPACITY BUILDING

In 2024, officers of the DPO attended the following capacity building sessions:

Course	Date	Training Institution
Strategic Management and Leadership Training Programme	18, 20, 22, 23 March 2024	Civil Service College Mauritius (CSCM)
Operation & Process Management Training Programme for Support Staff	19, 21, 23 February 2024 26, 28 February & 01 March 2024	CSCM
Training Programme for the Adoption of Generative Artificial Intelligence in the Public Sector	03, 08, 16, 23 & 30 April	CSCM
Capacity Building and Capability Development Programme for Public Officers	24, 26 & 30 April	CSCM
Safety and Health in Practice	19-Apr-24	Ministry of Public Service and Administrative Reforms (MPSAIR)
Operation & Process Management Training Programme for Support Staff	20,22 & 24 May	CSCM
Safety and Health in Practice	19-Jun-24	MPSAIR
Induction Course OMA	30/08/2024 03 05 10 13 Sep 2024	CSCM
Operation & Process Management Training Programme for Support Staff	21, 23, 25 Oct 2024	CSCM
Safety and Health in the workplace for MSOs	30-Sep-24	MPSAIR
Fire Safety and Fire risk Management for Fire Wardens	19 & 20 Nov 2024 3 & Dec 2024	MPSAIR

Operation & Process Management Training Programme for Support Staff	23, 25 & 27 Sep 2024	CSCM
Training Programme for the Adoption of Generative Artificial Intelligence in the Public Sector	20 & 25 Sep 02, 09 & 22 Oct 2024	CSCM
Leadership and Management Training Programme for Frontline/Supervisory/Technical Grade	11, 13 & 15 Nov 2024	CSCM
Safety and Health in the workplace for OA/SO	18-Nov-24	MPSAIR
Safety and Health in the workplace for OA/SO	18-Oct-24	MPSAIR
Operation & Process Management Training Programme for Support Staff	18,20 & 22 Nov 2024	CSCM

PROJECTS IN THE PIPELINE

I. Guide on Data Protection and Artificial Intelligence

The office has developed a draft guide on data protection in the context of artificial intelligence (AI). This guide addresses key issues such as data collection and storage, consent and transparency, anonymisation and pseudonymisation, model bias and fairness, secure deployment, data subject rights and auditing. It also explores future trends and considerations in the rapidly evolving field of AI.

To enhance the guide's content, the DPO has sought the collaboration of international partners namely the OECD and the US Embassy. The DPC carried out online meetings on 23 and 30 September 2024 with OECD and US Embassy respectively. This collaborative effort aims to ensure that the guide remains comprehensive and aligns with global best practices in data protection and AI.

II. Workshop on Data Protection Day

The Data Protection Office wrote to its parent Ministry regarding the organisation of a full day workshop for the Data Protection Day on 28 January 2025.

RECOMMENDATIONS

1. Enhance Staffing and Resource Allocation

To address the persistent challenges faced by the Data Protection Office due to staff shortages, it is recommended to prioritize the recruitment of additional personnel, particularly in critical grades such as Data Protection Officers. An urgent attention should be given to recruitment to ensure the timely hiring of staff to fulfill the growing demands of enforcement, compliance and international cooperation. Furthermore, a dedicated police unit and prosecution team should be established to streamline the investigation and enforcement of data protection violations.

2. Advance EU Adequacy Implementation

As Mauritius continues to work toward achieving EU adequacy, it is vital to expedite the implementation of the necessary legal reforms.

Data Protection Office
Email: dpo@govmu.org
Website: http://dataprotection.govmu.org
Tel: 4600251 Fax: 4897341
Address: 5th Floor, Sicom Tower, Wall Street, Ebene