Data Protection Office

ANNUAL REPORT

JANUARY TO DECEMBER 2019

11th Edition

Tel: 460 0251 **Fax:** 489 7341
Address: 5th floor, Sicom Tower, Wall Street, Ebene
Email: dpo@govmu.org
Website: http://dataprotection.govmu.org

ANNUAL REPORT

JANUARY TO DECEMBER 2019

TABLE OF CONTENTS

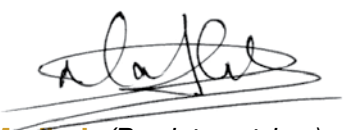
FOREWORD

Year 2019 has shown that this office has reached a stage where, despite all its endeavours to achieve resources and better work conditions for the skeleton personnel provided to it, it has not been able to progress in these spheres at the level required given that support from the relevant authorities did not materialise as expected.

For instance, a constant depletion of its human resources has become a common feature in the office given that more promising career paths with higher salaries are being offered to its personnel. The absence of any tangible improvement in current working conditions has become a high demotivating factor which is seriously impacting on the credibility of this office as a viable institution. The phenomenal increase in workload given the new responsibilities attributed to the office under the new DPA 2017 has substantially added to the complexities of handling an already weakened office structure.

International cooperation, one of the key legal functions of the Commissioner, has also been seriously undermined given that approvals, even at no cost to government, of missions of high importance, are not being entertained by the parent ministry.

Until these anomalies are not addressed and remedied, the office will continue to face difficult challenges which cannot be overcome and will thus lead to a situation of no return. After 13 years of existence, it is indeed high time for a reconsideration of the priorities of this office for it to function like any other respected public institution.



Mrs Drudeisha Madhub *(Barrister-at-law)*
Data Protection Commissioner

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.

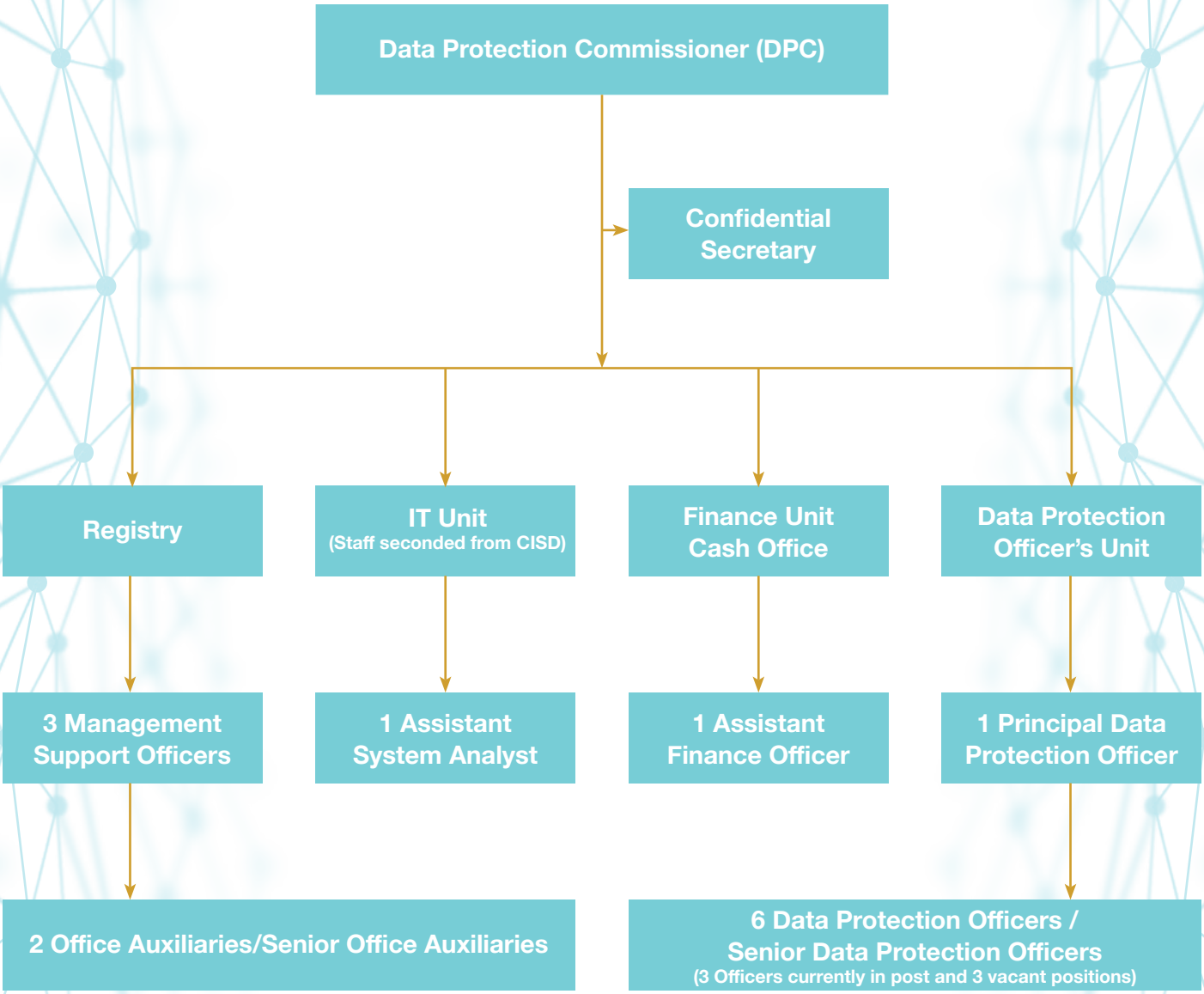
DATA PROTECTION OFFICE (DPO)

The Data Protection Office (DPO) became operational since 16 February 2009 when the Data Protection Act 2004 came into force. On 15 January 2018, the Data Protection Act 2017(DPA) replaced the Data Protection 2004. The new Data Protection Act 2017 (DPA) strengthens the control and personal autonomy of individuals over their personal data and complies with the requirements contained in the European Union General Data Protection Regulation (GDPR) which came into force on 25 May 2018. Mauritius has thus cemented its position in Africa at the forefront of technological innovation and protection of personal data.

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

Ensure compliance with the DPA and any regulations made under it;	Issue or approve such codes of practice or guidelines for the purposes of the DPA;
Maintain a register of controllers and processors;	Exercise control on all data processing operations, either of its own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with the DPA;
Promote self-regulation among controllers and processors;	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;
Take such measures as may be necessary to bring the provisions of the DPA to the knowledge of the general public;	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;
Examine any proposal for automated decision making or data linkage that may involve an interference with, or may otherwise have an adverse effect, on the privacy of individuals and ensure that any adverse effect of the proposal on the privacy of individuals is minimised;	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.

ORGANISATION STRUCTURE



BUDGET FINANCIAL YEAR 2019 - 2020

1. Human Resource Requirements

Our last annual report 2018 showed how this office struggled to meet service delivery due to a severe shortage of human resources. In 2019, the situation worsened since our workforce was reduced by two for better career options.

The DPO, being an enforcement body, has a huge responsibility to deal with non-compliance issues and try offences before the Intermediate Court. It is thus imperative to have police officers of appropriate grades posted at the office to deal with non-complying controllers and processors, to swear an information in respect of an offence under the Act or any regulations made under it before a Magistrate, to investigate and prosecute a case and assist in search of premises in the conduct of investigations and effecting notices and warrants.

Regarding the setting up of a prosecution unit at this office to ensure effective justice being provided to our citizens for offences committed under the DPA, discussion is still ongoing with the Commissioner of Police for the posting of police officers. During a previous meeting with representatives from the Police Department, questions arose about allowances, salaries and working conditions of these police officers. On her part, the DPC has earmarked office space to accommodate 5 police officers, namely 2-3 investigators and 2 prosecutors.

The DPC is still the only legal person and in charge of the administration of the office. Our proposal to have one Deputy Data Protection Commissioner (Legal) and one Deputy Data Protection Commissioner (IT) to assist the DPC in her daily tasks was not fulfilled in 2019.

However, concerning the posts of legal executive, assistant data protection officer and data protection officer/senior data protection officer which have been advertised on the public service commission's website since 26 September 2019 and 06 January 2020 respectively, they have not been filled yet.

Concerning the EU Adequacy process, this office has earmarked funds for retaining the services of a consultant to assess the adequacy of level of data protection of Mauritius with European Union Standards.

This office prepared a case for the restructuring of the DPO for appropriate and adequate human resources to be provided in order to carry out its functions and operations effectively. The restructuring plan was submitted to the Ministry of Finance and Economic Development and our parent Ministry. It is important to highlight that having adequate personnel is one of the essential requirements to be fulfilled to achieve EU adequacy.

We hope that 2020 will be the year where changes will be brought and our demands will be considered and granted.

ACTIVITIES IN 2019

1. Financial Status

I. Revenue Collected

During the year 2019, the DPO has collected a total revenue of Rs 7,127,550.

II. Audit observations for the year ended 30 June 2019

In February 2019, the Director of Audit sent audit observations for the accounts and records of the Ministry of Technology, Communication and Innovation (MTCI) for the financial year ending 30 June 2018 which included observations for the DPO. This office submitted its comments on the observations made for the DPO to our parent Ministry.

2. International Cooperation

I. Participation in International Conferences

The DPO is recognised on the international front as an effective regulator along with other privacy and data protection authorities around the globe. The DPC is often invited by international organisations to share her knowledge and expertise in the field of data protection enforcement and human rights. During 2019, the DPC participated in the following international conferences as expert:

Period	Event
13 – 14 June 2019	38th Plenary meeting of the Committee of Convention 108, Strasbourg
18 – 19 June 2019	The 5th Annual meeting of the ID4Africa Movement, Johannesburg, South Africa

II. Membership and cooperation with international organisations

The DPO participates actively in international privacy networks namely, 'Association Francophone des Autorités de Protection des Données Personelles' (AFAPDP), Réseau Africain des Autorités de Protection des Données Personelles (RAAPDP), Global Privacy Enforcement Network (GPEN), Common Thread Network (CTN), Council of Europe and the United Nations. Such participation enables this office to establish a dialogue with enforcement authorities, exchange information, undertake or support specific activities and sharing of enforcement knowledge as well as expertise along with best practices. As such, this promotes our country's democratic reputation and disseminates our commitment for the development of a sustainable global privacy framework, in line with the functions of the Commissioner as laid down in the Data Protection Act 2017. However, it is becoming increasingly difficult for this office to attend these important forums of discussion given that approvals to participate which are at no cost to Government are often not provided for reasons unknown to this office and to organisations which solicit our expertise.

(a) Council of Europe

The DPO contributed to the drafting of an article, which was published on the Council of Europe website on the occasion of the 13th International Data Protection Day.

(b) Commission Nationale de l'Informatique et des Libertés (CNIL France)

The DPO participated in the survey on the state of play of legal frameworks in relation to applicable children's rights during 2019.

(c) UN

The DPC participated in a video conference on 17 December 2019 to share the Mauritian AI Strategy with other African economies. The DPC's presentation focussed on the overall strategy, ethics and data protection in the context of AI.

(d) GPEN/CTN

The DPO is a member of the Global Privacy Enforcement Network (GPEN) as well as the liaison authority for the Common Thread Network (CTN), which is a data protection and privacy working group regrouping all Commonwealth countries. GPEN was established to foster cross border cooperation among privacy authorities. The DPC, as the GPEN liaison officer, is responsible for GPEN engagement in the Common Thread Network. As an expert in data protection and human rights, the DPC is often called to attend conferences and calls organised by GPEN and CTN.

3. National Engagement

I. Sensitisation

One of the main functions of this office is to take such measures as may be necessary to bring the provisions of the Data Protection Act to the knowledge of the general public.

(a) Data Protection Day

Each year on 28 January throughout the world, the Data Protection Day is celebrated. This day aims to raise public awareness of good data protection practices, informing people about their rights and how to implement them. The Honorable Yogida Sawmynaden, Minister of Technology, Communication and Innovation delivered a message to mauritian citizens on MBC 1 on privacy.

- **Business Connect – A Mauritius Broadcasting Corporation (MBC) Programme**

  On the same occasion, the MBC interviewed the DPC on compliance worldwide. The programme can be viewed on youtube at the following URL: https://www.youtube.com/watch?v=-GRKpf_jNFk

(b) Presentations / Speeches at Controllers' Sites

As part of its engagement in raising privacy and data protection awareness, this office delivers regular presentations; some are made at the request of controllers to provide training to their staff, others at the request of associations or organisations. In 2019, this office conducted the following off-site trainings:

Title	Presented By	Date	Audience
An Overview of the Data Protection Act 2017	Data Protection Officer/ Senior Data Protection Officer	24th July 2019	Candidates under the Compliance Competency Programme – Ministry of Financial Services and Good Governance
Workshop on DATA PROTECTION	Data Protection Commissioner	15th May 2019	Mauritius Police Force
Data Protection and Cybersecurity	Data Protection Commissioner	12th April 2019	Mobius Computing & BakerTilly
Data Collection, Types, Accuracy, Processing, Use & Security	Data Protection Officer/ Senior Data Protection Officers	11th April 2019	Local Government Services Commission
Managing Digital Information	Data Protection Officer/ Senior Data Protection Officers	11th April 2019	Local Government Services Commission

In addition, through the in-house training initiative put into place since 2018, this office provided training to Data Protection Officers to help them implement the new Data Protection Act in their respective organisations.

Title	Presented By	Date	Audience
An Overview of the Data Protection Act 2017	Data Protection Officer/Senior Data Protection Officers	14th November 2019	Participants from the Public, Parastatals and Private Sector
An Overview of the Data Protection Act 2017	Data Protection Officer/Senior Data Protection Officer	8th October 2019	Members of the Audit Forum
An Overview of the Data Protection Act 2017	Data Protection Officer/Senior Data Protection Officers	7th March 2019	Participants from the Public, Parastatals and Private Sector

(c) Sensitisation of government entities

The DPO issued a circular to all Ministries on the designation of a Data Protection Officer in government departments/Ministries for compliance with the Data Protection Act 2017.

(d) Articles in Press/Magazine and Interviews

- **Radio Plus – 'Au Coeur de l'Info'**

  The DPC was interviewed by journalists of Radio Plus regarding the national security certificate issued by the Prime Minister under the Safe City project.

- **Le DéfiPlus**

  The DPO provided its views on the publication of children's photos and on loyalty cards. The articles were published in the DéfiPlus's editions 29 June to 25 July and 21 to 27 September 2019 respectively.

RÉSEAUX SOCIAUX

Publication des photos d'enfants : attention gêne et danger !

Poster des photos d'enfants sur les réseaux sociaux est une pratique courantes. Pourtant cela peut s'avérer dangereux et devenir gênant à l'adolescence et l'âge adulte. Que dit la loi ? Quelles précautions prendre ? Éléments de réponses.

PATRICE DONZELOT
patrice@defimedia.info

Lorsqu'on est parent et qu'on est actif sur les réseaux sociaux, il est tentant de publier des photos de nos bambins sur Facebook ou Instagram, entre autres. Pourtant, ce qui peut paraître anodin aux yeux des parents, peut devenir un calvaire pour les enfants. En effet, imaginez qu'une photo de vous prise par vos parents il y a plusieurs décennies et qu'ils trouvent « *mignonne* », – mais qui ne vous met pas en valeur –, ressurgisse un jour publiquement sur Internet. Pas sûr que vous apprécieriez. C'est ce qui peut arriver à vos enfants quand ils seront grands et que des photos d'eux prises aujourd'hui réapparaissent. Un autre risque de la publication de photos d'enfants sur Facebook et d'attiser la convoitise d'individus malintentionnés, dont des pédophiles.

Contactée par Le Défi Plus, Drudeisha Madhub, *Data Protection Commissioner*, cite d'autres exemples de risques liés à la publication de photos d'enfants. « *Les réseaux sociaux peuvent être très dangereux pour les enfants. Ils peuvent être approchés par des prédateurs sexuels et être victimes de harcèlement, d'insultes, de l'envoi de photos obscènes, etc. de la part d'autres mineurs. Ce phénomène comporte plusieurs types de risques comme le détournement d'une photo. Une photo récupérée sur un réseau social comme Instagram ou Facebook peut être modifiée et détournée à l'insu de son propriétaire. En sus, ils sont exposés au vol pur et simple de leur identité. Certains internautes créent de faux profils à la place d'autres personnes et se font passer pour celles-ci sur Internet* », dit Drudeisha Madhub.

Elle offre quelques conseils aux parents qui publient des photos de leurs enfants. Tout d'abord, il faut que les photos ne soient pas visibles par tout le monde. Il est possible de paramétrer l'audience des publications sur Facebook. Pour les photos de mineurs, il est conseillé de limiter la visibilité aux personnes les plus proches comme les membres de la famille. « *Les enfants sont souvent exposés au harcèlement en ligne. Il est important de ne jamais publier des photos compromettantes et d'en bloquer la diffusion par d'autres personnes* », ajoute Drudeisha Madhub.

Poster la photo d'un enfant peut devenir un calvaire pour lui à l'adolescence et à l'âge adulte.

La *Data Protection Commissioner* précise que les photos sont considérées comme des données personnelles sous le *Data Protection Act* (DPA) lorsque des personnes peuvent y être reconnues. Elle ajoute que les enfants méritent une protection spécifique concernant leurs données personnelles dont leurs photos. En vertu de l'article 30 de la DPA, il est interdit à toute personne de traiter les données personnelles d'un enfant de moins de 16 ans sans l'autorisation des parents ou de son tuteur légal.

« *Par conséquent, la publication des photos des enfants sur Internet ou les réseaux sociaux nécessite le consentement du parent ou du tuteur légal. La personne qui publie des photos a aussi le devoir de vérifier si le consentement a été donné ou autorisé. Il est à noter que le non-respect de l'article 30 de la DPA est passible, sur déclaration de culpabilité, d'une amende maximale de* Rs 200 000 *et d'un emprisonnement maximal de cinq ans* », prévient Drudeisha Madhub.

DONNÉES PERSONNELLES

Les cartes de fidélité vous récompensent et surveillent vos habitudes

Les commerçants proposent des programmes de fidélité à travers des cartes. Ces dernières ne servent pas uniquement à récompenser les clients loyaux, elles regorgent de données sur leurs habitudes de consommation.

PATRICE DONZELOT
patrice@defimedia.info

Elles sont de plus en plus nombreuses dans nos portefeuilles. Les cartes de fidélité sont proposées aux consommateurs pour, comme leur nom l'indique, fidéliser et récompenser les clients loyaux. Dans la pratique, les commerçants utilisent également les données dont ces cartes regorgent à des fins commerciales.

Il y a d'abord les données que le consommateur fournit lui-même lorsqu'il s'inscrit à un programme de fidélité. Il s'agit des informations personnelles et des coordonnées tels que le nom, le genre, l'adresse email, le lieu de résidence, le numéro de téléphone, la date de naissance et le numéro de carte d'identité. Ces données servent à identifier le client. D'autres informations comme le statut marital et le nombre d'enfants peuvent également être demandées. Elles servent à définir son profil en tant que consommateur.

Justement, pour mieux cerner le type de consommateur qu'est un client, les commerçants qui ont des programmes de fidélité utilisent d'autres données plus inattendues. Il s'agit des détails sur les achats à chaque passage en caisse, comme on peut le lire par exemple sur le site internet du programme de fidélité Wiiv du groupe mauricien IBL. Ainsi, à chaque fois qu'un client présente sa carte de fidélité en caisse, les produits ou services qu'il achète ainsi que les montants dépensés sont enregistrés dans le système. Sur son site internet, IBL indique que ces données servent entre autres à suggérer des produits ou services, incluant ceux de commerçants tiers, qui peuvent intéresser les clients. Elles permettent aussi aux commerçants d'analyser les habitudes de leurs clients afin entre autres de leur soumettre des informations et des promotions ciblées.

DATA PROTECTION ACT 2017

Contacté par le Défi Plus, le groupe IBL précise que les données servent au bon fonctionnement du programme Wiiv. « *C'est-à-dire que le membre obtienne bien les avantages offerts par chaque partenaire, tout simplement* ».

À Maurice, tout le monde ne peut pas faire ce qu'il veut de données personnelles. Les entreprises qui en collectent doivent se conformer à la Data Protection Act 2017. Le Data Protection Office est l'organisme chargé de veiller que les données soient collectées, stockées et traitées selon la loi. Répondant aux questions du Défi Plus, le Data Protection Office indique que concernant les détails sur les transactions, le consentement accordé par le client doit correspondre aux finalités pour lesquelles les données sont utilisées.

« *Dans le cadre du programme Wiiv, nous avons tout mis en œuvre pour que le traitement des données personnelles de nos membres soit en totale conformité avec les dispositions de la Data Protection Act 2017. Nous avons aussi retenu les services d'une plateforme de gestion spécialisée pour le stockage des données alignée sur les règlements européens de la protection des données. L'accès aux données est strictement limité aux personnes habilitées* », affirme Cécile Henry, IBL Group Loyalty Manager, dans une correspondance au Défi Plus.

« *Il incombe à l'organisation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour empêcher l'accès non autorisé, l'altération, la divulgation, la perte accidentelle et la destruction de données à caractère personnel conformément à l'article 31 de la Data Protection Act 2017* », ajoute le Data Protection Office.

L'agence précise que les commerçants doivent déterminer qui a le droit d'accéder aux informations personnelles de ces clients. L'accès aux données doit être limité aux personnes qui doivent y accéder dans l'exercice de leurs fonctions. En outre, ces personnes doivent être soumises à la plus stricte confidentialité. Les entreprises doivent être aussi attentives à sécuriser les données afin qu'elles ne soient ni volées ni utilisées à d'autres fins. Selon le Data Protection Office, la vente de données personnelles est illégale à Maurice. Mais si les clients sont informés au préalable, elles peuvent être partagées avec d'autres entreprises partenaires. Enfin, si un client décide de mettre fin à son compte, il peut demander au commerçant de supprimer ses données.

- **Le Mauricien**

  The DPC was interviewed regarding the following: the number of entities which are not yet registered with the DPO, registration of public sectors, the prosecution unit as well as on Safe City Project. The article was published by le Mauricien on Monday 03 June 2019.

- **Business Magazine**
  - Guest writer in Business Yearbook 2019

    To mark the 51st anniversary of the Independence of Mauritius, Business Magazine came up with a special edition featuring guest writers delivering their opinion on different themes. The DPC was one amongst the guest writers for this edition and provided an overview of the DPO, its achievements and the way forward. The article was published on 13 March 2019.

  - Data Protection Act and New Financial Services

    Upon the introduction of new payment facilities in Mauritius to the protection of users' private data, Business Magazine solicited the views of the DPC on this matter.

- **Global Finance Mauritius (GFM) Magazine**

  The tenth edition of the GFM magazine was published in November 2019. The DPC explained the requirements of the DPA. The article is also available online at the following URL: https://globalfinance.mu/emagazines/issue10/.

- **Data Protection Africa Summit Newsletter 2019**

  The DPC was interviewed regarding her experience and highlights as the host of the Data Protection Africa Summit, which was organised by Africa Digital Rights' Hub. The interview was published in the Data Protection Africa Summit Newsletter.

- **Essentielle Magazine**

  For Women's day, Essentielle magazine compiled a directory of 100 women CEOs and/or women who are assigned key positions in Mauritius. The DPC was also featured in the special edition "Essentielle Actives - Le Management au féminin, in collaboration with Business Magazine." This article was published in May 2019.

Nom : Madhub
Prénom : Drudeisha
Poste occupé : Data Protection Commissioner
Société : Data Protection Office
Un mot qui la définit : progressive
Ce qui la passionne : son travail car elle y puise une motivation constante pour avancer

L'ESPRIT FAIT TOUT. ON DEVIENT CE QUE L'ON PENSE.

Dans une ère propice à la capture et à la vente de données numériques publiques ou privées, Druideisha Madhub dirige un organisme clé, dédié à la protection de ces informations. Commissaire au Data Protection Office, rattaché au Prime Minister's Office, elle a une charge lourde en sens et en responsabilités.

Ce domaine, qui peut paraître intimidant à d'autres, passionne la jeune femme qui se dédie corps et âme à mettre en place l'architecture de gestion des donnes privées par les entreprises. Experte en la matière, Druidesha Madhub n'est pas peu fière de rappeler que «*Maurice est le premier pays africain à s'être doté d'une* Data Protection Act.»

Et à la commissaire d'ajouter : «*Depuis que l'Europe a mis en œuvre la Réglementation sur la protection des données, la RGPD, les établissements mauriciens qui gèrent des données de clients européens, comme l'hôtellerie, le BPO ou les sociétés de sous-traitance, se sont vite mis à la page. Or, peu de gens réalisent, que la* Data Protection Act *de Maurice est encore plus pointue que la RGPD.*»

Après un LLB à l'université de Maurice, elle est reçue première aux *Bar exams*. Elle rejoint le bureau de l'*Attorney General* pendant six ans et demie comme *Senior State Counsel* avant de décrocher la prestigieuse bourse Chevening pour poursuivre un LL.M en *International Human Rights*.

Depuis 2011, la Commissaire est reconnue comme experte en *data protection and human rights* par Interpol. Depuis 2014, elle fait partie des experts des Nations unies au sein du *UN Global Pulse Data Advisory Group*. Druidesha Madhub est aussi membre de prestigieux réseaux internationaux comme l'Association francophone des autorités de protection des données personnelles, le Réseau africain des autorités de protection des données personnelles, le Global Privacy Enforcement Network, le Common Thread Network (CTN) et le Conseil de l'Europe.

(e) Notices to the Public

In view of the growing number of telephone calls and queries from the public and the very limited number of staff available, the DPC issued a notice on 13 December 2019 which was displayed in the office to inform the public on the procedures for handling legal queries and complaints by this office to ensure effective customer service.

II. Capacity Building

In 2019, officers of the DPO had the opportunity to attend the following workshops.

Title	Date
Utilisation of Infohighway	26th September 2019
National risk assessment of money laundering and terrorism financing risks	29th August 2019
IDC CIO Summit 2019 Mauritius	22nd August 2019
Blockchain and AI by Gartner	25th July 2019
Advanced Passenger Information System	10th July 2019
Cyber Drill Workshop for Critical Sectors	24th-25th April 2019
Cybersecurity Capacity Maturity Model for Nations	13th-15th February 2019

III. Enforcing Data Protection

(a) Investigation on Complaints

During the period January to December 2019, the DPO received fifty-two (52) new complaints regarding investigations on the below subjects, among others:

- Unauthorised use of CCTV Camera
- Unlawful disclosure of personal information
- Unauthorised access to personal data

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.

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

- Challenges faced

  This office noted an increase in the number of complaints received as compared to previous years. Out of 52 complaints filed at this office, 31 complaints concerned the use of CCTV cameras. It is indeed difficult for three (3) data protection officers to handle complaints of such nature where site visits need to be effected at a remote far and/or sometimes at unsecured locations.

  In addition, as per section 53 (3) of the Data Protection Act, no prosecution shall be instituted under the Act except by, or with the consent of, the Director of Public Prosecutions. During the year 2019, 2 cases regarding CCTV cameras were sent to the Office of the Director of Public Prosecutions (DPP) for advice on prosecution. However, we were informed by the DPP's office that there are queries which need to be addressed before the DPP can proceed with its advice. Consequently, the enquiries need to be redone in a way similar to how the police would proceed. Furthermore, the data protection officers who are IT experts do not have the required expertise to prosecute and file warrants.

  Thus, there is a pressing need for police officers to be posted to this office to address these issues.

(b) Decisions on Complaints

- Decision No 53 - 02.05.2019 - Complaint on use of CCTV Camera

  No offence was found to be committed under the DPA, the enquiry was closed.

- Decision No 54 - 06.05.2019 - Complaint on use of CCTV Camera

  No offence was found committed under the DPA, the enquiry was closed.

- Decision No 55 - 08.05.2019 - Complaint on use of CCTV Camera

  No offence was found to be committed under the DPA, the enquiry was closed to the satisfaction of all parties.

- Decision No 56 - 09.05.2019 - Complaint on use of CCTV Camera

  Since Respondent complied with all the directives of this office, there was no justifiable reason to suggest that an offence was committed under the DPA. The enquiry was thus closed.

- Decision No 57 - 26.06.2019 - Unlawful disclosure of personal data

  Respondent took corrective measures in order to avoid the repetition of such incidents. The enquiry was closed.

- Decision No 58 - 05.09.2019 - Unlawful disclosure of personal data

  The enquiry was closed to the satisfaction of all parties concerned and no breach of the DPA was found.

- Decision No 59 - 25.09.2019 - Complaint on use of CCTV Camera in a mosque

  This office was satisfied that appropriate measures were taken to protect the personal spiritual life of the people attending the mosque for their prayers by Respondent, to the satisfaction of every party concerned. The enquiry was closed and no breach of the DPA was found committed.

- Decision No 60 - 10.10.2019 - Unlawful disclosure of personal data

  Since no concrete evidence was adduced by either party to this case to substantiate the allegations raised, this enquiry was closed and no breach of the DPA was found committed.

- Decision No 61 - 17.10.2019 - Complaint on the use of CCTV Cameras

  The enquiry revealed that, to the satisfaction of both parties, no cameras were capturing prohibited images and thus no breach of the DPA was established.

- Decision No 62 - 31.10.2019 - Complaint on unlawful disclosure of personal data

  After a careful analysis of submissions from both parties which was the established procedure laid down by this office to gather founded and substantiated evidence regarding any enquiry lodged, no breach of the DPA was found proven, namely sections 28(b) (iv) and/or (v), which indicated that consent was not required where the processing was necessary:-

  - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
  - for the performance of any task carried out by a public authority, respectively, given that it concerned a parastatal body operating under the aegis of a particular Ministry.

- Decision No 63 - 04.11.2019 - Complaint on unlawful disclosure of personal data

  The enquiry was conducted successfully to the satisfaction of all parties concerned relating to the territorial applicability of the DPA within the Mauritian context. The enquiry was thus closed.

(c) Prosecution Unit

Complaint investigation involves a series of tasks such as recording statements of parties concerned, issuing enforcement notices, performing onsite verifications, warrants for effecting entries and searches, preservation orders, sealing of evidence and preparation of investigation reports.

Given the nature of tasks required and since this office is required to prosecute cases under the DPA before the Intermediate Court as provided for by section 53 of the Act, it requested for 5 police officers of appropriate grades to be posted to the DPO to perform the following duties:

- Dealing with controllers and processors who are contravening the DPA,
- Conducting investigations and searching of premises (Data Protection Officers also assist with complaints' investigation on IT-related issues),
- Preparing and swearing of information in respect of offences under the Act or any regulations made under it before a Magistrate and prosecuting the case,
- Filing of warrants,
- Carrying out site visits.

Discussions and negotiations regarding this unit started since 2016. We are now awaiting an official reply from the Police.

IV. Improving Legal Protection

By virtue of section 51 of the Data Protection Act, 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 is co-respondent in a case regarding a data subject access request. The person also lodged a complaint in October 2019 to this office which is currently under investigation.

(b) ICT Appeal Tribunal

In 2019, an appeal was lodged at the ICT Appeal Tribunal against the decision of the Commissioner regarding a case of unlawful use of camera surveillance in lorries carrying hazardous products. The case is still ongoing.

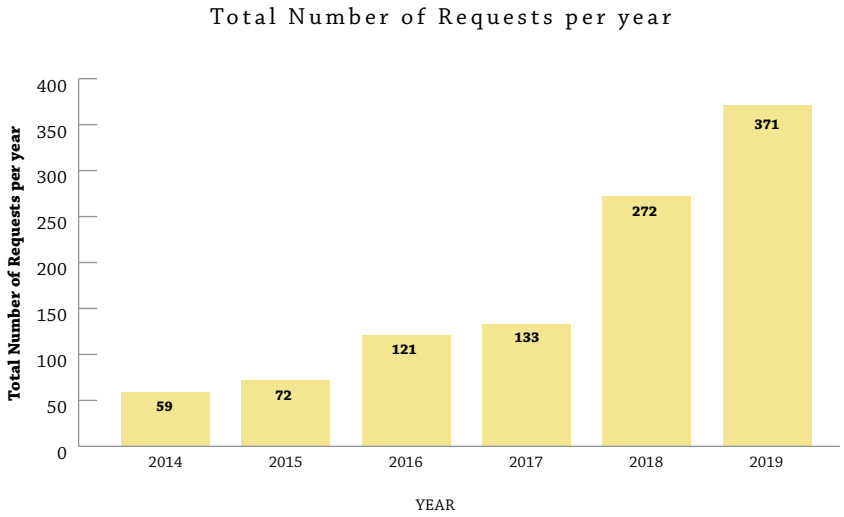
V. Registration of Controllers

This office has received approximately seven hundred and ninety-five (795) applications for registration as controller and two thousand, five hundred and three (2503) applications have been processed for renewals of registration of controllers.

VI. Requests for Legal Advice

In 2019, this office received a total of three hundred and seventy-one (371) written requests for advice comprising of 189 from private bodies and 182 from ministries, governmental departments and parastatal bodies. The increase was due to the growing awareness of the DPA and the GDPR.

VII. Advisory Role/Stakeholder in Projects



(a) API and Passenger Name Records (PNR) Project

The DPO submitted views on the draft regulation for API and Passenger Name Records (PNR) prepared by the Prime Minister's Office.

(b) E-Passport Project

The Office provided its views on the inception report submitted by the Consultants regarding this project.

(c) E-Health Project

The DPO provided advice to the Ministry of Health and Quality of life regarding the e-health project.

(d) Bonus Malus System

The DPO formed part of the Sub-Committee, that was chaired by the Financial Services Commission to make recommendations for the Centralised Database of Information of the Bonus Malus System.

The DPO also provided its comments on the Bonus Malus Report, submitted by the Technical Committee, which was led by the Ministry of Financial Services and Good Governance to look into the feasibility of establishing a Bonus Malus System in Mauritius.

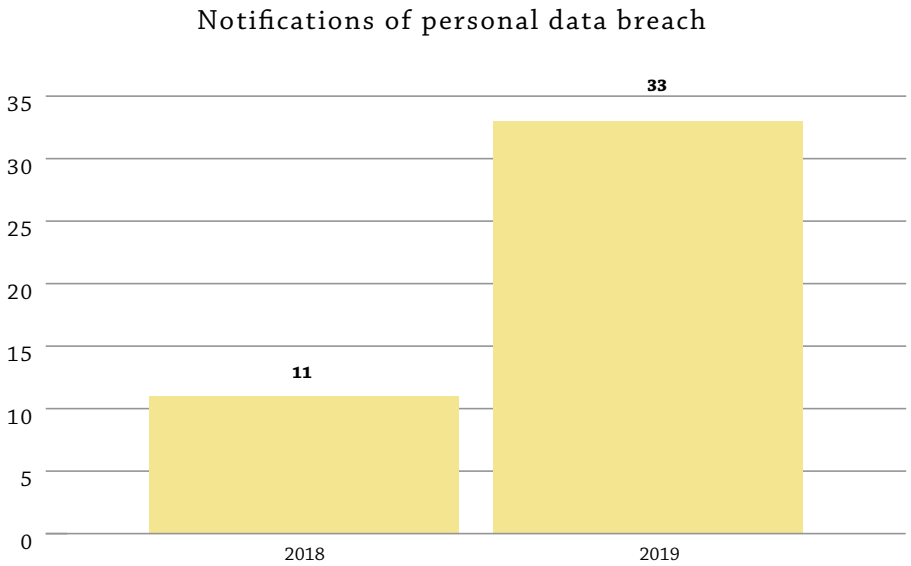
(e) Trade-In Service Agreement

The DPO provided its views on proposals made with regard to the processing of personal data in Trade in Services agreements for the African Continental Free Trade Area and WTO Agreements.

VIII. Personal Data Breach Notification

Thirty-three (33) personal data breaches have been reported to this office last year. The number of breaches has increased compared with the previous year due to the fact that organisations are increasingly more aware of their legal obligation to report personal data breaches.

An analysis of the breaches received confirmed that email phishing attacks, employee's wrong usage of emails and business email compromise remain the common causes of potential breaches.



IX. Transfer of Personal Data Abroad

The DPC authorised twenty-eight (28) companies, which provided proof of appropriate safeguards as required under section 36 of the Data Protection Act to transfer personal data outside Mauritius.

X. New forms designed in line with DPA 2017

Certification

This office finalised the certification process. The concept of certifying data processing operations is a significant development in creating a reliable and auditable framework for organisations. The certification mechanism is voluntary and is a way of demonstrating that controllers and processors are implementing appropriate technical and organisational measures. A certificate is then issued by this office as the certifying body, which is renewable after a period of 3 years.

XI. Modernised Convention 108

The Ministry of Technology, Communication and Innovation in collaboration with DPO has initiated procedures with the Ministry of Foreign Affairs for the ratification of the Modernised Convention 108 with the Council of Europe.

The benefits of signing the Protocol is that the Convention lays down the principles and values which aim at protecting the rights of individuals whilst providing a framework for international data flows. This is critical as global information flow play an increasingly significant role in modern societies, enabling the exercise of fundamental rights and freedom while triggering innovation and fostering social and economic progress as well as playing a vital role in ensuring public safety. Furthermore, the development and use of innovative technologies should also respect these rights. The Convention thus aims to reinforce co-operation and mutual assistance between Parties, thereby providing the appropriate legal basis for a framework of co-operation and exchange of information for investigations and law enforcement.

This Convention is the first and, to date, the only international legally binding instrument dealing with data protection. It is to be highlighted that Mauritius ratified the Convention 108 on 17 June 2016 which came into force in October 2016.

The new Convention also lays down international standards which are based on the principles contained in the GDPR also to be found in our DPA 2017.

XII. EU Adequacy

Obtaining adequacy with EU signifies that Mauritius satisfies the EU criteria for an adequate level of data protection and thus, personal data can easily be transferred from EU to Mauritius, thereby facilitating business/trade with EU. This office has already initiated negotiations with the EU in collaboration with its Ministry.

XIII. Other Achievements

(a) DPO's Website

The DPO's website has been revamped to make it more user-friendly. The information has been categorized under specific headings for ease of navigation and animations have been included as part of the enhancement process. It has now become a very good source of information for users.

(b) Guide on Data Protection and Media

This guide aims at safeguarding the privacy of public figures and private persons and explains how media organisations should comply with data protection principles while maintaining a free and independent role. It also elaborates on a general recommended approach towards compliance with the DPA 2017 and best practices. The guide was completed in 2019 but launched on 16 January 2020 during a conference organised by the DPO.

(c) Data Protection Training Toolkit – Frequently Asked Questions

This office made an analysis of questions received from the public and private sectors and drew a list of Frequently Asked Questions. This list of FAQs was incorporated in the data protection training toolkit to assist controllers and processors.

XIV. Projects in the Pipeline

(a) Data Protection Training Toolkit – Corporate Video and Clips

The DPO embarked on the development of a training toolkit on data protection since 2018 as one of its major sensitisation activities. It is a self-learning tool on the DPA which will be available freely on this office's website. The Training Toolkit is expected to be completed by the beginning of January 2020.

(b) Data Protection Regulations

This office drafted the Data Protection Regulations in line with the advice provided by the State Law Office. The Regulation is expected to be proclaimed in 2020.

(c) Code of Practice for the operation of SafeCity

The office is currently drafting a code of practice for the operation of the Safe City Project in compliance with the DPA. This code of practice is expected to be completed by early 2020.

(d) Updating DPO's Computerisation System

With the proclamation of the Data Protection Act 2017 in January 2018, the existing computerisation system needs to be updated to meet the requirements contained in the new Act. As such, this office has submitted its change request requirements to the supplier.

(e) Guide on National Security and Privacy

A guide on National Security is being drafted by this office. This guide will present an overview of the legal architecture of the data protection landscape in the United Nations, the European Union, Africa as well as in Mauritius on national security. It will also offer some relevant guiding principles that institutions should adopt in order to monitor citizens for national security purposes and at the same time without infringing privacy rights.

(f) Information sheet on Virtual Currencies

An information sheet on privacy and virtual currencies is expected to be issued in 2020.

Designed and printed by the Government Printing Department - June 2020
Resources: www.freepik.com