

Annual Report

January to December 2018

10th Edition



DATA PROTECTION OFFICE

Table of Contents

MISSION AND VISION STATEMENTS	3
1. Mission of the Data Protection Office	3
2. Vision of the Data Protection Office	3
FOREWORD	5
DATA PROTECTION OFFICE (DPO)	7
ORGANISATION STRUCTURE	8
BUDGET FOR FINANCIAL YEAR 2018-2019	9
I. HUMAN RESOURCE REQUIREMENTS	9
II. EXPENDITURE	10
ACTIVITIES IN 2018	11
1. FINANCIAL STATUS	11
I. Revenue Collected	11
2. INTERNATIONAL PARTICIPATION	12
I. Participation in International Conferences	12
II. African Union Workshop	13
III. Membership and cooperation with international organisations	14
a) Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)	14
b) International Conference of Data Protection and Privacy Commissioners (ICDPPC)	14
c) The Global Privacy Enforcement Network (GPEN) and Common Thread Network (CTN)	14
d) Commission Nationale de l'Informatique et des Libertés (CNIL)	14
e) The Council of Europe (CoE)	14
f) Organisation for Economic Co-operation and Development (OECD)	15
g) Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP)	15
3. NATIONAL ENGAGEMENT	16
I. Sensitisation	16
a) Data Protection Workshop	16
b) Publications	17
c) Requests for Presentations / Speeches at Controllers' Sites	18
d) In House Presentations	19
e) Training in Rodrigues	19
f) Articles	20
g) Press Communiqué / Interview	20
II. Benchmarking Visit from Ugandan Delegates in Mauritius	20
III. Data Protection Africa Summit	22
IV. Enforcing Data Protection	24
a) Investigation on Complaints	24
b) Decisions on Complaints	25
V. Improving legal protection	26
a) ICT Appeal Tribunal	26

b)	Supreme Court	27
c)	Industrial Court	27
VI.	Registration of Controllers	27
VII.	Requests for legal advice	28
VIII.	Advisory Role / Stakeholder in Projects	29
IX.	Modernised Convention 108	29
X.	New forms designed with respect to requirements of DPA 2017	30
a)	High Risk Processing Operations	30
b)	Data Protection Impact Assessment (DPIA) Form	30
c)	Personal Data Breach Notification Form	30
d)	Controller and Processor Registration/Renewal Forms	30
e)	Transfer of Personal Data Form	31
f)	Records of Processing Template	31
g)	Certification	31
XI.	Personal Data Breach Notification	32
XII.	Transfer of Data Abroad	32
XIII.	Other achievements	32
a)	MS ISO 9001:2015	32
b)	Computerisation	33
c)	Information Security Management System (ISMS)	33
d)	Forensics	33
e)	Capacity building provided to officers of this office	34

PROJECTS IN PIPELINE	35
I. GUIDE ON DATA PROTECTION AND MEDIA	35
II. AUDIO VISUAL CLIPS	35

MISSION AND VISION STATEMENTS

1. Mission of the Data Protection Office

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

2. Vision of the Data Protection Office

- 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

As depicted in our previous annual reports, this office is continuing its perpetual struggle with a depleted workforce in meeting its new and huge mandate attributed to it under the new Data Protection Act (DPA) which came into force on 15 January 2018 without undermining the immense impact that the new European Union General Data Protection Regulation (GDPR) which came into force on the 25 May 2018, has on the role and functions of this office. The latter is regularly called upon to ensure that alongside compliance and enforcement under DPA, the GDPR is also being respected in its fundamentals, in order to avoid any situation where the reputation of Mauritius as a safe and democratic country respecting the basic human rights of people including the right to privacy, is not put at stake.

Indeed, it is expected that this report will enlighten our government on the urgency of ensuring that this office does not lose the momentum it has gathered over the years by equipping it with the right expertise for it to flourish and assist in promoting the interests of our country in the international arena together with the promotion of the protection of personal information as a prerequisite for healthy and ethical business.

With these words, I sincerely hope that this office will not have to face the same difficulties it has painfully endured and its new mandate will provide it with a new and promising profile, with due recognition to all the staff of this office who work under extreme pressure to meet the exigencies of their respective duties.



Mrs Drudeisha MADHUB (BARRISTER-AT-LAW)

DATA PROTECTION COMMISSIONER

DATA PROTECTION OFFICE (DPO)

The Data Protection Office became operational since 16th February 2009 when the Data Protection Act 2004 came into force. On 15th January 2018, the Data Protection Act 2004 was repealed and the Data Protection Act 2017 was proclaimed. The coming into force of the new DPA in 2018 has been a pioneering achievement of this office in order to strengthen the control and personal autonomy of individuals over their personal data and to timely comply with the requirements of the General Data Protection Regulation (GDPR) which came into force on 25th May 2018 in the European Union; thereby contributing to cement Mauritius's 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:

- (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, 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 this Act;
- (e) Promote self-regulation among controllers and processors;
- (f) Investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under the DPA;
- (g) Take such measures as may be necessary to bring the provisions of this Act 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 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;
- (j) To cooperate with supervisory authorities of other countries, to the extent necessary for the performance of his duties under this Act, in particular by exchanging relevant information in accordance with any other enactment;

The Data Protection Office, headed by the Data Protection Commissioner, is located on the 5th Floor of Sicom Tower, Wall Street, Ebène.

Phone: 460 0251

Fax: 489 7341

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

Email: dpo@govmu.org

ORGANISATION STRUCTURE

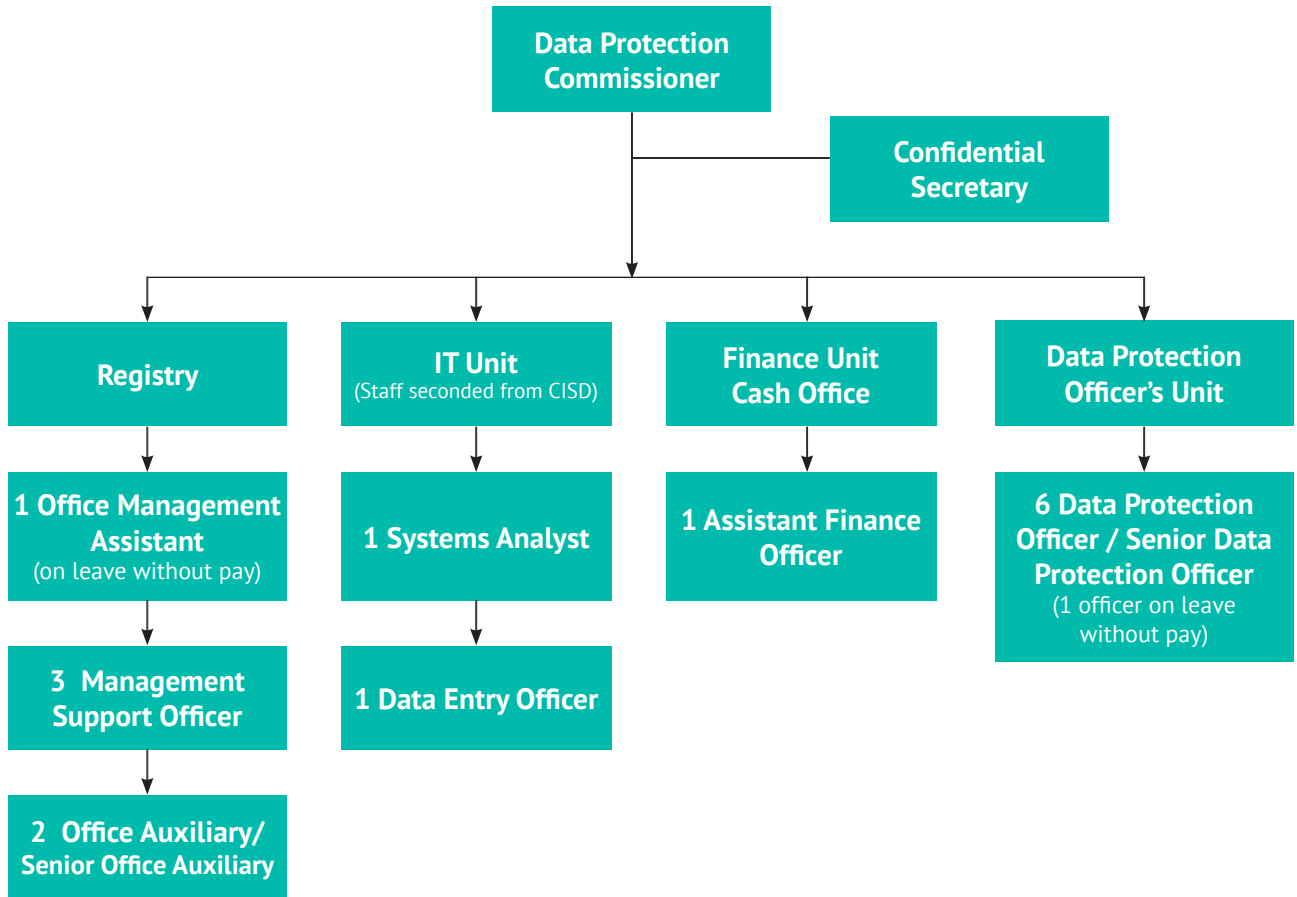


Figure 1 : Organisation Structure

BUDGET FOR FINANCIAL YEAR 2018-2019

I. Human Resource Requirements

In March 2018, the Data Protection Office began drafting its budget proposals consisting of the human resource requirements and expenditure for the financial year 2018/2019.

Unfortunately, over the past years, one long outstanding problem faced by this office is the severe insufficiency of human resources, which inevitably hampers on the efficiency of service delivery. The effect of limited staff was felt even worse in 2018 because with the coming into force of the Data Protection Act 2017, the volume and complexity of work increased substantially with the introduction of new functions in line with international practices regarding personal data breaches, data protection impact assessments, certification seals, sensitisation, auditing, security checks, hearing of complaints and preparing and swearing of information in Court for offences under the DPA.

However, by the end of 2018, there has been no perceptible change concerning human resource. For instance, the schemes of service for the grades of Principal Data Protection Officer, Data Protection Officer/Senior Data Protection Officer, Legal Executive, and Assistant Data Protection Officer were still not yet prescribed, failing which recruitment cannot be effected. It is noted with concern that these grades were recommended since PRB 2016 report but by December 2018 this has been a dwelling issue and no recruitment has been possible to bring relief to existing staff.

On the administrative side, our request to have an Office Management Executive posted at the Data Protection Office to manage all procurement, purchasing and human resource matters was not fulfilled during 2018. Additional Office Management Assistant and Management Support Officers were also not obtained. Replacement for the existing post of Office Management Assistant was also not fulfilled.

As regards top management, the Commissioner is 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 Data Protection Commissioner in her daily tasks was not fulfilled in 2018.

The Data Protection Office, being an enforcement body, has the huge responsibility to deal with non-compliance issues and try offences before the Court. It is thus imperative to have police officers of an appropriate grade 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. Till date, there are no police officers posted at the office to handle these matters.

During 2018, one Assistant Finance Officer and one Systems Analyst were posted at the office. The office also wrote to the Ministry of Labour, Industrial Relations, Employment and Training for 6 Youth Employment Programme (YEP) to assist the office in the Registry section. 6 YEP trainees joined the office in October 2018.

II. Expenditure

The purchase of a car for DPO has not been executed in the first six months of the financial year 2018-2019. This has partly impacted on the site visits to be carried out by this office. The running cost for the office expenditure has remained the same as the previous financial year despite the new functions and responsibilities added by the Data Protection Act 2017.

ACTIVITIES IN 2018

1. FINANCIAL STATUS

I. Revenue Collected

During the year 2018, the Data Protection Office has collected a total revenue of Rs 6,280,900. The increase in total revenue compared to years 2015-2017 may be attributed to the proclamation of the Data Protection Act 2017 and the fact that 2018 has been a promotional year for the office and a series of sensitisation initiatives have been undertaken to help controllers and the public in general understand the provisions of the new Act.

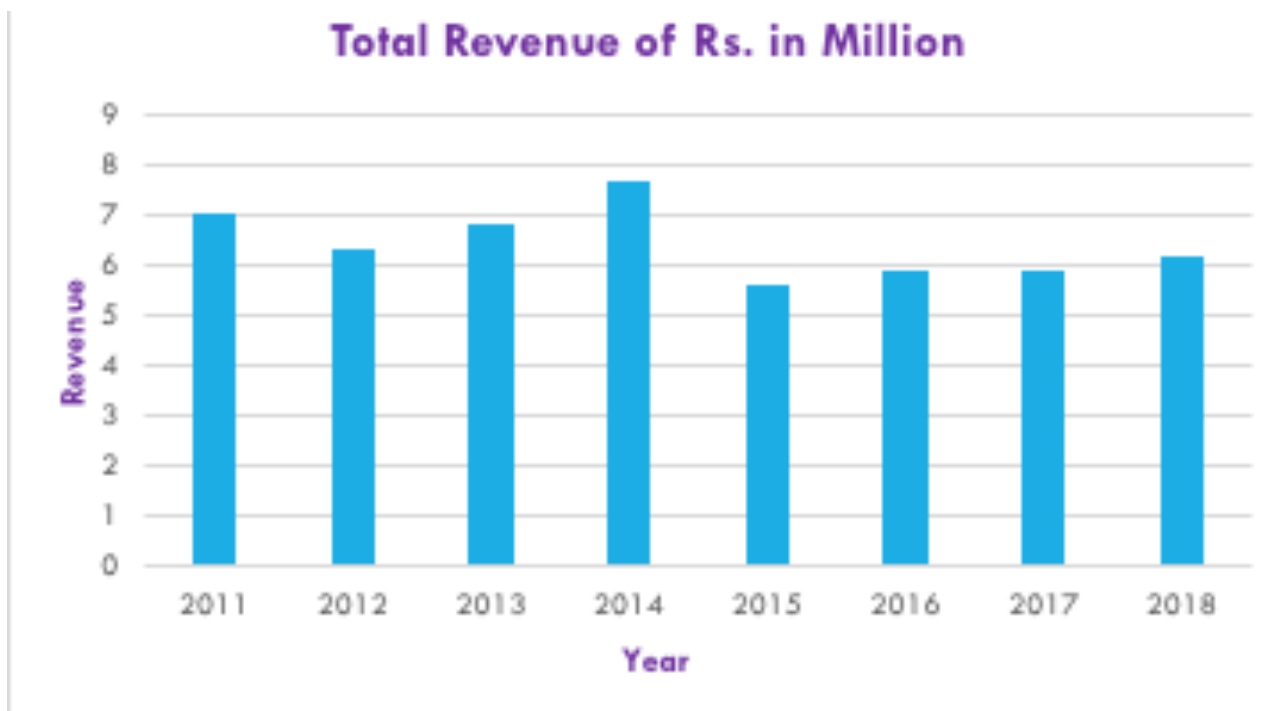


Figure 2 : Line Chart representing revenue collected for year 2018

It is simultaneously observed that the amount of revenue collected depends on:

- The issue of renewal notices to controllers who have failed to pay their renewal fees; and
- The issue of enforcement notices to controllers who have not yet registered with the office.

However, due to shortage of staff, renewal and enforcement notices could not be issued to controllers on a regular basis during 2018.

2. INTERNATIONAL PARTICIPATION

I. Participation in International Conferences

The Data Protection Office of Mauritius is recognised on the international front as an effective regulator along with other privacy and data protection authorities around the globe. The Data Protection Commissioner is often invited by international data protection authorities to share her knowledge and expertise in the field of data protection enforcement. Cooperation with privacy and data protection authorities around the world helps privacy authorities to effectively fulfill their mandates, both individually and in concert, through diffusion of knowledge and supportive connections.

During 2018, the Data Protection Commissioner participated in the following international conferences:

Period	Event
19-21 June 2018	36 th Plenary Meeting of Committee of Convention 108 Strasbourg, Paris
25-27 November 2018	2 nd Additional Protocol Budapest Convention, Palais de l'Europe – Strasbourg, France

The Data Protection Commissioner could not attend the following conferences:

Period	Event	Remarks
18-19 October 2018	12th General Assembly of AFAPDP	Approved but could not attend as it was closely related to the Brussels Conference below
22-26 October 2018	40th ICDPPC Conference in Brussels	Not approved by parent Ministry
20-22 November 2018	37 th Plenary Meeting of Committee of Convention 108 Strasbourg, Paris	Not attended as the Commissioner was already taken up with the Data Protection Africa Summit

II. African Union Workshop

One Data Protection Officer/Senior Data Protection Officer participated in the workshop organised by the African Union on 17 and 18 December 2018. Participants from all member states were invited. The workshop provided an overview of the main challenges and opportunities of processing personal data in Africa and its impact on the development of the Internet economy and data analytics as well as the protection of digital rights of african people.

A specific focus was dedicated to raising awareness of african governments/businesses and individuals on the challenges related to the sustainable and responsible use of personal data. The workshop also highlighted the urgent need for african countries to develop a consistent approach on data governance through the establishment of a National Data Protection Authority to sustain trust and confidence in their national cyberspace.

An analysis of national and international data protection principles and regulations was made through the sharing of experience of participating african countries. A situational status of the readiness with regard to the protection of african people's data and respect of online privacy was presented.

Furthermore, as the EU is a trading partner of most african countries, this workshop also explained the global impact of the General Data Protection Regulation (GDPR). Participants debated on GDPR's wider scope and its potential implications on african businesses and government institutions, and discussed challenges related to compliance with GDPR requirements.

The workshop provided an opportunity for the participants to discuss specific african concerns, exchange best practices, familiarise with regional and international best practices and develop guidance on the creation of National Personal Data Protection Authority aiming to regulate the national data processing as well as the cross border transfer of personal data.

Requests were made to member states to ratify the African Union Malabo Convention on Data Protection which Mauritius has already ratified in March 2018.

III. Membership and cooperation with international organisations

- a) **Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)**
The AFAPDP contributes to guaranteeing the fundamental rights of individuals in Francophone digital space by developing and enhancing expertise in the protection of personal data. During 2018, this office participated in a survey carried out by AFAPDP aiming to collect information on the implementation of GDPR from member countries who do not form part of the European Union. The questionnaire helped the AFAPDP Secretariat to identify the common difficulties encountered by non-EU Francophone authorities and to think about joint actions on this matter. The answers submitted were used to animate the meeting of 19th October 2018.
- b) **International Conference of Data Protection and Privacy Commissioners (ICDPPC)**
The Data Protection Office participated in the ICDPPC Global Privacy and Data Protection Awards 2018 and submitted its Introductory Guide on Data Protection Act 2017 as entry in the category 'Education and public awareness'.
- c) **The Global Privacy Enforcement Network (GPEN) and Common Thread Network (CTN)**
The Data Protection Office is a member of GPEN and CTN. During 2018, our office participated in a survey carried out by GPEN regarding audit activities. The objective of the survey was to improve the general mutual understanding of the member authorities' respective audit programs, how these have been implemented and to incorporate those learnings.
- d) **Commission Nationale de l'Informatique et des Libertés (CNIL)**
CNIL launched a survey in June 2018 to ask for views from data protection members on privacy rights, both in practice and in the legislation, and related information delivered to parents and children on educational platforms online.
Our office contributed in the survey and provided input to the questionnaire on e-learning platforms and other online educational services. Useful feedback information was thus collected by CNIL and its counterparts to formulate relevant draft recommendations and resolutions adapted to the protection of children.
- e) **The Council of Europe (CoE)**
The Data Protection Office provided inputs on the major developments in the data protection field which was presented at the 36th plenary meeting in Strasbourg from 19-21 June 2018 and published on the Council of Europe's website.

The office also found the following recommendations prepared by the Council of Europe as comprehensive:

- Practical guide on the use of personal data in the police sector
- Draft recommendation on the protection of health-related data

f) **Organisation for Economic Co-operation and Development (OECD)**

The office participated in a survey conducted by OECD on personal data breach notification reporting.

The objective of the survey was to encourage privacy enforcement authorities to collect and report to enhance comparability in personal data breach notification reporting and strengthen evidence-based policy making for privacy and personal data protection.

g) **Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP)**

The Data Protection Office is a member of RAPDP.

3. NATIONAL ENGAGEMENT

1. Sensitisation

Given that the Data Protection Act 2017 was proclaimed on 15 January 2018 with new requirements on controllers and enhanced data subjects' rights, this office engaged actively in various awareness promoting activities in 2018. Indeed, the spirit of year 2018 has been educating people and the office left no stone unturned to venture in diverse initiatives and awareness programmes to the benefit of our people despite the limited resources available.

a) Data Protection Workshop

The Data Protection Office organised a full day workshop themed the 'Data Protection Act 2017' on the 06th of March 2018 at InterContinental Mauritius Resort, Balaclava to create awareness on the new Data Protection Act in Mauritius.



Around 550 participants comprising consumers, private organisations, government officials, academia, non-profit organisations and privacy professionals came under one roof to discuss the application of the Act.

Data Protection Officers/Senior Data Protection Officers made presentations on the obligations of controllers and processors, new concepts such as data protection impact assessments, notification by controllers of personal data breaches to the Data Protection Office and data subjects, voluntary certification mechanisms and data protection seals and marks for controllers.

b) Publications

i. Leaflet on Data Protection Act 2017

This office designed a leaflet on DPA 2017 that provides a brief overview of the Data Protection Act 2017. The leaflet provides a quick, easy and summarised outline on the obligations on controllers and processors and on the rights of individuals.

ii. Introductory Guide to the Data Protection Act 2017

The Data Protection Office prepared and launched on 06 March 2018 an 'Introductory Guide to the Data Protection Act 2017'. This guide has been issued to assist controllers and processors to implement the provisions of the Data Protection Act 2017. It highlights the key changes, challenges and actions that organisations should adopt in order to achieve compliance.

iii. Guide on Registration/Renewal

In 2018, the office received a surge of queries via phone and emails regarding the procedures for registration and renewal as controller. This may be attributed to the fact that with the coming into force of the new Data Protection Act, more controllers have become aware of their legal obligation to register and renew their registration with the office.

In order to address the queries effectively, this office published a guide on its website on registration and renewal procedures. This guide has been very useful as an informative tool to the public given that this office already has a severe shortage of staff and the audiotext service which was available to the public for any queries on registration/renewal was terminated in July 2017 by the Ministry.

The guide provides a step by step assistance on:

- Obligations of controllers
- Procedures for registration
- A stepwise approach on how to fill the application form for registration and renewal
- Procedures for renewal
- Arrears of payment for registration and renewal(s)
- Procedures on how to obtain a certificate of registration from the Data Protection Office.

c) Requests for Presentations / Speeches at Controllers' Sites

In view of the high influx of requests from controllers to provide training or to act as focal speakers, the limited staff at the office has been able to deliver only 9 trainings as follows:

Title	Presented By	Date	Audience
Legal Panel Discussion: Compliance to and enforcement of DPA and GDPR	Data Protection Commissioner	31st August 2018	Data Protection Conference organised by Juristconsult Chambers
An Overview of the Data Protection Act 2017	Data Protection Officer/Senior Data Protection Officers	29th August 2018	Poivre Corporate Services Ltd
An Overview of the Data Protection Act 2017	Data Protection Commissioner	31st July 2018	Members of Association of Trust and Management Companies (ATMC)
Challenges and Opportunities for law practitioners	Data Protection Commissioner	26th July 2018	Institute of Judicial and Legal Studies
An Overview of DPA 2017	Data Protection Officer/Senior Data Protection Officers	21st June 2018	Administrative and Academic staffs of Le Bocage International School
DPA 2017 Part 1 - Morning Session Part 2 - Afternoon Session	Data Protection Officer/Senior Data Protection Officers & DPC	15th May 2018	Workshop on Data Protection Act 2017 at Hennessy Park Hotel, Ebene (organised by Baker Tilly & Global Finance)
An Overview of the Data Protection Act 2017	Data Protection Commissioner	5th April 2018	Temple Professionals Limited
An Overview of the Data Protection Act 2017	Data Protection Officer/Senior Data Protection Officers	9th March 2018	Staff of Confident Asset Management Limited
A Legal Overview of Data Protection Act 2017	Data Protection Commissioner	6th February 2018	Members of MEXA

d) In House Presentations

In view of the growing demand of controllers and processors for answers and guidance on the Data Protection Act 2017, this office spearheaded the innovative initiative to conduct inhouse trainings despite the severe lack of human resource and limited training space. 70 controllers were convened for training at the Data Protection Office which spanned over 4 training sessions in 2018. Participants had the opportunities to ask face to face questions with the Data Protection Commissioner.

Title	Presented By	Date	Audience
An Overview of the Data Protection Act 2017	Data Protection Officer/ Senior Data Protection Officers & DPC	29 th November 2018	Participants from Parastatal and Private Sector
An Overview of the Data Protection Act 2017	Data Protection Officer/ Senior Data Protection Officers & DPC	15 th November 2018	Participants from Private Sector
An Overview of the Data Protection Act 2017	Data Protection Commissioner & DPC	4 th October 2018	Participants from Public and Private Sector
An Overview of the Data Protection Act 2017	Data Protection Officer/ Senior Data Protection Officers & DPC	20 th September 2018	Participants from Public and Private Sector

e) Training in Rodrigues

This office has conducted a 2 day 'Train the Trainer' course in Rodrigues in the month of October 2018 in collaboration with the Commission for ICT of Rodrigues. The Commissioner for ICT, Mrs. Franchette Gaspard Pierre Louis, opened the training session and stressed on the importance of data protection especially before the advent of fibre optics in Rodrigues. The following topics were discussed:

- Overview of Data Protection Act 2017,
- The concept of consent,
- Lawful processing under DPA 2017,
- Records of processing operations,
- Transfer of personal data abroad,
- Cloud computing,
- Security of processing,
- Data breaches,
- Privacy policy, and
- Registration of controllers and processors.

A further half day session was organised with senior officers from different departments in Rodrigues. The feedback received has shown that the training has allowed participants to better understand the new provisions of the Data Protection Act.

f) Articles

The office provided input to the U.S. Embassy to Mauritius and Seychelles for the Investment Climate Statement (ICS) 2018 on data protection for Mauritius.

The Data Protection Office also contributed in the drafting of an article titled 'Mauritius's achievement in the field of Data Protection' for the Seventh Edition of Global Finance Mauritius (GFM) magazine.

g) Press Communiqué / Interview

A communiqué regarding the proclamation of the new Data Protection Act 2017 in Mauritius was published in the local newspaper as well as the international magazine 'The Economist'.

On 26 March 2018, the Data Protection Commissioner was interviewed by Le Defi Media for an article titled "Vol de données sur Facebook: la commissaire du Data Protection Office mauricien est <<choquée>>."

In April 2018, a press communiqué was issued by this office to sensitize citizens on the precautions, rights and avenues of remedy concerning those using social media and the Internet in Mauritius. This office deemed necessary to publish this communiqué in the light of comments raised during the year regarding the Facebook and Cambridge Analytica Scandal.

In September 2018, another press communiqué was issued by this office to inform organisations (public and private) that the Data Protection Office will be organising inhouse training sessions on the Data Protection Act 2017.

II. Benchmarking Visit from Ugandan Delegates in Mauritius

The Ugandan Parliament approached United Nations Pulse Lab Kampala to request support on best practices from the region to explore the role of data processing for sustainable development, why organisations need laws to assure legal certainty and how countries have developed compatible systems. The objective was to share lessons learned within the context of developing and least developed economies to ultimately incorporate recommendations in their national Bill.

Mauritius was chosen because we have long experience of implementing data privacy and protection legislation. To foster the exchange of ideas, UN Pulse Lab Kampala organised a visit to Mauritius for a delegation of parliamentarians and other officials from Uganda from 9th to 11th May 2018. The delegation met with key public and private sector stakeholders in the area of data protection and privacy in Mauritius. Exchanges with authorities like the Ministry of Technology, Communication and Innovation (MTCI) and the Data Protection Office as well as other relevant stakeholders from the private and government sector enabled the delegation to better understand challenges and best practices in implementing data privacy legislation from the perspective of both legislators and controllers.



The visit aimed to be a peer-to-peer learning opportunity to share knowledge and experiences regarding the establishment and implementation of national data protection and privacy legislations.

The specific objectives were :

- to share experiences with counterparts in Mauritius on the implementation of a data protection legislation;
- to understand the magnitude of financial, human and other resources required by a country to implement data protection legislation;
- to establish strategic and technical partnerships to foster continuous peer learning and sharing of ideas;
- to document key best practices and lessons to be considered by the ICT Committee when scrutinizing the Data Protection and Privacy Bill in Uganda.



A delegation of 10 members comprising of the ICT Committee of the Ugandan Parliament, National Information Technology Authority (NITA) , Ministry of Justice and Constitutional Affairs (FPC), Pulse Lab Kampala and UN Global Pulse participated in the benchmarking trip.

III. Data Protection Africa Summit

Africa Digital Rights’ Hub organised a Data Protection African Summit in Mauritius from 19 to 23 November 2018. The theme of the Summit was “Breaking New Frontiers”.

The Summit brought together controllers, processors, tech companies, policymakers, regulators, innovators, business communities and individuals together to discuss and proffer solutions to the emerging issues on data protection and privacy. The main objectives of the Summit were to –

- (a) influence the development of relevant national and regional frameworks for data protection;
- (b) build industry capacity to ensure data protection compliance on the Continent;
- (c) formulate key lessons and issues for advocacy;
- (d) explore issues for regional cooperation and collaboration between African regulators, policymakers and their counterparts in the rest of the world; and
- (e) showcase tools for data protection compliance.



The Data Protection Commissioner made an opening speech and has chaired the focus group discussion on “African dialogue on the harmonisation of Data Protection Laws” with participants during the workshop.



The Data Protection Commissioner has played a supporting role in making this event happen in Mauritius to position Mauritius on the African Continent in the field of data protection.

IV. Enforcing Data Protection

The Data Protection Office is entrusted with the power to investigate complaints for any alleged contravention of the DPA 2017. This serves as an effective deterrent for any non-adherence and also provides remedy to an aggrieved individual where an offence is being or has been committed. Once a complaint is registered with the office, an enquiry is initiated unless the Data Protection Commissioner is of the opinion that the complaint is frivolous or vexatious. At the end of an enquiry, the Data Protection Commissioner provides a decision on the case. In case an amicable resolution by the parties concerned of the complaint cannot be settled within a reasonable time, the individual who made the complaint is informed about the decision so that the individual may, where he considers that he is aggrieved by the decision, appeal against it under section 51 of the DPA. The office may also try an offence under this act at the Intermediate Court after the Director of Public Prosecutions has given his consent.

a) Investigation on Complaints

During the period of January to December 2018, the Data Protection Office has received a total of 20 new complaints for investigations on the below subjects, among others:

- Unauthorised use of CCTV Camera
- Unlawful disclosure of personal Information
- Unauthorised access to personal data
- Anonymisation of published report

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

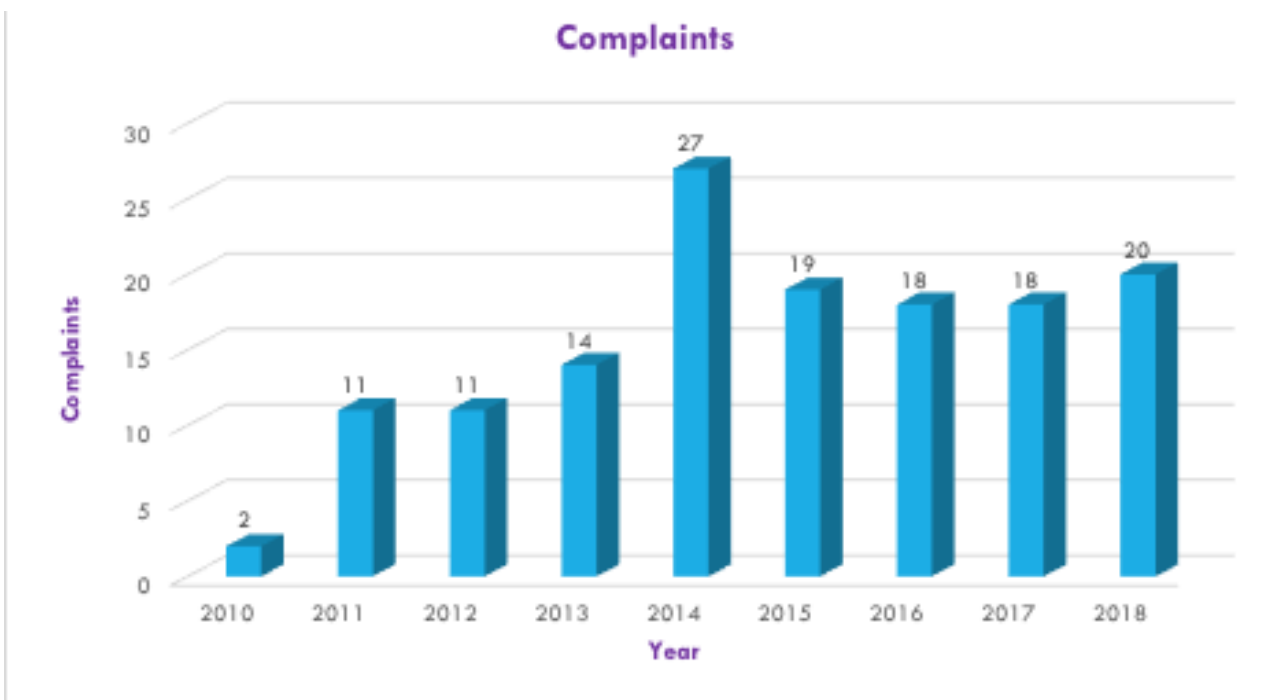


Figure 3: Number of new complaints per year

This office carried 3 site visits for investigation purposes subject to the availability of police officers to accompany DPO officers onsite.

b) Decisions on Complaints

The decisions of the Data Protection Commissioner (DPC) contribute in protecting the privacy rights of our citizens and are seen as an effective deterring measure in avoiding the reoccurrence of such breaches. The DPC has provided 5 decisions in 2018. This office has requested 2 legal executives to assist the Commissioner but the delays in prescribing the scheme of service has hampered the recruitment of these officers. Currently, the Commissioner is providing decisions on all cases in solo which is time consuming and the recruitment of legal executives is important to streamline operations in this area.

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 issues of site visits, human resources and setting up of a prosecution unit raised during the year 2017 were still outstanding in 2018. These have influenced negatively the progress of investigation on complaints.

A brief of the decisions are provided below:

- [Decision No 47 - 17.09.2018 – Complaint on alleged monitoring and/or automatic copying of emails](#)

The data protection issue is whether there has been an alleged monitoring and/or automatic copying of the emails sent by Complainant to Respondent Head Office without the consent of the former.

A site visit was undertaken by this office at the premises of Respondent to investigate on how the Cluster Manager and the Country Controller became aware of the email sent by Complainant to Respondent regional office on 14th October 2016. The laptops of both the Cluster Manager and the Country Controller were verified and it was observed that the Mauritius HR Executive (who was in copy of the said email) received Complainant's email on Friday 14th October 2016 at 10:16 a.m. and then the Mauritius HR Executive forwarded the said email to the Cluster Manager and Country Controller on the same day at 10:19 a.m.

Evidence regarding the forwarding of the email was submitted during the site visit.

The findings of the enquiry have also revealed that Respondent has appropriate organisational measures in place such as End User Security Policy and the Email/Internet Guide. Moreover, staff is required to sign an acknowledgement note that they have read and understood these policies.

After careful perusal of the investigation carried out, no evidence of any such breach was detected in order to reach the conclusion that an offence under the Data Protection Act has been committed.

Respondent has also satisfied this office that it has appropriate security and organisational measures to protect the processing of personal information within the company. However, Complainant's termination of employment based on her performance was found to be a suitable case under the Employment Rights Act and not within the jurisdiction of this office.

- [Decision No 48 - 27.09.2018 – Complaint on illegal access to personal data](#)

In view of the enquiry, it was clear that no breach had occurred under the Data Protection Act and as such the enquiry was closed to the satisfaction of all parties concerned.

- [Decision No 49 - 18.10.2018 – Complaint on alleged unauthorised access to Complainant's personal Dropbox account](#)

After careful analysis of the evidence of record and the detailed explanations provided by Respondent, no breach of the Data Protection Act was detected by this office. Should Complainant have come forward with more concrete proof regarding any unauthorised use of personal data by Respondent, the Data Protection Commissioner would have been in a better position to determine whether any potential breach could indeed have taken place. Therefore, the enquiry was closed.

- [Decision No 50 - 19.10.2018 – Complaint on use of CCTV Camera](#)

This enquiry was closed since Complainant had informed that he did not intend to lodge a formal complaint to this office.

- [Decision No 51 - 17.12.2018 – Complaint on alleged disclosure of students ' private information on Respondent's website](#)

Corrective measures have been duly implemented by Respondent as per the recommendations of this office and to the satisfaction of all parties. The enquiry is thus closed and no offence has been found proven under the Data Protection Act. However, should Respondent have acted diligently regarding the queries from this office, this enquiry would have been completed in a lesser period of time.

V. Improving legal protection

Under section 58 of the Data Protection Act, any person aggrieved by a decision of the Commissioner in respect of the performance of her duties and powers under the Data Protection Act shall have a right of appeal within 21 days from the date when the decision is made known to that person to the Tribunal.

a) ICT Appeal Tribunal

The ICT Appeal Tribunal has set aside an appeal made by an appellant against the Data Protection Office on the decision to refer the matter to the Police in March 2018.

b) Supreme Court

The appellant above has appealed to the Supreme Court on the determination of the ICT Appeal Tribunal in March 2018 and this office has resisted the appeal through the representative of the State Law Office. The case is still pending at the Supreme Court.

c) Industrial Court

This office was called as a witness in a case where an employee was dismissed by a controller for refusing to give his fingerprint for attendance. The case was settled in court in June 2016 against payment by the controller to the said employee.

VI. Registration of Controllers

This office has received a total of four hundred and ninety three (493) applications comprising of new registrations in 2018. Alongside renewals for the previous years, a total of **32692** applications have been processed.

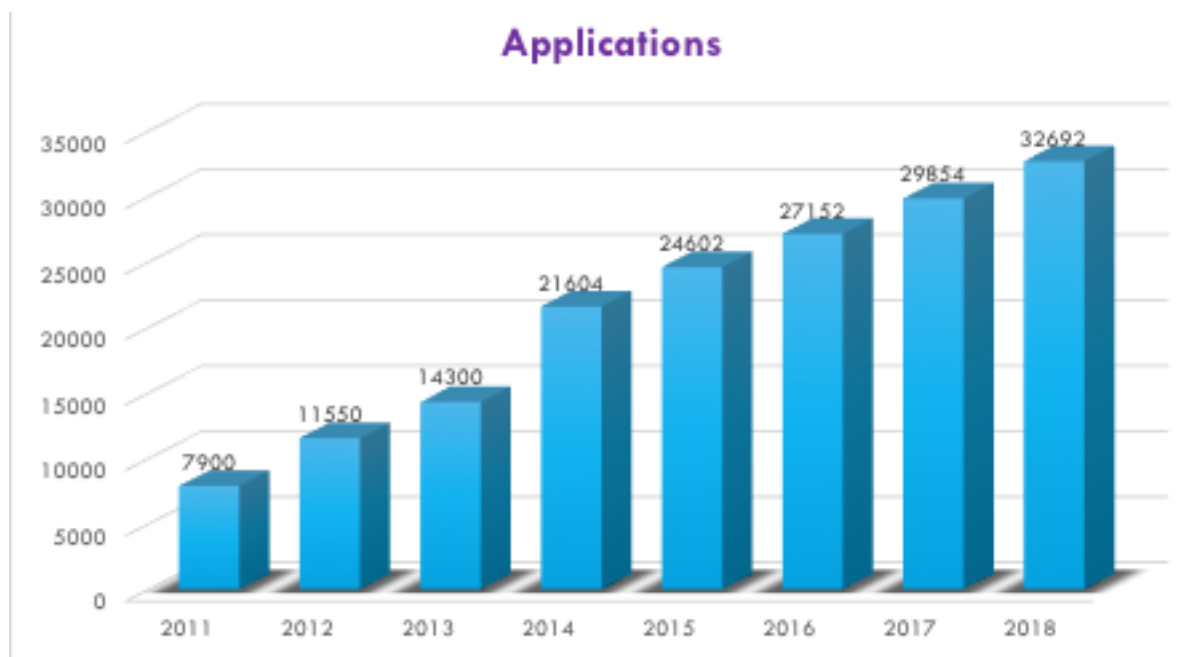


Figure 4: Cumulative Registrations & Renewals of Controllers

VII. Requests for legal advice

In 2018, this office received a phenomenal number of requests for advice from both the public and private sector due to the coming into force of the new Act and the growing awareness of individuals on the right to privacy and data protection.

Many requests concerned the following aspects of the DPA:

- Overview of the DPA
- The role of Data Protection Officer
- Transfer of data abroad
- Cloud computing
- Consent
- Exemption
- Registration and renewal fees
- Pseudonymisation and encryption
- EU adequacy
- Mobile data

A total of two hundred and seventy two (272) written requests for advice comprising of 210 from private bodies and 62 from ministries, governmental departments and parastatal bodies were received.

Total Number of Requests

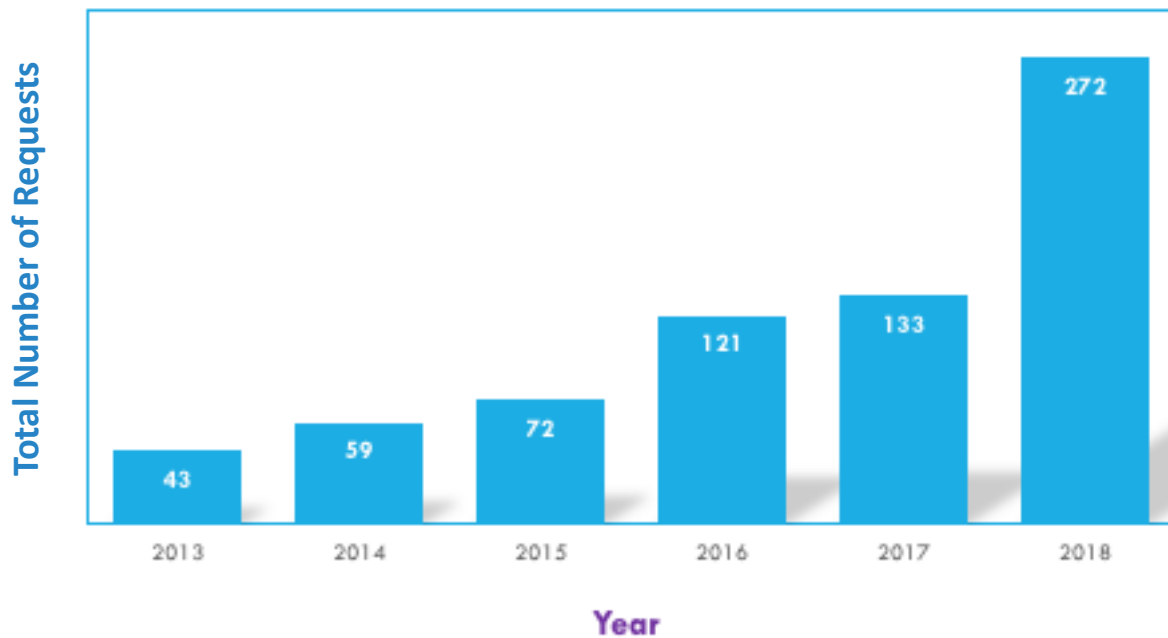


Figure 5: Number of requests for advice

The office has also received a remarkable number of phone calls for information on the DPA 2017 and registration procedures. Indeed, this has been a very tedious year since everybody was looking at the office for answers whilst on the other hand, the office was barely having the human resources to cope with the outburst of requests.

Attending a request takes time because it involves analysis and research on the legal aspects, technical aspects and knowledge of the business sector. However, with only a handful of officers and absence of legal executives, it was hectic to attend to requests emanating from the diverging sector and the public. Privacy is a right that affects each and every individual in Mauritius including business operators. The office also had the huge challenge to keep pace and self train itself with the new requirements and concepts introduced in GDPR and DPA 2017 and simultaneously train and advise other organisations in a short span of time.

In addition, the office received business sector queries from associations regrouping requests from all its members in the relevant sector. The drafting of advice proved to be time-consuming during 2018 again because of limited resources available at the office.

VIII. Advisory Role / Stakeholder in Projects

The Data Protection Office plays an advisory role in the implementation of many government projects involving the processing of personal data such as the Info Highway Project, Safe City Project, Smart Mobile Apps, National Disaster Cyber Security and Cybercrime Committee, Trade in Services Agreement (TISA), China-Mauritius Free Trade Agreement, amongst others. Participation in these projects consume considerable amount of time due to the analysis of voluminous documents submitted by the stakeholders involved.

Moreover, the Data Protection Office is a stakeholder in the Online Citizen Support Portal and the Mauritian Cybercrime Reporting System (MAUCORS).

IX. Modernised Convention 108

Mauritius has ratified, since 17 June 2016, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as “Convention 108” and its Additional Protocol which is the only international legally binding instrument dealing explicitly with data protection.

On 18 May 2018, the 128th Ministerial Session of the Council of Europe’s Committee of Ministers adopted the Protocol amending the Convention 108, now known as the ‘Modernised Convention 108’.

Subsequently, this office studied the Modernised Convention 108 during 2018 and requested our parent Ministry to initiate the process for the signing of the Modernised Convention 108.

X. New forms designed with respect to requirements of DPA 2017

As soon as the Data Protection Act was proclaimed in January 2018, this office had the underpinning tasks of carrying research to design the required forms and templates to meet the requirements of the new Act. The following new forms and templates have been designed by this office during the year 2018:

a) High Risk Processing Operations

The new Data Protection Act 2017 has imposed on controllers and processors the legal obligation to perform a Data Protection Impact Assessment (DPIA) for processing operations that may result in high risks to the rights and freedoms of individuals. This obligation is also found in the General Data Protection Regulation (GDPR).

The Data Protection office has published a document on its website to assist controllers and processors to better understand when a processing operation is likely to constitute “high risk”.

The criteria used to evaluate high risk processing, whilst not definitive, provides greater insight to controllers and processors in their daily operations.

b) Data Protection Impact Assessment (DPIA) Form

A DPIA is a recommended privacy by design practice undertaken for processing operations likely to present high risks to individuals. It helps to identify privacy risks, foresee problems and bring forward solutions prior to any envisaged processing. It thus serves as an assessment tool to decide whether the security measures in place in an organisation are adequate compared to the risks to individuals and whether the necessity of an envisaged processing operation does not outweigh the rights and freedoms of individuals.

In 2018, the Data Protection Office published a DPIA form which controllers and processors can use in order to carry out a DPIA assessment. This office also issued an add-on guide explaining controllers and processors how to complete each section of the DPIA form.

c) Personal Data Breach Notification Form

Once a personal data breach occurs, a controller must complete the Personal Data Breach Notification Form available on the website of this office and submit it to the Data Protection Office within a timing delay of 72 hours after having become aware of the incident. The emphasis is on swift containment and recovery from a personal data breach. Every effort should be taken by controllers to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

d) Controller and Processor Registration/Renewal Forms

All controllers and processors must register with the Data Protection Office. During 2018, the office drafted the required new forms for registration and renewal of controllers and

processors as per the requirements of the Data Protection Act 2017. However, the forms will be published on the office website once the new “Data Protection Regulations” come into force. A draft Regulation has already been prepared by this office and submitted to our parent Ministry. The office has also been involved in discussions with our parent Ministry and the Ministry of Finance and Economic Development regarding the new quantum of fees for registration and renewal.

This regulation has taken quite a considerable amount of time to be prescribed which this office is awaiting in order to apply the new provisions of part III of the Data Protection Act.

e) **Transfer of Personal Data Form**

In line with section 36(1) of the Data Protection Act 2017 for transfers of personal data outside Mauritius, this office has updated the ‘Transfer of Personal Data’ form available on the website of this office to enable a controller or processor to submit the types of safeguards implemented by the latter to protect personal data.

Upon submission of the form, this office makes an assessment of the safeguards implemented and provides an advice to controllers/processors regarding the transfer of data.

f) **Records of Processing Template**

According to section 33, every controller or processor has to maintain a record of all processing operations under his responsibility. This office has published an excel sheet template on its website which controllers and processors can use to document their records of processing operations as it is a mandatory requirement of the Data Protection Act. The template also contain a sample sheet where some records have been filled for further assistance.

g) **Certification**

This office has drafted the processes for certification which is being reviewed. The concept of certifying data processing operations is a significant development in creating a reliable and auditable framework for data processing operations. Certification mechanism is voluntary and is a way of demonstrating that controllers and processors are implementing technical and organisational measures. A certificate will be issued by this office as the certifying body, which will be renewable after a period of 3 years.

XI. Personal Data Breach Notification

This office has received 11 data breach notifications from the private sector together with the duly filled breach notification forms. Recommendations on measures to be taken have been advised by this office. Analysis of the various breaches received so far has confirmed that email phishing attacks, employee wrong usage of emails, business email compromise and disposal of confidential document are among the various causes of potential breaches.

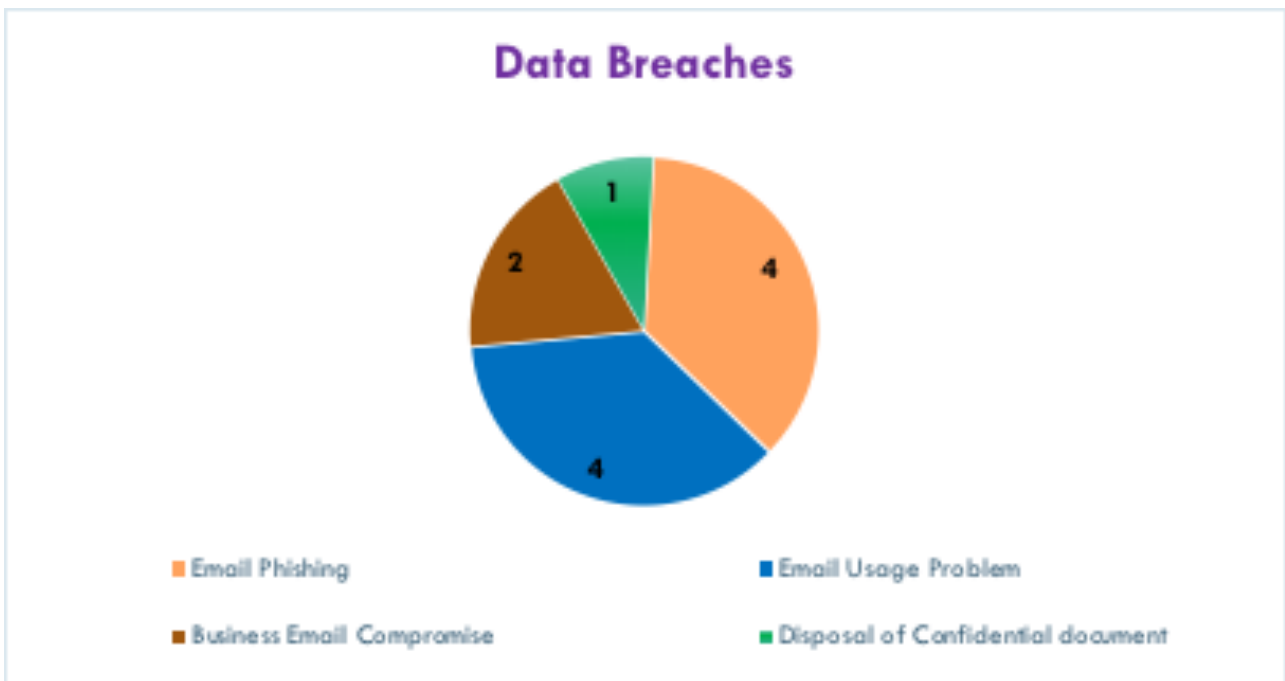


Figure 6: Data breaches by Categories

XII. Transfer of Data Abroad

The Data Protection Commissioner granted authorisation to nineteen (19) companies to transfer data outside Mauritius based on appropriate safeguards under section 36 of the DPA 2017.

XIII. Other achievements

a) **MS ISO 9001:2015**

The ISO 9001:2008 certificate has expired on 14 September 2018. This office is preparing to be certified again under the new ISO 9001:2015 standard. We also have the assistance of a facilitator. The documentation have been reviewed and new processes have been worked out to reflect the changes in the Data Protection Act 2017. This office will apply for certification again after internal audits have been carried out in early 2019. The customer charter has been updated in line with the Data Protection Act 2017 to reflect new functions.

The lack of staff has prevented this office to timely migrate to the new ISO 9001:2015 standard because of high loads of work to be finalised for this transition to take place. The priority was

to focus on the implementation of the different functions of the new Data Protection Act.

b) Computerisation

The computerisation project implemented has been criticised by the National Audit Office in their 2017-2018 report because of the delays in operations. The online registration and renewal though tested during the user acceptance phase has not been activated due to a problem of data entry backlog which existed in the old system. The Ministry decided to clear the backlog through outsourcing the data entry work for a period of 5 months. After clearing of the backlog, online application and payment will be operational in the application.

Due to the changes brought by the Data Protection Act 2017, changes have to be reflected in the new computerised application to include new functionalities. The approval to authorise the implementation of those changes is being awaited from the parent Ministry.

c) Information Security Management System (ISMS)

The Data Protection Office embarked on the implementation of an information security management system using the ISO 27001:2013 standard in order to demonstrate that information security risks are being adequately managed within the office. During 2018, the office completed the following tasks:

Definition of the scope of the DPO's Information Security Management System

Definition of the objectives and risk treatment plans

Drafting an information security policy

The office also carried out 3 internal audits and a management review meeting.

However, due to shortage and constant turnover of staff and priority on other underlying tasks and functions to be carried out, the office still has to complete the elaboration of all controls, after which the office can apply for certification.

d) Forensics

This office has acquired the forensic tool in 2018 and the tools have been commissioned. Training was given to data protection officers and technical officers of the Central Information System Division (CISD). Officers will have to be acquainted with the software. This will allow the office to be better equipped to face the situation of gathering forensic evidence whenever the case arises.

e) Capacity building provided to officers of this office

Officers attended the following trainings during the year 2018 to improve the performance and effectiveness of the functions carried out by this office:

DATE	TITLE	ORGANISED BY
22-24 January 2018	Harmonization of legislation on cybercrime and electronic evidence	Attorney General's Office
26-Jan-18	Advisory Mission on the streamlining of procedures for Mutual Legal Assistance related to cybercrime and electronic evidence under the GLACY + project	Attorney General's Office
06-Feb-18	Safer Internet Day 2018	National Computer Board
15-Mar-18	Launching of Mauritian Cybercrime Online Reporting System and ITU Cyber Drill for Top Management Officials	CERT- MU
22-23 March 2018	Workshop on Compliance with the new DPA 2017	Geroudis Law Firm
26-27 March 2018	Internal Auditor Course on 9001:2015	Mauritius Standards Bureau
25-26 April 2018	Workshop on Open Data	National Computer Board
30-Apr-18	Leadership Excellence Workshop	Foxwire Communications
18-May-18	Workshop on the National Code of Corporate Governance for Mauritius	Ministry of Financial Services and Good Governance
07-Jun-18	Validation Workshop on Digital Strategies	Ministry of Technology, Communication and Innovation
09-Aug-18	Data Protection and GDPR Event	Baker Tilly & Mauritius Telecom
01-02 October 2018	Workshop on Open Licensing - Open software - Open content - Open data	Ministry of Technology, Communication and Innovation
25-Oct-18	Workshop on the EU General Data Protection Regulation (GDPR)	Financial Services Commission
28-30 November 2018	World AI Show 2018 and World Blockchain Summit 2018	Ministry of Technology, Communication and Innovation
17-Dec-18	Workshop for the Launching of Digital Mauritius 2030 Strategic Plan, Digital Government Transformation Strategy 2018-2022	Ministry of Technology, Communication and Innovation

Despite the acute human resource problem, this office tried as far as possible to designate at least one officer to attend trainings whenever the exigencies of this office permitted so.

PROJECTS IN PIPELINE

I. Guide on data protection and media

During 2018, the Data Protection Office started drafting a guide titled 'Data Protection and the Media'. The purpose of the guide aims at safeguarding the privacy of public figures and private persons and it 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 Data Protection Act (DPA) 2017 and best practices. It. The guide is expected to be completed by early 2019.

II. Audio visual clips

This office has decided to produce a corporate film on the Data Protection Office and a training toolkit to be produced on DVDs which will be distributed to controllers on the Data Protection Act. This will allow a more efficient way of training a large number of controllers/processors. Several working sessions were held with the Mauritius Film Development Corporation. Training materials were prepared and shootings and recordings were carried out.

