Data Protection Office

2023
ANNUAL REPORT

15th Edition

Data Protection Office

2023

ANNUAL REPORT

15th 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

2023 has been a year full of important responsibilities and challenges for the Data Protection Office, given its persistent acute shortage of qualified personnel over the years, to shoulder the functions elaborated under section 5 of the Data Protection Act.

Given the fast evolutive environment associated with data digitalisation globally, the local landscape is no exception, which is evidenced by the numerous data breaches happening across all sectors with heightened interventions required from this office.

Ranging from inspections to complaints handling and decisions delivered, certifications, data protection impact assessments, compliance audits, training of data protection officers both in public and private sector, sensitisation campaigns, regular international cooperation on the development of international data privacy standards, legal opinions based on queries received, online monitoring of the E-DPO system, this office has been very active ensuring an efficient and customer oriented delivery of its services.

The production of the guide for the financial sector to regulate data privacy is one of its most important achievements and highly sought after by professionals in the finance sector.

Data protection occupies a very prominent place in compliance today and to ignore the benefits that such compliance brings will result in a heavy price for all sectors dealing with personal data, affecting trust in the quality and reliability of services, their reputation and the international image of the country as a whole.

The statistics relating to the number of complaints received by this office is testimony of the fact that awareness about data protection issues has reached a reasonable level of torching the various layers of our society.

The role of the data protection officer within each organisation is one of the key components of compliance which is depicted by the amount of trainings being delivered by this office to equip these officers with the required knowledge in the exercise of their daily functions.

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 measure 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

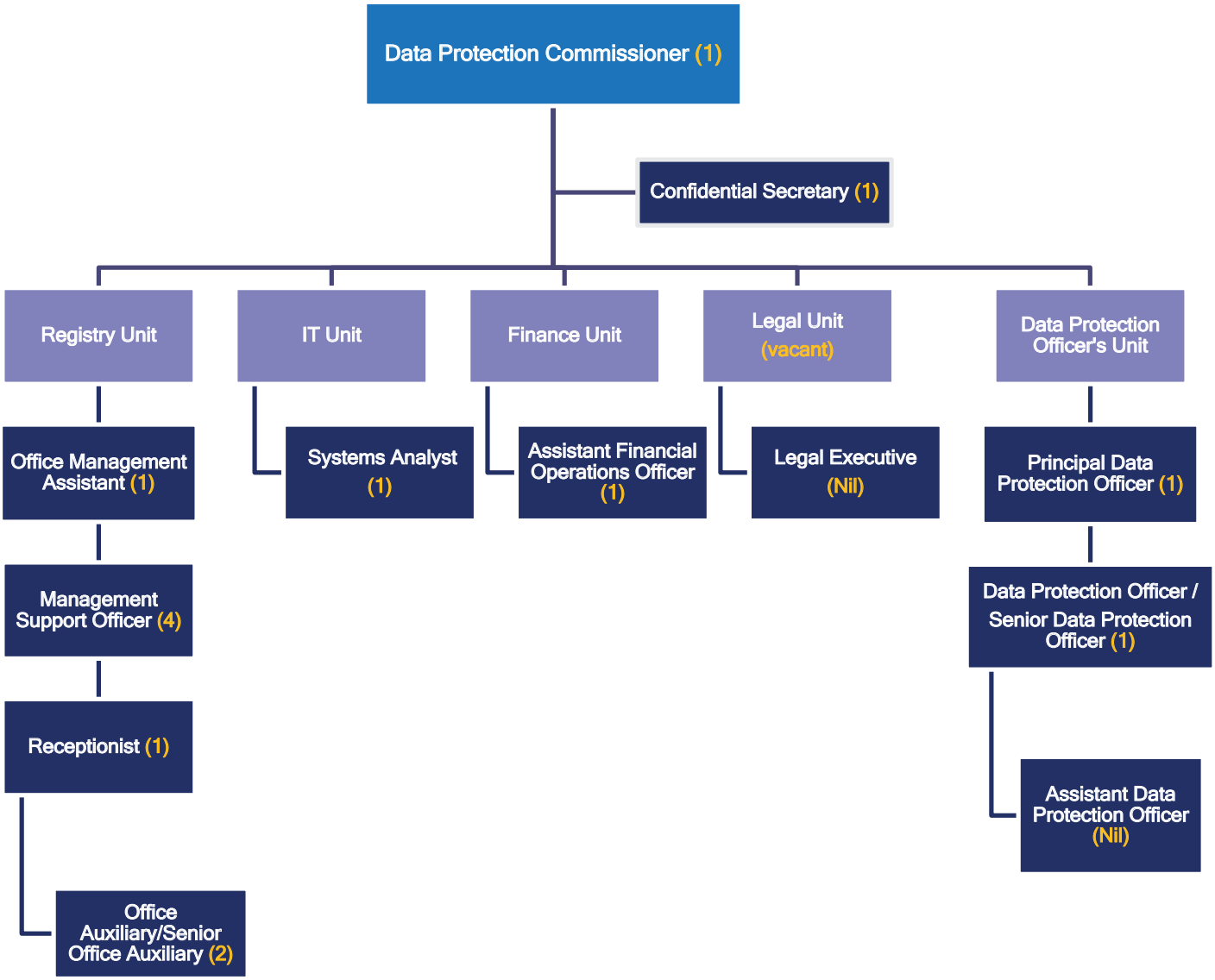


Figure 1: DPO Organisation Structure

BUDGET FOR FINANCIAL YEAR 2023 – 2024

I. Human Resource Requirements

Over the years, the office has been struggling with a persistent staffing issue that hinders the execution of its mandate, as evidenced by the following:

a) Recruitment of departmental staff has not been undertaken for the past **8 years**, leading to a **85.7%** staff leaving rate among Data Protection Officer/Senior Data Protection Officers.

b) For over 2 years now, the office is operating in a solo mode at the level of the 3 departmental grades namely the:
   - Data Protection Commissioner (DPC),
   - Principal Data Protection Officer and
   - Data Protection Officer/Senior Data Protection Officer.

   Each day presents new challenges as a result of the substantial workload and responsibilities stemming from the DPA, the alarming percentage of staff departures without replacements and the lack of recruitment for additional human resources.

c) Grades for "Legal Executive" and "Assistant Data Protection Officer" whose schemes of service were prescribed since 2019 are still unfilled.

a) Chart on human resources required and number of officers approved

Grade	Number of officers in post	Number of posts required	Number of additional officers funded
Data Protection Officer/ Senior Data Protection Officer	**1**	**11** (5 for replacement + 6 additional)	**4**
Principal Data Protection Officer	**1**	**1** (additional)	**Nil**
Assistant Data Protection Officer	**Nil**	**3**	**3**
Legal Executive	**Nil**	**2**	**1**
Deputy Data Protection Commissioner (Legal - new post)	**Nil**	**1**	**Nil**
Assistant Data Protection Commissioner (new post)	**Nil**	**2** (Legal:1 and Information Technology:1)	**Nil**

Vacancies for Assistant Data Protection Officer, Data Protection Officer/ Senior Data Protection Officer and Legal Executive were advertised on 22 June 2023, 04 October 2023 and 27 October 2023 respectively. As of 31 Dec 2023, these posts have not yet been filled and matters are being followed up with the Public Service Commission.

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 is thus delegating any investigating or enforcement powers to the Police as provided for under section 13 of the DPA. The Police is collaborating with DPO by providing assistance in the investigation of complaints.

ii. Youth Employment Programme (YEP) Trainees

YEP trainees have played a crucial role in carrying out specific tasks of the office, particularly related to registration and renewal of controllers and processors. The number of YEP trainees posted at DPO for each year is outlined below:

Year	**Number of YEP trainees posted at DPO**
2021	7
2022	6
2023	6 ⟶ 0

Unfortunately, as of 31 December 2023, all 6 YEP trainees left. The office requested their replacements to our parent Ministry. Action has been initiated for replacement with Ministry of Labour, Human Resource Development and Training but no replacement was effected.

Running cost of the office

The running cost of the office for the financial year 2023-2024 is Rs 5.5 million and has remained the same as for the previous financial year 2022-2023.

2023 HIGHLIGHTS

I. Data Protection Day 2023

The Data Protection Day is celebrated globally each year on the 28th of January to raise awareness and promote privacy and data protection best practices. This day commemorates an international effort to encourage everyone to own their privacy responsibilities and to protect data to create a culture of privacy. 28 January 2023 marked the 17th edition of the Data Protection Day.

The office engaged in numerous activities to celebrate this special day as follows:

a) The Data Protection Commissioner was interviewed by the Mauritius Broadcasting Corporation. The interview was broadcasted on 28 January 2023.

b) The Data Protection Office and the Ministry of Information Technology, Communication and Innovation organised a conference on the theme '*Protecting personal data across all economic sectors*' on 30th January 2023 at the Shri Atal Bihari Vajpayee Tower in Ebène to mark the Data Protection Day.

The objective of the conference was also to sensitise individuals on the importance of respecting data privacy and enabling trust in our day-to-day operations. Speakers from the public and private sectors namely telecommunications, banking, insurance, healthcare, police, cybersecurity, amongst others, participated during the event and shared valuable knowledge with the audience. Around 200 participants attended the event. All presentations are available on the DPO website.

The new computerised Integrated Data Protection Office system, the "e-DPO", was also launched during the event. The e-service is available 24/7 and provides for:

i. Online registration and renewal of controllers and processors with e-payment facility,
ii. Generation of server signed registration certificates,
iii. Online search of registered controllers and processors,
iv. Online lodging of complaints, and
v. Online submission of eforms (personal data breach notification form, data protection impact assessment form, transfer of data form, certification form and compliance audit form).

The main highlights of the conference was broadcasted on MBC TV news bulletin during prime time.

c) The office submitted the list of events that were organised by the Data Protection Office for the 17th Data Protection Day to the Council of Europe. The information provided was published on the «Data Protection Day» page of the website of the Council of Europe (http://www.coe.int/dataprotection).

II. Cooperation agreement between Data Protection Office of Mauritius and Information Regulator of South Africa

On 09 March 2023, the High Commissioner, Dr P.V. Lutchmun and Adv. P. Tlakula, Chairperson of the Information Regulator of South Africa signed a Cooperation Agreement between the Data Protection Office of Mauritius and the Information Regulator of South Africa at the High Commission.

During the meeting, the High Commissioner stated that the Agreement will further consolidate the bilateral relations and cooperation that already exist between Mauritius and South Africa. The Agreement will facilitate the exchange of data and information between these two important offices.

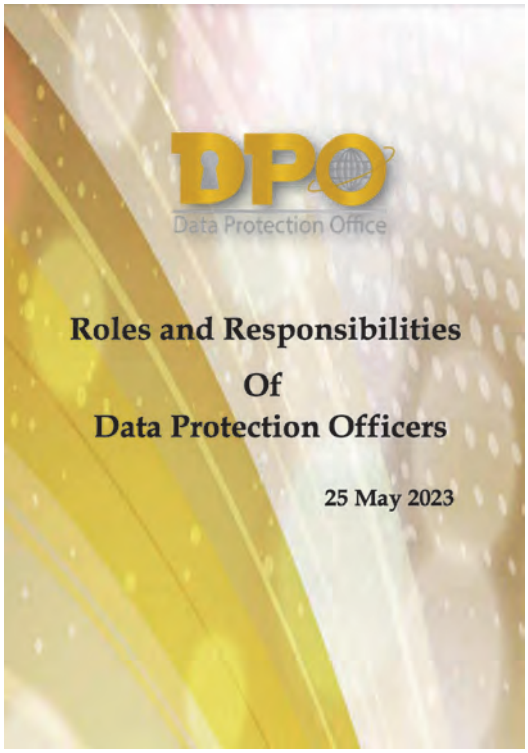
III. Networking Forum for Data Protection Officers

The National Committee on Corporate Governance (NCCG), in collaboration with DPO, hosted a half-day event on 25 May 2023 for the launch of the networking forum for data protection officers.

His Excellency, the Vice President of the Republic of Mauritius delivered the keynote address and launched the networking forum.

Around 100 participants from the public and private sectors attended the event and shared valuable insights and experience regarding this laudable initiative for the establishment of a forum for Data Protection Officers in Mauritius. The forum will assist Data Protection Officers to become an effective force and power to deliver their roles and responsibilities and to communicate freely among themselves independently from the regulator.

A factsheet titled 'Roles and responsibilities of Data Protection Officers' prepared by DPO was distributed to participants during the event.



IV. European Union Adequacy

The DPO prepared and submitted a comprehensive report in 2022, in compliance with the adequacy requirements established by the EU, for the European Commission (EC) to conduct an objective assessment of data protection in Mauritius.

In 2023, the European Commission kickstarted a series of discussion meetings with the office on thematic elements of the Data Protection Act to propose any amendments to be made to the DPA.

The following online meetings were held in 2023:

6 July 2023	Discussion for possible changes to Mauritius' data protection legislation
13 July 2023	First thematic meeting
20 July 2023	Second thematic meeting

Based on discussions with the EC, this office prepared a draft Data Protection Bill and submitted it to the European Commission for feedback. The office is now awaiting the final report from the EC.

V. Privacy Symposium Africa 2023

The Unwanted Witness is a civil society organisation based in Uganda. It was established in 2012 and works at the intersection of law, internet and human rights. It has been at the centre and forefront of advocating for digital rights especially the right to privacy.

The Privacy Symposium Africa (PSA) is a Pan African Privacy and Data Protection platform established in 2019 by Unwanted Witness to attract, present, and discuss original research results and latest technology developments related to personal data protection and privacy.

The Privacy Symposium Africa since establishment has offered innovative propositions in legal, regulatory, academic, policy and technological development in the area of privacy and data protection. The platform brings together business community, ICT experts, academics, lawyers, regulators, researchers, policy-makers, and civil society for three days of inspiring keynote addresses, thought-provoking panels, master classes and limitless high-value networking.

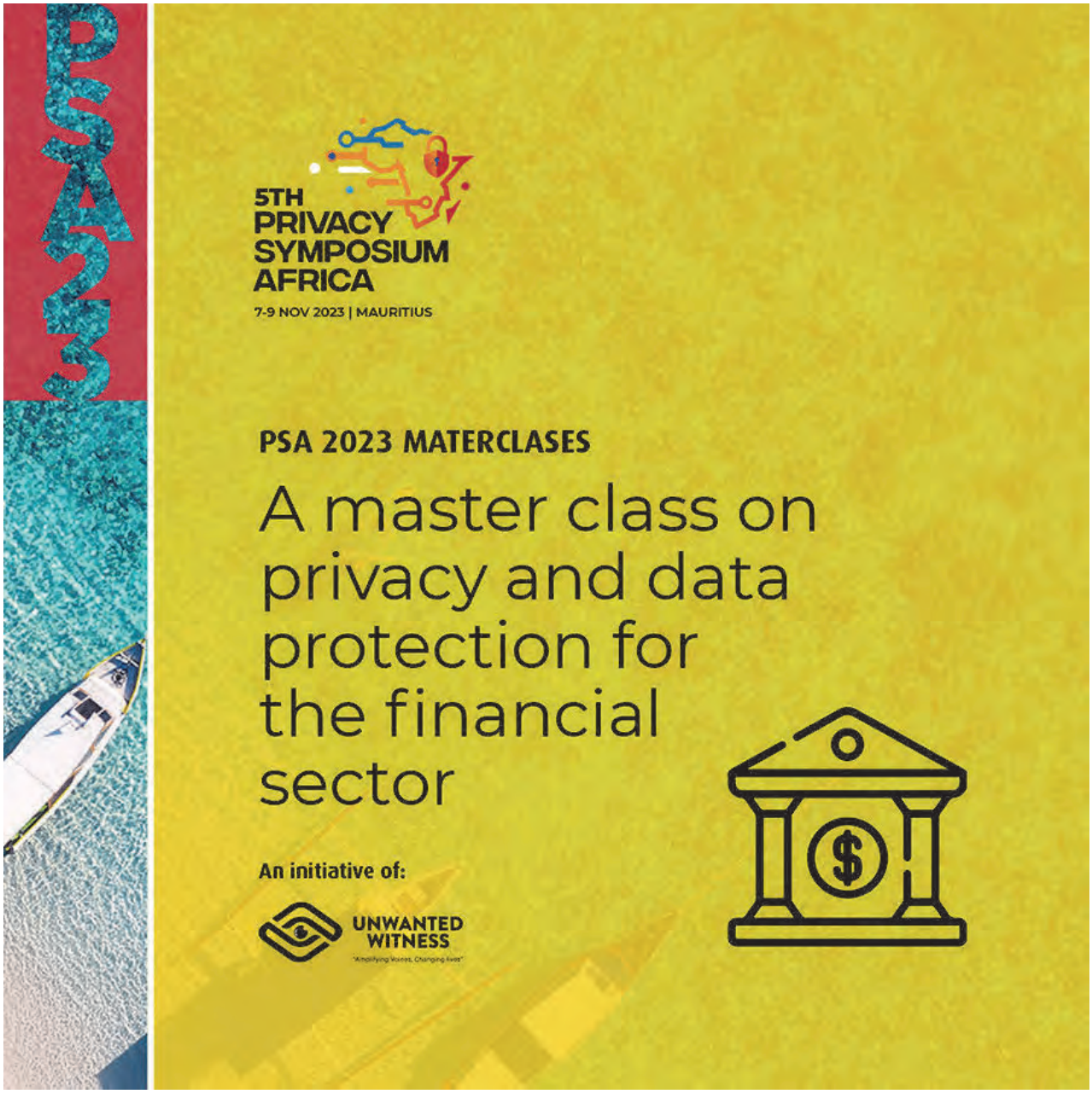
The 5th edition of Privacy Symposium Africa was held in Mauritius from 07th to 9th of November 2023 in collaboration with the Data Protection Commissioner. A mixture of virtual and physical events (hybrid) were organised. The website link to the event is available on https://privacysymposiumafrica.com/

Women in Privacy Meet-up

The Women in Privacy Meet-up was a special event organized as part of the 5th Privacy Symposium Africa, which aimed to create a platform for women working in the field of privacy to connect, share experiences, and discuss key issues affecting their work. The DPC participated as guest during the session and shed light on crucial matters impacting women in privacy.

Masterclasses

One of the key features of PSA are master classes which provide participants with in-depth training and education on various privacy-related topics. The Master Classes at the Privacy Symposium Africa are designed to provide participants with a deeper understanding of the latest developments and best practices in the field of privacy and data protection. They are led by experienced privacy professionals and experts, and provide participants with hands-on training and practical knowledge on a range of privacy-related topics. The DPC facilitated the masterclass on privacy and data protection regulations and standards applicable to the financial sector.



Privacy Scorecard

The Privacy Scorecard report gives critical information on how different collectors/processors comply with the principles and standards of data protection.

Unwanted Witness launched the Privacy Scorecard report for Uganda, Kenya and Mauritius 2023 during the 5th Privacy Symposium Africa.

VI. Benchmarking visits

(a) Ivory Coast

The DPO received a request from the Personal Data Protection Authority of Ivory Coast for a study visit with a view to improving the personal data regulation system of the Ivory Coast. The DPO of Mauritius was identified as an inspiring model of good practices in the protection of personal data in Africa.

The DPO received delegates from the Personal Data Protection Authority of Ivory Coast from 10 to 14 July 2023.

The delegation from the Ivory Coast was composed of the following members:

- Director General of the Personal Data Protection Authority, Head of delegation;
- Head of the Compliance and human rights protection;
- Head of technical department;
- Head of economy and health sector department;
- Head of the control and complaints department;
- Head of the innovation department;
- Head of State activities department.

The study visit was highly appreciated by the delegates.

(b) Seychelles

On 21 September 2023, the office received delegates from the Department of Information Technology of Seychelles comprising of :

- Principal Secretary - Department of Information Communications Technology (DICT)
- Director Policy Strategy and Research - DICT

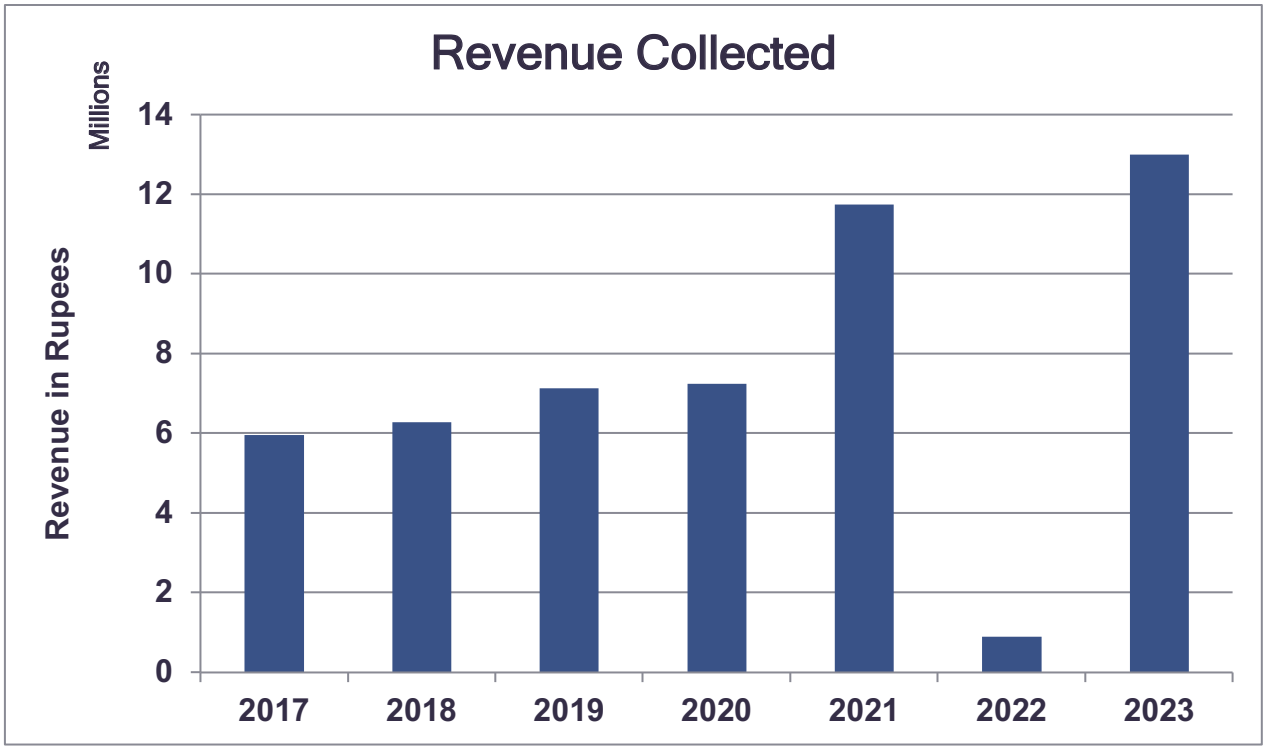
The office shared its experience on the setting up of the office, made a presentation of the Data Protection Act of Mauritius and the e-dpo system and answered questions from the delegates.

ACTIVITIES IN 2023

I. Financial Status

(a) Revenue collected

DPO collected a total revenue of Rs 12,992,600 for registration of controllers and processors in 2023.



A high revenue was collected during 2023 given that all controllers and processors renewed their first registrations.

II. International Cooperation

The Data Protection Office (DPO) is actively involved in various international privacy networks, including the 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), the Council of Europe, and the United

Nations, among others. This participation facilitates the exchange of information, the undertaking or support of specific activities, and the sharing of knowledge and best practices.

(a) International Conferences - Council of Europe (CoE)

44th Plenary meeting of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data

The Committee of Convention 108 (T-PD), held in Strasbourg from 14 to 16 June 2023, was particular fruitful where two fundamental texts that contribute to the implementation of Convention 108+ were discussed namely:-

- Guidelines on Data protection for the processing of personal data for anti-money laundering/countering financing of terrorism purposes;
- A first module of Model contractual clauses for transborder data flows of personal data, for data flows from data controller to data controller.

The Data Protection Commissioner participated in the conference which focused on the interpretation of article 11 of Convention 108+ and on Guidelines on data protection, including biometrics, within the framework of vote and elections.

(b) Participation with international organisations

i. AU Commission

An officer of the DPO participated in the Capacity Building Workshop on AU Data Policy Framework from 4-6 Jul 2023 in Adis Ababa, Ethipia.

The workshop was aimed at achieving the following key objectives:

- To enable member states from the East African Region and representative of EAC, IGAD and EACO to gain a better understanding of the AU Data Policy Framework,
- To enable participants to understand the Implementation Plan of the AU Data Policy Framework as well as the Self Capacity Assessment Tool,
- Deliberate on key follow-up actions to reinforce the use of data as a valuable asset to foster innovation and tackle development challenges across the region.

The Framework aimed at creating a common data space and a uniform data governance mechanism and framework to enable African countries to take advantage of the ever-increasing production and use of data as a strategic asset to boost the development of sustainable and inclusive digital / data driven economy and society.

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

In August 2023, the RAPDP distributed the final report on the Africa Data Governance Landscape study, conducted by Smart Africa, to African countries to engage with authorities in the region. Subsequently, online meetings were held.

iii. Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)

AFAPDP organised a session on "Les fondamentaux de la sécurité des données personnelles" for the benefit of its members. Additionally, Executive Committee elections were held, and new members joined the organisation.

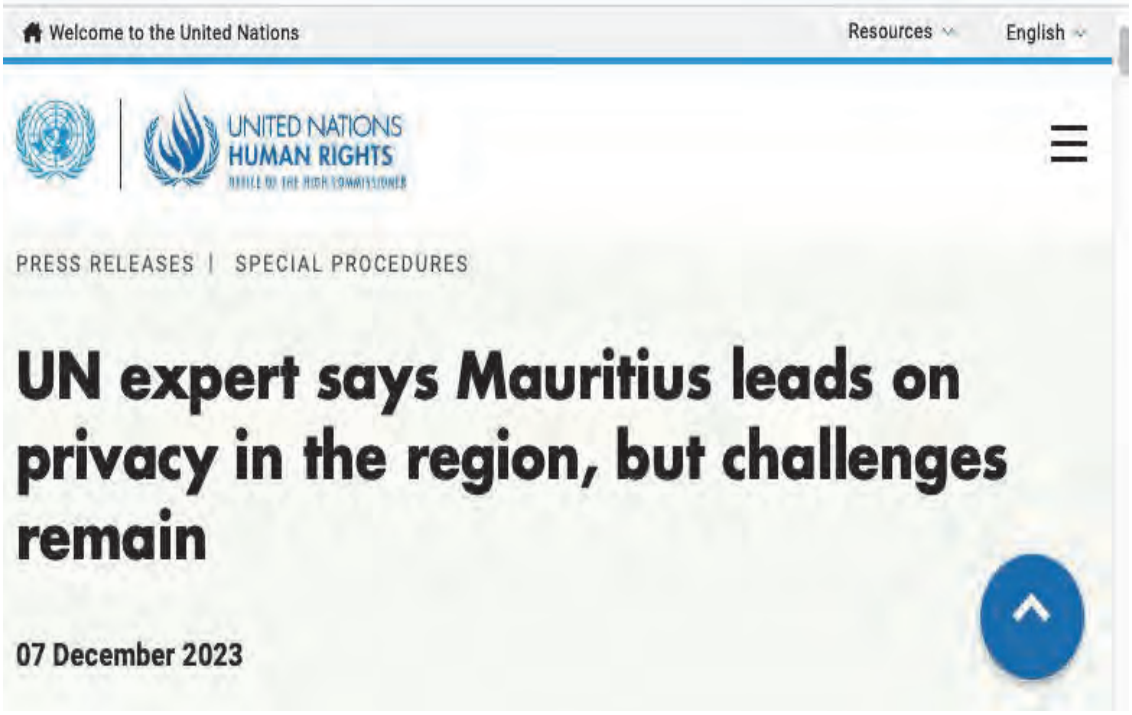
iv. Global Privacy Assembly (GPA)

The GPA is a leading global forum for data protection and privacy authorities, providing international leadership by uniting over 130 data protection and privacy authorities worldwide.

As GPA membership has become payable in 2023, request has been sent to MITCI for the DPO to become an accredited member with detailed information on the benefits of being a member for approval.

v. United Nations Special Rapporteur

A UN Special Rapporteur on the right to privacy, after an eight-day visit to the country welcomed the comprehensive legal framework to safeguard privacy and data protection in Mauritius, but warned that challenges remain in its implementation. The link is available at https://www.ohchr.org/en/press-releases/2023/12/un-expert-says-mauritius-leads-privacy-region-challenges-remain



(c) Virtual meetings

During 2023, the DPO engaged in numerous prestigious international virtual meetings, actively collaborating with the DPC. The DPC shared the Mauritius data protection experience and journey, with her interviews, presentations, and valuable insights being deeply appreciated by foreign counterparts. Officers from the Data Protection Officer's unit conducted substantial research on internationally discussed topics and assisted the DPC in preparing materials and briefs for her interviews and presentations. The office attended the following virtual meetings in 2023:

Date and Time	Subject	Organiser	Remarks
27 March 10.00	Lessons learned and challenges from Mauritian perspective	Hogan Lovells International LLP	DPC participated as panelist
3 April 14h00	Launching of Privacy Symposium Africa 2023 Roadmap- Mantle Handover Ceremony	Unwanted Witness	Speech by DPC
11 April 12h00	Discussion on possible cooperation	Privacy Laws & Business	DPC attended meeting
26 April 12h15	13th UNWDF Programme Committee Meeting 2023	UNWDF	DPC participated as high-level speaker
19 May 15h30	On line meeting Introductory discussion on Training of Data Protection Officers with an IAPP certificate	IAPP	DPC participated in meeting
27 June 10h00-12h00	Meeting of the Minds: Conference Brainstorming Session- Harnessing AI for Breakthrough Innovation	Doracrea	DPC participated

7 July **10h30**	Discussion on Module 5 of the MOOC	Centre for Human Rights University of Pretoria	DPC participated
31 July **16h00**	Online Consultative Meeting on the Responsibility Matrix - Implementation of the AU Data Policy Framework	RAPDP/AUC	Officer from Data Protection Officer's Unit attended meeting
24 October **10h30**	Discuss Module 5 of the MOOC on the right to privacy in the digital age in Africa	Centre for Human Rights, University of Pretoria	DPC participated
13th December **13h00**	60th TPD Bureau Meeting	COE	DPC attended online meeting
13th December **14h00-16h00** **18h00-21h00**	Generative AI & Data Protection in Africa Building Trust Framework for Data Transfer Across Africa.	Africal Digital Rights' Hub	DPC participated as panelist

III. Participation in surveys

In 2023, the office participated in the following surveys:

- the Global Privacy Assembly (GPA) census on Cybersecurity.
- the UNCTAD Survey on Electronic Commerce Legislation together with MITCI,

- the training needs analysis in line with paragraph 8.3 of the PRB Report 2023, conducted by MITCI for officers in the technical grades.
- the UNESCO survey relating to Data Protection and Privacy Laws in collaboration with MITCI.

Our office has also received a request from CNIL (National Data Protection Commission), which is dedicated to preserving individual freedoms amidst advances in information technology. The request pertains to a draft survey titled "Teachers' Perceptions of Personal Data Protection and Digital Citizenship". The request was forwarded to Ministry of Education, Tertiary Education, Science and Technology for consideration.

The office provided inputs related to data protection for the fifth edition of the ITU's Global Cybersecurity Index (GCIv5) to the Ministry of Information Technology, Communication and Innovation through the Computer Emergency Response Team of Mauritius (CERT-MU) who collected data to fill the questionnaire from different stakeholders.

IV. Sensitisation

One of the key functions of this office is to implement measures necessary to inform the general public about the provisions of the Data Protection Act (DPA). Throughout 2023, numerous awareness-raising activities were conducted to achieve this goal.

(a) Press Communiqués/Interviews

- **Business magazine**

The Data Protection Commissioner (DPC) participated in Business Magazine's 2023 edition of The Business Year, offering crucial insights from both business and economic perspectives. The DPC's contribution emphasized the importance of robust data protection measures in fostering consumer trust and enhancing economic stability. By highlighting the intersection of data privacy and business growth, the DPC underscored how adherence to data protection regulations can drive competitive advantage and support sustainable economic development.

DATA PROTECTION

DATA PROTECTION FROM A BUSINESS AND ECONOMIC PERSPECTIVE

BY DRUDEISHA MADHUB,
Data Protection Commissioner

AS the number of privacy laws worldwide continues to grow, businesses need to focus on privacy trends to protect users' personal information and comply with privacy regulations. Huge fines for breaching data privacy regulations are not the only reason companies must improve personal data security measures. As users' awareness about their personal data grows, handling personal data lawfully will influence users' trust in businesses and their profits. Here are the top data privacy trends and tendencies that one needs to understand in 2023, which are and will highly impact businesses worldwide including Mauritius.

Data processing has taken on a critical role with the rise of an ever-expanding digital economy. The proliferation of data in the economy presents a tremendous opportunity to boost growth through efficiency and innovation. Rights and obligations over data must be clarified for the market to function efficiently, and the way in which these are effected will impact growth and equity. Data has long been of value in economic activity. The collection of personal data has always involved a trade-off between respecting the individual's desire for privacy and reaping the commercial and social benefits that can be derived from its collection and dissemination.

Effective data policy requires an integrated perspective to balance competing objectives: promoting growth and competition through data access, ensuring incentives exist for data to be collected and processed, promoting stability by adequate investment in cybersecurity and data protection, and ensuring that individual privacy preferences are respected. Organisations and individuals increasingly generate, collect and process personal data. A strong data protection framework helps foster consumer trust and increased use of digital tools, which in turn can incentivize investment, competition and innovation in the digital economy. They seek to identify specific attributes of a data protection framework that can help policymakers and regulators build a digital economy that includes — and serves — everyone.

Privacy-driven spending on compliance with privacy laws will continue to increase in 2023. As new privacy regulations are evolving constantly, companies will invest more in privacy technologies to get the trust of users and avoid fines for breaches of personal data. Currently, advertisers and marketing agencies employ business models that rely on sharing personal information. However, this is changing fast. Privacy-enhancing technologies took the centre stage in 2022 and will continue to rise in 2023. The introduction of the General Data Protection Regulation (GDPR) in Europe in 2018 initiated the growth of data privacy regulations worldwide. Today, over 100 countries have privacy or data protection laws, and the number of countries is growing. The global rise in data privacy regulations will continue in 2023. By the end of 2024, it is expected that 75% of the global population will have its personal information covered under privacy regulations. The European privacy laws are currently the world's most powerful data protection framework.

These privacy regulations and even cookies or other tracking technologies themselves are continually evolving, which means website owners should continuously update their current privacy policies and process personal information accordingly. A cookieless future is therefore right upon us: with the increasing importance of first-party data and users' awareness of their personal data, third-party cookies are going away. Google has announced that by the end of 2023, it will officially stop supporting Third-Party Cookies on the Google Chrome browser. However, later it had to delay blocking third-party cookies until 2024 due to the full testing of technological solutions of alternatives. The trend will continue for removing cookies in favour of consent-based data-collecting solutions. With the trend towards first-party data, advertisers and marketing agencies are increasingly interested in investing in direct partnerships with brands and businesses that own the data.

In light of the above, businesses that handle the personal information of users seriously will see an increase in their active users and profits compared to their competitors. Data subjects are becoming more aware of their rights and want to protect their personal information. As individuals continue to exercise their right to know, update, delete, or otherwise handle the personal information businesses have collected about them, this will follow by a significant increase in data subject requests and complaints in 2023. Increasing and changing privacy regulations worldwide will lead to more data security jobs for people in the coming year. The increase in related jobs in recent years dispels the myth that Data Science and Artificial Intelligence has replaced human labour.

The ongoing march of AI technology across all sectors will be shaping our societies in years to come, for good or ill. Likewise, there is much prominence given to the metaverse even if most of us are not yet clear how it will operate in practice and what are its implications for people's privacy. The challenge in 2023 and beyond will be for companies and governments to act responsibly and for regulators to achieve a fair balance between encouraging the deployment of new technologies while protecting all of us from abuse, and the most vulnerable especially. While there are a number of international initiatives looking at how to meet these challenges, by far the most likely scenario is that piecemeal legislation will emerge, potentially starting with the EU's AI Act and the new kid on the block, the AI Liability Directive.

With increasing reliance on cloud and online transactions, many organisations are handling more and more data. Bad actors, outside an organization and inside of it, constantly look to compromise an organization's data security for their own ends. Data breaches often aim to steal information from a company, selling it to others, or using it to commit acts of fraud. Since organisations handle a great deal of personal identifiable information from their customers, employees, and stakeholders, a data breach can do a great deal of harm. Some of the most potentially damaging effects come from data breaches that steal especially sensitive information, such as social security numbers, driver's licenses, and passports. If a bad actor gets their hands on this information, they can do a significant amount of damage to an organisation and anyone who has given the organisation data.

Most organisations have established business ethics policies, or a code of ethics. Even those that have not, still need to follow ethical practices if they expect to stay in business for any length of time. Such ethics policies typically indicate something to the effect that confidential information will be handled responsibly, not used in business activities in ways that do harm as a result, and used only as indicated for business purposes. By implementing security controls for personal data, breaches that negatively impact data subjects can be avoided.

Our mission is attaining ever-greater importance locally, regionally and across borders. Ensuring adequate data protection is proving day by day an increasingly essential prerequisite for any respected democracy to work healthily and fundamental rights and freedoms to be made real. It is imperative that privacy protections are reinforced at all levels and that all organisations commit to achieving a level of protection of personal data that corresponds to the changes linked to rapidly evolving technologies. Getting assurances that our data is protected and safeguarded is fundamental in order to prevent new technologies from becoming a threat – turning us all into the inhabitants of an out-of-control, disquieting technological world. Being aware of the demands for national security which fathers the claim for increasingly pervasive surveillance tools, the risks that society might jeopardise its own freedom and thus, its very soul, must be balanced with the need for defending itself in cases of emergency.

Privacy has become a necessity. The protection of personal data is no "luxury" or "decorative" item one can do without. It is actually indispensable in a world where using data is a vital precondition for economic growth, indeed for the very survival of businesses. Data protection, privacy and cybersecurity breaches are on top of the agenda of corporate and national data protection oversight agencies worldwide.

As we have seen, the environment we faced at the end of 2022 is increasingly uncertain amidst geo-political tensions and economic fragility, but new approaches and ideas born of technology and innovation continue to emerge, designed to enrich and enhance the way we live and potentially help respond to the challenges we face. A number of these technologies look set to dominate 2023 and drive new legal developments in data privacy.

WHAT YOU NEED TO KNOW

The Data Protection Office published a fact sheet on legitimate interest to assist controllers and processors understand what this terminology means as per the provisions of the DPA and how it can be applied in their business operations. The fact sheet covers the following main aspects:

- Lawful processing of personal data
- Legitimate interests as a lawful criterion for processing
- Criteria of legitimate interest
- Steps to consider when performing the legitimate assessment

EXAMPLES

The fact sheet is published on the website of the office.

Number of Registered Controllers: 15337
Number of Registered Processors: 721

During the year 2022, the following were accomplished:
Complaints Resolved: 36
Personal Data Breaches Processed: 22
Authorisations for Personal Data Transfers outside Mauritius: 72
Data Protection Impact Assessments processed: 3

- **Eclairage economiques – MBC**

  The DPC was interviewed on the MBC which was broadcasted on 31 March 2023 on the topic "Fintech from a Data Protection perspective" in the programme eclairage economique .

- **Collaboration with MCB Consulting Services Ltd for publication on Artificial Intelligence**

  The DPO submitted inputs for an article on the above subject. The DPC warns about the risks of adopting AI without proper understanding and control.

THOUGHT LEADERSHIP PAPER ON AI

AI: a future-proof force or undermining power

Exploring the flip side of this new technology, the Data Protection Commissioner for the Mauritian jurisdiction issues a stark warning about adopting and using AI without fully understanding and managing its myriad risks, or controlling its parameters.

Emerging digital technologies and services including Artificial Intelligence (AI) creates an unprecedented promise to the world with limitless benefits in terms of enhanced efficiency, accuracy and timeliness. But just like the saying that everything that glitters is not gold, the simulation of human intelligence towards virtual intelligence also brings along human weaknesses and risks in its path.

For instance, AI presents significant challenges and concerns in the realm of privacy and data protection.

"AI is not just about technology but delves into fundamental and interdisciplinary human rights and freedoms."

Not only does AI force us to better understand its impact on human rights and fundamental freedoms, but it also entails in-depth reflection on who is responsible for its harmful consequences.

"The foundational principles of any AI system should rely on transparency, fairness and accountability".

This will ensure that processing operations are not opaque to individuals and that they are informed of the identity of the AI institutions processing their data as well as how their data is used, decisions that are made on this basis and the logic behind those decisions to prevent any unfair bias against them. AI institutions must establish the provenance of data and ensure the quality and relevance of the data enteredinto the algorithms.

Additionally, adopting a risk-based approach to AI is of paramount importance. Robust data security measures and the use of pseudonymisation and anonymisation techniques should be advocated to prevent personal data from being easily linked to specific individuals. Since AI systems process huge amounts of data, they are often the target of cyber threats. Therefore, deploying the necessary organisational and technical measures will prevent data control from falling into the wrong hands. Regular audits and assessments are also necessary to identify and mitigate data privacy and security issues. Privacy design should be embedded at the heart of technology development.

The essence of all technological developments, including AI, should be based on user consent and control. Users should have the right to understand and control how their data is used in AI systems. This perspective strengthens the idea that individuals should be active participants in the data-driven AI ecosystem. The caution line in this environment is: "If it is not you who control the parameters of your data, then it's someone else controlling you!"

The rapid development of AI, especially in the case of OpenAI ChatGPT, has transformed the current business landscape. Businesses leverage ChatGPT for a variety of purposes, including automating customer service, improving business intelligence, and facilitating strategic decision-making. However, the adoption of ChatGPT is not universal. Some countries have even banned its use. This situation highlights a paradox: while AI has the potential to drive innovation by automating many digital tasks, it is also seen as a potential threat that requires regulation.

The European Union introduced a groundbreaking initiative by the formulation of the EU AI Act and paved the way for comprehensive AI regulation. The European Parliament passed the EU AI Act on 14 June 2023. It is the first legislation of its kind in the world, which regulates the use of AI in Europe, respects the values and rules, and harnesses the potential of AI for industry. The gist of the AI Act is a classification system that determines the level of risk an AI technology could pose to the health and safety or fundamental rights of a person. The framework incorporates four risk tiers: unacceptable, high, limited and minimal.

Our Mauritius Data Protection Act 2017 (DPA) caters for strong and robust principles applicable in the AI sphere, covering amongst others:

SECTIONS

21	Principles relating to processing of personal data	38	Automated individual decision making
22	Duties of controller	23	Collection of personal data
25	Notification of personal data breach	27	Duty to destroy personal data
28	Lawful processing	29	Special categories of personal data
31	Security of processing	34	Data protection impact assessment
37	Right of access	39	Rectification, erasure or restriction of processing
40	Right to object		

Setting up the right data governance, legal and ethical framework is crucial to contain the risks associated with AI. This requires a multi-faceted approach to AI, including robust data governance, privacy-preserving AI techniques, responsible AI development practices, transparency in AI decision-making, and adherence to relevant legal and ethical frameworks. AI organisations and policymakers need to collaborate to strike a balance between harnessing the potential of AI and safeguarding individuals' rights and interests regarding their data.

The dangers of AI, as identified by AI itself

We have queried BARD, the generative AI tool of Google, to depict the data protection risks arising from AI, and below is the outcome:
AI systems can be used to collect and process personal data on a massive scale. This data can be used to track individuals' movements, habits, and preferences. It can also be used to build profiles of individuals that can be used for marketing or other purposes.
Another concern is that AI systems can be used to make decisions that have a significant impact on individuals' lives. For example, AI systems can be used to make hiring decisions, loan decisions, or even medical decisions. If these decisions are based on biased or inaccurate data, it can have a negative impact on individuals.
Finally, AI systems can be hacked or manipulated, which could lead to the unauthorized access or disclosure of personal data. This could have a devastating impact on individuals, as it could lead to identity theft, financial loss, or even physical harm.
To address these concerns, it is important to develop strong data protection regulations for AI systems. These regulations should ensure that AI systems are only used in a lawful and ethical manner. They should also protect individuals' privacy and ensure that their personal data is not used without their consent.

Conclusion

As leaders in integrating AI within the banking and non-banking sectors, we recognise the limitless opportunities that this technological marvel presents. Our partners, including Temenos, are setting benchmarks for innovation in the field, utilizing AI to redefine traditional practices. But what does this mean for you? It marks the beginning of a new era, an era where the consultant is no longer confined by traditional boundaries but empowered by AI to provide direct and impactful solutions. Join us as we explore this thrilling future, where we are committed to leading this exciting evolution, providing services that resonate with the demands of the modern world, and ensuring that your business stays ahead in this competitive landscape.
The dawn of this new era in consulting is upon us, an era that MCB Consulting is not merely observing but actively leading. This is a time of transformation, where the traditional role of the consultant is being reimagined and enhanced by the power of Artificial Intelligence.

(b) Circular to ministries and departments on their obligations for registration/renewal and designation of data protection officer.

Circulars were issued to Ministries and Departments through MITCI to assist them in complying with their registration requirements and the designation of a data protection officer.

(c) Raising awareness with businesses

- **Ascentrix - Data Privacy Day**

  The DPC participated at the Data Protection Conference 2023, held on January 26th in celebration of Data Privacy Day. She discussed various aspects of data privacy and protection, providing insights on what to expect in 2023 and beyond.

- **Mauritius Finance**

  The DPC participated as keynote speaker in the Mauritius Finance workshop on the theme ”Privacy Trends in 2023 in Mauritius and internationally”

- **BDO IT Consulting Ltd - Annual Compliance Conference**

  The DPC participated as a panelist in the 2nd Annual Compliance Conference organized by BDO Consulting which was held on Wednesday, 31st May 2023 at The Ravenala Hotel, Balaclava. She delivered a speech on "Protecting Personal Data in a Digital Age - The role of businesses, governments and data subjects".

- **MCB Consulting**

  The DPC participated in the forum titled "Comment Intégrer Les Avancées Technologiques pour Améliorer l'Efficacité et la Portée des Services Bancaires" from a data protection viewpoint in October 2023.

- **Innovationmauritius.com Conference**

  The DPC made two presentations on the following subjects:- "Metaverse" and " Ethical and Compliance concerns of AI" from a data protection perspective in October 2023 at Caudan Arts Center.

(d) Training

Two officers of the DPO conducted a training at the Mauritius Revenue Authority (MRA) on 29th March 2023 to sensitise officers of the MRA.The DPC intervened online for question and answers.

(e) Mauritius Investment Climate Statement

In 2023, the Data Protection Office provided updates for the Investment Climate Statement (ICS) 2023 for Mauritius to the U.S. Embassy to Mauritius and Seychelles.

(f) Distribution of Data Protection Training Toolkit DVDs

The DPO has distributed approximately 2182 DVDs in 2023 to registered controllers/processors to assist them understanding and complying with the provisions of the DPA.

Enforcing Data Protection

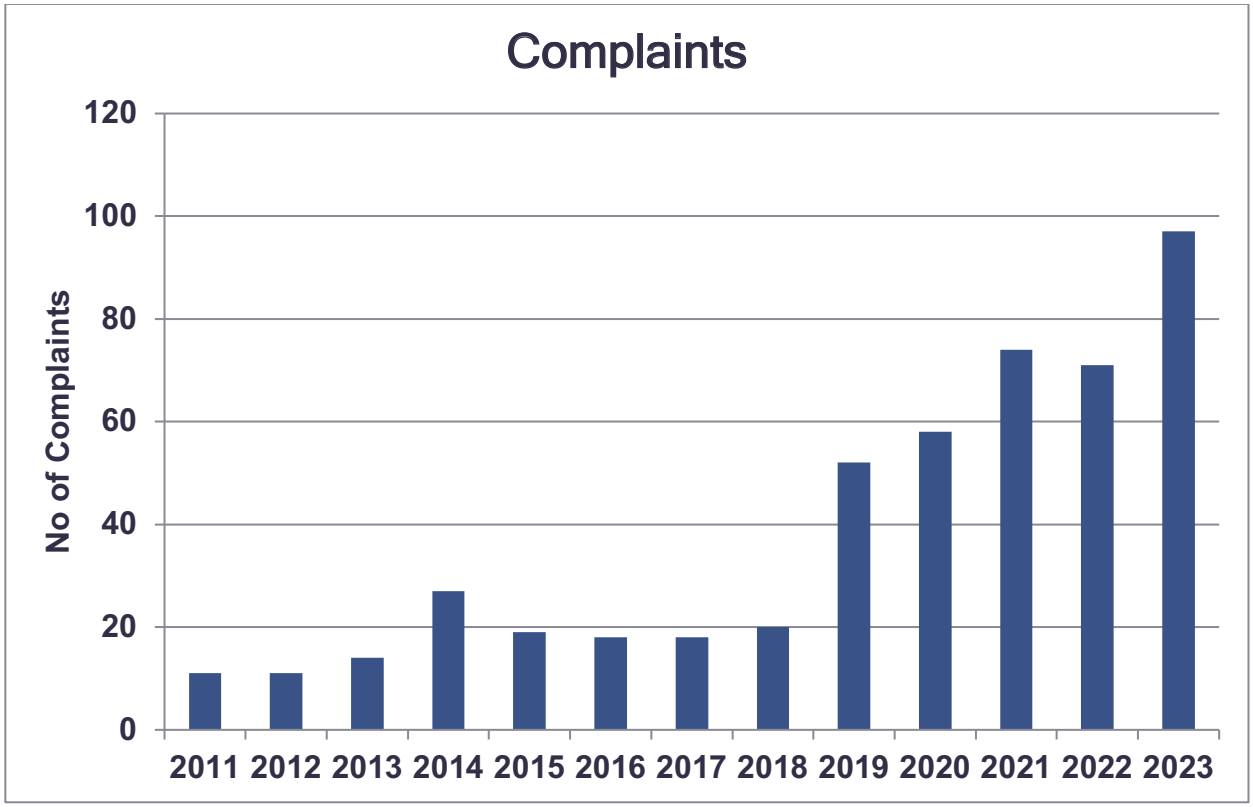
The Data Protection Office (DPO), in collaboration with the police, has effectively conducted numerous inquiries, leading to the successful resolution of many complaints. This partnership has proven to be highly productive, combining the investigative expertise and resources of both entities to address and resolve issues efficiently. By working together, the DPO and the police have enhanced their capability to uphold data protection laws, ensuring that complaints are thoroughly examined and resolved.

(a) Investigation on Complaints

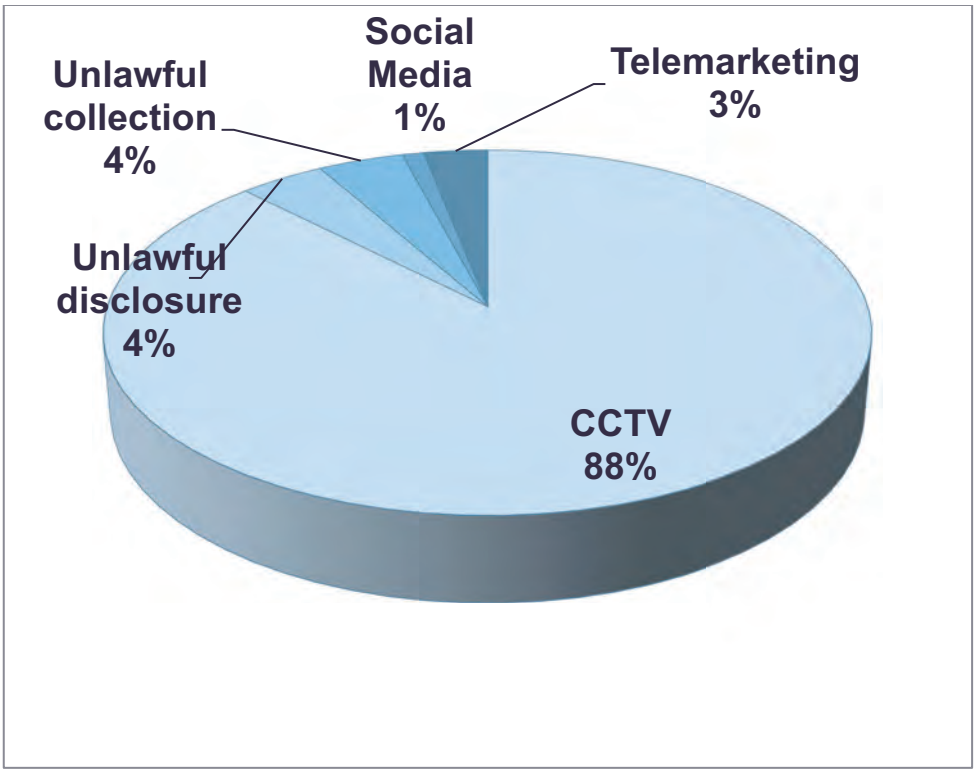
During the period January to December 2023, the DPO received ninety seven (97) new complaints regarding investigations on the below subjects, among others:

- Unauthorised use of CCTV camera
- Unlawful processing of personal data
- Rights of access
- Telemarketing

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



The different categories of complaints are 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.

(b) Complaints Closed

The office closed **forty two (42)** complaints in 2023. **Five (5)** of the cases were resolved through amicable resolution.

VI. Improving Legal Protection

To reinforce its enforcement actions, the Data Protection Office (DPO) has been involved in various court cases.

(a) Supreme Court Cases

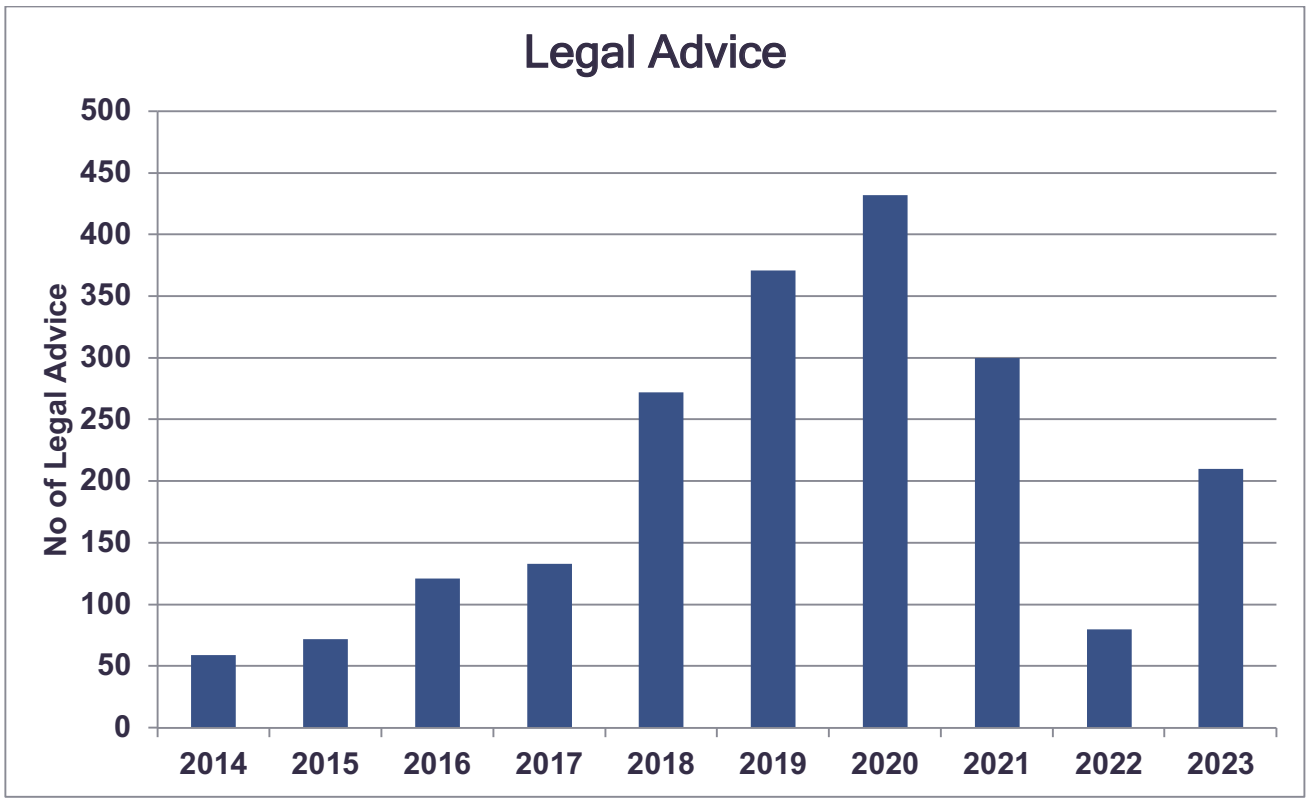
The DPO was represented by the State Law Office in two cases at the Supreme Court, where the latter was a co-defendent and a third party. One case has been set aside and DPO has been put out of cause. The other case was fixed for filing in November 2023.

VII. Registration of Controllers and Processors

Under the Data Protection (Fees) Regulations 2020, the cumulative number of registered controllers and processors as at 31 December 2023 reached 18303 and 997 respectively. 11415 registration certificates were issued in 2023. The office has also attended a voluminous amount of phone calls and emails in assisting the registration/renewal of controllers and processors.

VIII. Requests for Legal Advice

In 2023, the office received around **two hundred and ten (210)** written requests for legal advice on the interpretation of the DPA.

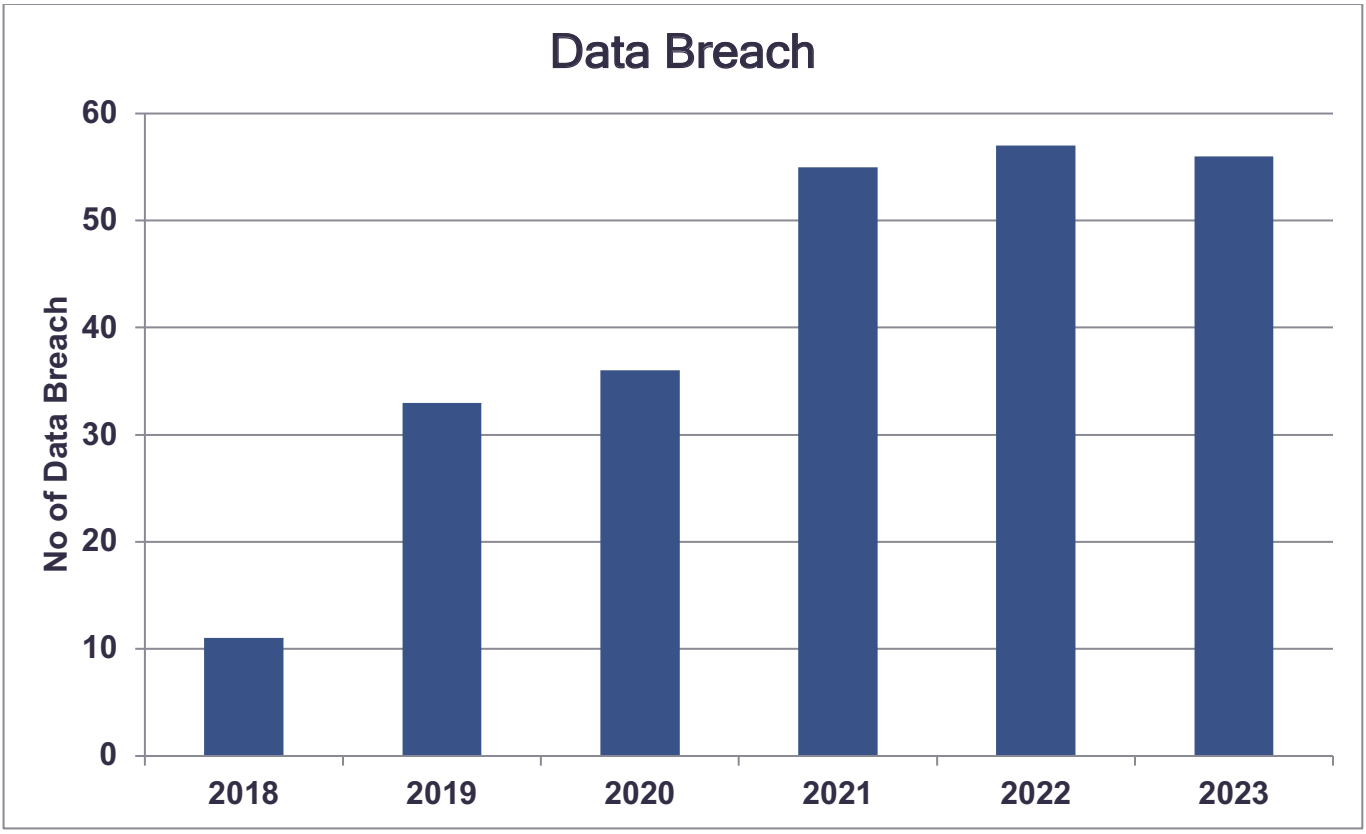


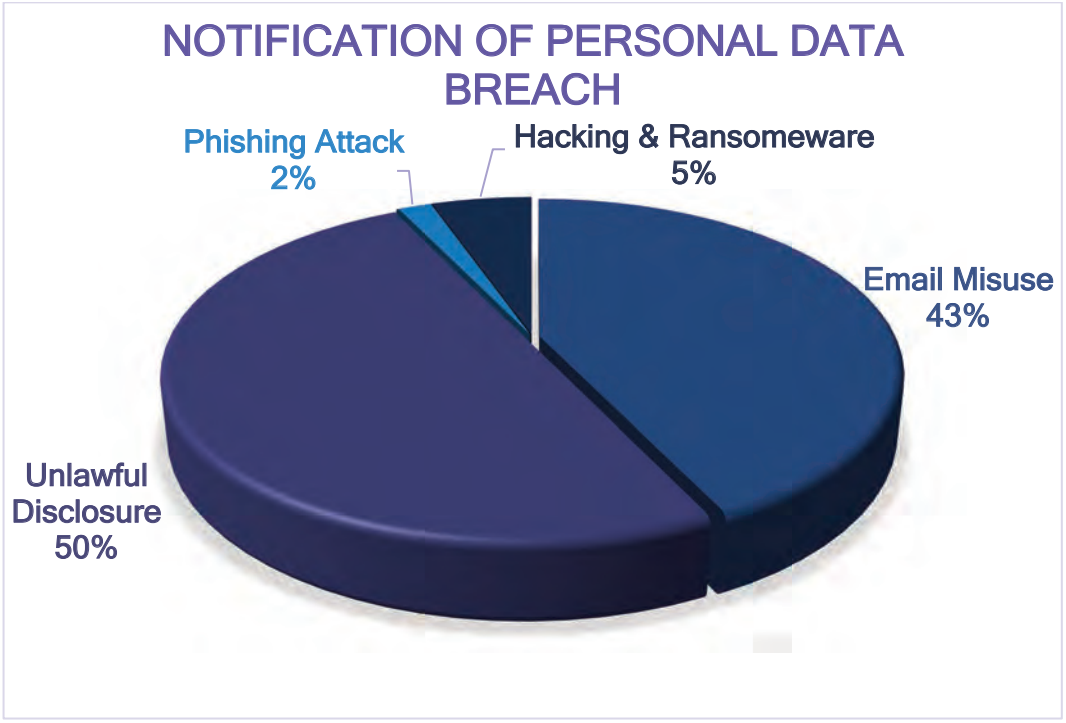
IX. Advisory /Stakeholder Role in Projects

DPO is a stakeholder in projects which involve the processing of personal data. In 2023, the office has provided recommendations on many projects from both the public and private sectors.

X. Personal Data Breach Notifications

In 2023, fifty six (56) personal data breaches have been reported to this office. Those organisations were advised to implement recommendations within a period of three months.



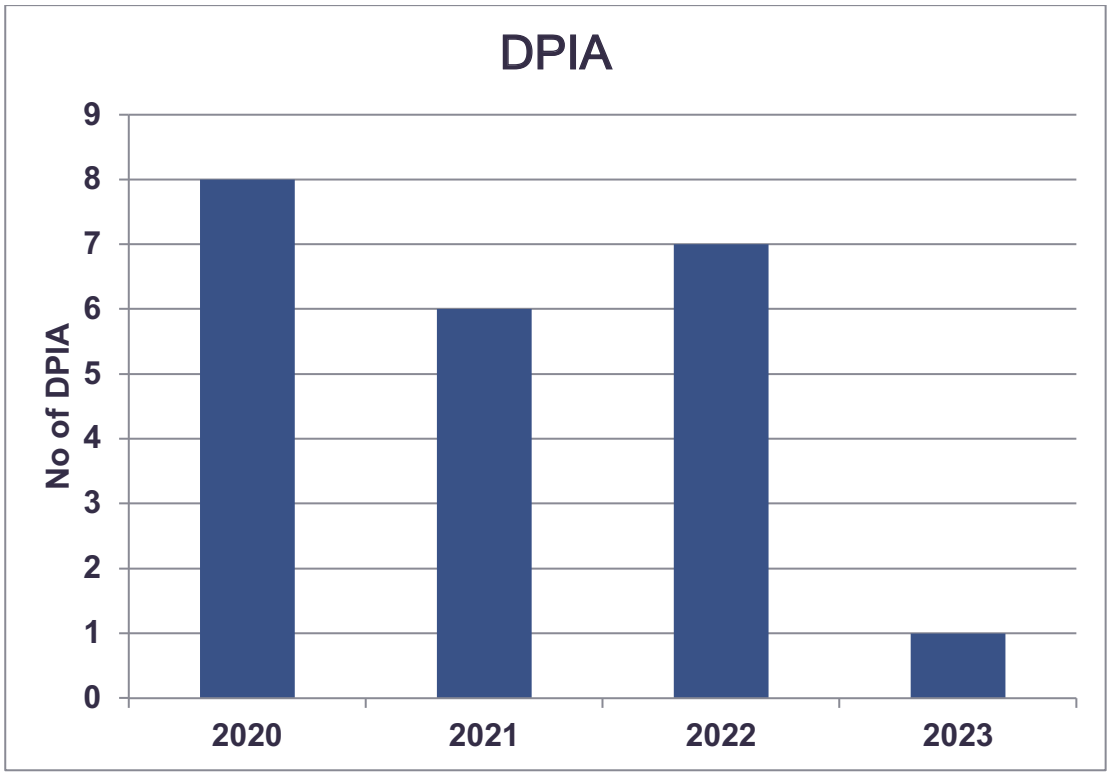


XI. Data Protection Impact Assessments

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 2023, the office has received **one(1)** data protection impact assessment submitted by an organisation.



XII. Transfers of Personal Data Abroad

The DPC authorised **ninety three (93)** requests for transfer of personal data outside Mauritius with proof of appropriate safeguards under section 36 of the DPA. 4 applications for transfers were rejected due to insufficient safeguards mentioned on the forms.

XIII. Certification

The Data Protection Office issues certifications 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 required 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.

The process of certification is lengthy and complex and requires expert human resources at the office. For instance, the certification for ABSA took around 1 and a half year. All applications are treated in strict confidentiality under section 49 of the DPA.

The office has received a total of 7 applications for certifications, out of which 1 has been completed as mentioned above and the rest are ongoing as per the table: -

Applicant	Date of Application	Status	Date of issue of certificate
A	09 April 2021	completed	30 September 2022
B	22.03.2022	ongoing	-
C	22.02.2022	ongoing	-
D	22.02.2022	ongoing	-
E	22.02.2022	ongoing	-
F	22.02.2022	ongoing	-
G	24.04.2023	ongoing	-

The complexity of certification arises from its comprehensive scope and the need for interdisciplinary expertise in legal, information technology, technical knowledge and assessments and understanding the business contexts of an organization's operations. The function has been impeded by the prolonged absence of legal and technical officers, which has affected the office's ability to perform this function according to the required standards and timeframe.

RISK MANAGEMENT FRAMEWORK

Risk management is a fundamental element of corporate governance. Risk is associated with possible events which, should they occur, could prevent the Ministry from fulfilling its mission, meeting its commitments and achieving its objectives. Risks may adversely affect the Ministry's strategy, people, assets, environment or reputation.

The Risk Management Framework provides the foundation and organisational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Ministry. The Framework applies to the Ministry, including all its units, sections and departments.

The Data Protection Office submitted inputs to its parent Ministry:

a) By describing the objectives and activities of DPO.
b) For each business objective, the office identified the key risks that would impede the achievement of the respective business objectives.
c) The office carried out a risk analysis and evaluation exercise to prioritise the most important risks in a risk assessment table and
d) It identified key risks that would have a significant impact on the business objectives, categorised as medium or high, in the Risk Register.

CAPACITY BUILDING

In 2023, officers of the DPO attended the following capacity building sessions:

Title	Date	Organised by
Induction Course for newly recruited Management Support Officers	02, 06, 08, 12 & 14 June 2023	Civil Service College Mauritius
Training Programme for Assistant Financial Operations Officer	23 & 24 October 2023	Ministry of Finance, Economic Planning and Development
Training Programme for Support Staff	10, 12, 14 April 2023	Civil Service College Mauritius
Training Course on First Aid	07to 11 August 2023, & 14 August 2023	Civil Service College Mauritius
Training Programme for Middle Management	29 & 31 March 2023 04 & 06 April 2023	Civil Service College Mauritius
Training on Wordpress	28 March 2023 to 03 April 2023	Central Information System Division
Training Programme for Workmen's Group	21 & 23 February 06 & 08 March	Civil Service College Mauritius
Awareness session on "Occupational Hazard and Risk Assessment"	10 May 2023	Ministry of Information, Technology, Communication and Innovation.

PROJECTS IN THE PIPELINE

I. Guide - Data Protection in The Mauritian Financial sector

The DPO is working on a guide titled "Data Protection in The Mauritian Financial sector" with key stakeholders in the financial sector which would delve into the critical importance of data protection in the financial sector amidst data breaches and cyber threats having consequences which can be financially devastating and reputationally catastrophic. This guide would impart knowledge, best practices, and insights on data protection for institutions (public and private) in the financial sector.

II. Workshop for Youth sensitisation

The DPO has planned to organise a workshop in 2024 to sensitise the Youth.

III. eDPO system enhancement.

The eDPO IT system, implemented in December 2022, requires enhancements based on user feedback and additional requirements that cropped up. Users have highlighted the need for new functionalities including new modes of payment such as point of sale and instant payment system. These enhancements are crucial to ensure the system meets the evolving needs of users and provides a more efficient and user-friendly experience.

RECOMMENDATIONS

1. To enhance the effectiveness of services delivered by the DPO, it is essential to provide the necessary human resources. The HR baseline should include technical and legal expertise to align with DPA functions, covering areas such as policy advice, compliance audits, data protection impact assessments, certification, personal data breaches, and investigations. Key recommendations for additional staff include:
   (a) the urgent filling of advertised posts for Data Protection Officer/Senior Data Protection Officer, Assistant Data Protection Officer and Legal Executive to improve service delivery and boost the morale of existing skeleton staff.
   (b) fund the posts of Deputy Data Protection Commissioner to assist the Data Protection Commissioner, one additional Principal Data Protection Officer, additional Data Protection Officer/Senior Data Protection Officers and Legal Executive as requested by this office to the Ministry for the right sizing of the DPO.

2. It is recommended that all Ministries and Departments designate a Data Protection Officer (DPO) to address compliance issues related to personal data processing. Unlike private organisations, which are already advanced in this area, public sector entities must catch up to ensure robust data protection practices and compliance with legal standards. Designating a DPO will help Ministries and Departments effectively manage data protection policies, conduct compliance audits, handle data breaches, and align with best practices, thereby safeguarding citizens' personal information and enhancing public trust.

Email: dpo@govmu.org
Website: http://dataprotection.govmu.org
Tel: 4600251 Fax: 4897346
Address: 5th Floor, Sicom Tower, Wall Street, Ebene

Designed and Printed by The Government Printing Department-2024