African and International Perspective on Data Protection

Mrs. D. Madhub
Data Protection Commissioner
Data Protection Office

30 January 2023
Leadership is not about size

It's about knowledge & wisdom
10 Reasons Why Privacy Rights are Important
<table>
<thead>
<tr>
<th></th>
<th>Privacy Rights prevent the government from spying on people (without cause)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Privacy Rights keep organisations from using personal data for their own goals</td>
</tr>
<tr>
<td>3</td>
<td>Privacy Rights help ensure those who steal or misuse data are held accountable</td>
</tr>
<tr>
<td>4</td>
<td>Privacy Rights help maintain social boundaries</td>
</tr>
<tr>
<td>5</td>
<td>Privacy Rights help build trust</td>
</tr>
<tr>
<td>6</td>
<td>Privacy Rights ensure we have control over our data</td>
</tr>
<tr>
<td>7</td>
<td>Privacy Rights protect freedom of speech and thought</td>
</tr>
<tr>
<td>8</td>
<td>Privacy Rights let you engage freely in politics</td>
</tr>
<tr>
<td>9</td>
<td>Privacy Rights protect reputations</td>
</tr>
<tr>
<td>10</td>
<td>Privacy Rights protect your finances</td>
</tr>
</tbody>
</table>
Data Privacy Trends in 2023
Global rise in data privacy regulations

Companies will invest more in privacy technologies

A cookieless future

Greater transparency in the collection and processing of personal data

Increase in requests and complaints of data subjects

More data security and privacy job positions
1. Global rise in data privacy regulations

The global rise in data privacy regulations will continue to rise in 2023. By the end of 2024, it is expected that 75% of the global population will have its personal information covered under privacy regulations.

2. Companies will invest more in privacy technologies

Privacy-enhancing technologies took the center stage in 2022 and will continue to rise in 2023. In 2019 Google launched Privacy Sandbox and is currently working on Trust token API and other privacy technologies to replace third-party cookies. In 2021–2022, big tech companies were charged with multi-million fines for the GDPR breaches. The total amount of fines appointed on Meta alone until the end of 2022 by the Irish Data Protection Commission for breaching the GDPR and ePrivacy Directive seeks nearly €1 billion. In addition, the Irish Data Protection Commission also has 40 open inquiries for other big tech companies. This tendency will continue in 2023, and we should see more companies charged with big fines for breaches of privacy regulations, especially the European ones.

Source: https://cookie-script.com/blog/data-privacy-trends-in-2023
3. A cookieless future

Google has announced that by the end of 2023, it will officially stop supporting Third-Party Cookies on the Google Chrome browser. The trend will continue for removing cookies in favor of consent-based data-collecting solutions.

4. Greater transparency in the collection and processing of personal data

User privacy survey shows that website users value data privacy, and over 50% of them would change service providers simply because of their data policies or data sharing practices. The trend will continue in 2023.

5. Increase in requests and complaints of data subjects

Data subjects of the privacy regulations are becoming more aware of their rights and want to protect their personal information. As data subjects continue to exercise their right to know, update, delete, or otherwise handle the personal information businesses have collected about them, this will follow by a significant increase in data subject requests and complaints in 2023.
6. More data security and privacy job positions

Increasing and changing privacy regulations worldwide will lead to more data security jobs for humans in the coming year. The increase in related jobs in recent years dispels the myth that Data Science and Artificial Intelligence replace human labor.

Source: https://cookie-script.com/blog/data-privacy-trends-in-2023
Mar 2021
533,000,000 records lost. Phone numbers, full names, locations, email addresses and biographical information on 533 million users from 106 countries. Scraped due to vulnerability “patched in 2019”

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Data Breaches exceeding 15,000,000 records lost

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Data Protection and Privacy

- 137 out of 194 countries had put in place legislation to secure the protection of data and privacy.

- Africa and Asia show different level of adoption with 61 and 57 per cent of countries having adopted such legislations.

- The share in the least developed countries is only 48 per cent.

Guiding Principles

1. Global interoperability
2. Collaboration
3. Ethics
4. Privacy impact
5. Anonymity and pseudonymity
6. Data minimization
7. Choice
8. Legal environment
9. Technical environment
10. Business environment

Source: Privacy and Personal Data Protection Guidelines for Africa
Key Considerations

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Source: Privacy and Personal Data Protection Guidelines for Africa
Existing Privacy Laws and Frameworks in Africa

- ECOWAS Supplementary Act A/SA.1/01/10 on personal data protection (2010)
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)
- Privacy & Personal Data Protection Guidelines for Africa
- African Union Continental Data Policy Framework
- The Digital Transformation Strategy for Africa (2020-2030)
- African Continental Free Trade Area (AfCFTA) agreement
European Union (EU)

The Evolving Landscape of European Data Privacy Laws

- General Data Protection Regulation (GDPR)
- Data Governance Act (DGA)
- ePrivacy Directives
- ePrivacy Regulation
- Digital Markets Act
- Digital Services Act
- The Draft Data Act
- European Health Data Space (EHDS)
- Artificial Intelligence Regulation
Council of Europe (CoE)

Ratification of Mauritius to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) which came into force on **01 October 2016**.

Ratification of the Protocol amending Convention for the Protection of individuals with regard to automatic processing of personal data on **04 September 2020**.

Source: https://www.pinterest.com/
United Nations

- United Nations International Covenant on Civil and Political Rights
- Universal Declaration of Human Rights
- UN Principles on Data Protection and Privacy
- UN Reports of the Special Rapporteur on the Right to Privacy
- Guidance Note on Data Privacy, Ethics and Protection for the United Nations Development Group (UNDG)
- UNESCO’s Principles on Personal Data Protection and Privacy
- United Nations High Commission on Human Rights’ resolution on The Right to Privacy in the Digital Age

Source: https://www.worldatlas.com/
American Data Privacy and Protection Bill, California Privacy Rights Act (2020), Consumer Data Protection Act (Virginia), Utah Consumer Privacy Act (UCPA), Connecticut Privacy Act, Colorado Privacy Act, (CPA), Children’s Online Privacy Protection Bill

United Kingdom

• Data Protection Act 2018
• Online Safety Bill

China

• Personal Information Protection Law (PIPL)

India

• Digital Personal Data Protection Bill 2022

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Main Achievements of the Data Protection Office

Revenue Collected

DPO collected a total revenue of **Rs 11,741,500** in 2021 and **Rs 2,736,500** for registration of controllers and processors in 2022.
European Union Adequacy

In conjunction with the adequacy requirements established by the European Union, the office prepared and submitted a report to the European Commission (EC) Directorate for its study and perusal with a view to a subsequent adequacy finding for Mauritius. The report aims to provide an overview of the Mauritian system in order for the EC to conduct an objective assessment.
Enforcing Data Protection Statistics 2021 – 2022

Number of controllers registered: 14,571
Number of processors registered: 701
Statistics & Nature of Cases/Complaints

For the year 2021 to October 2022, 135 complaints have been received at the DPO. Out of the 135, 34 complaints have been resolved. 101 complaints are still ongoing which are classified as per table below:

<table>
<thead>
<tr>
<th>Nature of Complaint</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV Cameras</td>
<td>125</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>1</td>
</tr>
<tr>
<td>Unlawful Disclosure of Personal Data</td>
<td>8</td>
</tr>
<tr>
<td>Rights of Data Subject Access</td>
<td>1</td>
</tr>
</tbody>
</table>
THE FUTURE

A call for Global Privacy Standards

Source: https://www.videezy.com/
Artificial Intelligence
SETTING THE RIGHT EQUILIBRIUM
Thank You
For
Your Attention…

Source: https://www.videezy.com/
E-DPO Explained

Mr R. Mukoon

Data Protection Officer/Senior Data Protection Officer

Data Protection Office

30 January 2023
eDPO Explained

https://dpo.govmu.org
Option 1
Individual with BRN or no BRN. Requires a Maupass Account

Option 2
Societe, Trust, NGOs and Ministries having or not having a BRN through Representative(s)

Option 3
Register controllers/processors under his management through Representative(s)

Option 4
One company and/or other companies through Representative(s)
Concepts in eDPO Portal

Administrator account other than Individual (3 types)

- Must add its representative(s) under Manage Representatives menu
- The representative must have a Maupass account

Representative

- Must log in with its Maupass Account
- It is the representative who register controller/processor on behalf of the Administrator (3 types)
- Submit the Eforms for a controller/processor
Concepts in eDPO Portal

Administrator account other than Individual (2 types)

- Management Companies and Group of Companies
- Add controller/processor (Manage Organisations)
Administrator and Companies(s)

3. Management Companies

Must add (Manage Organisation menu)

Controller/Processor

4. Group of Companies
Administrator and Representative(s)

2. Organisations
3. Management Companies
4. Group of Companies

Must add

Representative(s)
Misconceptions in eDPO Portal

Log in as Administrator account other than Individual (3 types) Scenario

- This account cannot submit controller forms
- Neither submit eForms
- Can view controller(s)/processor(s), Eforms and its status

Solution to the above scenario?

- The representative must log in with its Maupass Account
- It is the representative who register controller/processor on behalf of the Administrator
- Submit the Eforms for a controller/processor
Controller/Processor form
Fill and Submit

Make Payment using the modes available: Cash, Cheque, Voucher, Epayment

Vetting by DPO
Request for Amendment if required
Approve and Certificate generated

View Status / Certificate(s) in your Portal (Administrator/Representative)
### Epayment

#### DRAFT APPLICATIONS

No records found.

#### PENDING FEES

<table>
<thead>
<tr>
<th>Click to Pay</th>
<th>DPO/2022/09/0091</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New Controller for LTD</td>
</tr>
<tr>
<td></td>
<td>Amount: 1000.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Click to Pay</th>
<th>DPO/2022/09/0082</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New Controller for Ltd</td>
</tr>
<tr>
<td></td>
<td>Amount: 1000.00</td>
</tr>
</tbody>
</table>

#### REGISTERED CERTIFICATES

- **C10020**
  - Controller for limited
  - View Certificate

- **C10021**
  - Controller for CO LTD
  - View Certificate

- **C10022**

### Home

- register New Controller
- register New Processor
- renew Application
- controller
- Processor
- Query Complaints
- transactions
## Sample Portal View (status/certificate)

<table>
<thead>
<tr>
<th>Reference</th>
<th>Application Type</th>
<th>Controller Name</th>
<th>Representative Name</th>
<th>Status</th>
<th>Edit</th>
<th>Application</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPO/2022/08/0004</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/08/0001</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Application Submitted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/09/0031</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/10/0101</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>In Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/08/0019</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/09/0033</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/10/0105</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/10/0107</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/10/0106</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO/2022/10/0108</td>
<td>Controller</td>
<td>[redacted]</td>
<td>[redacted]</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Status of Application in eDPO portal

- **Completed**: Indicates application has been fully processed and Certificate has been generated.
- **Submitted**: Indicates Application has been submitted to be vetted by the DPO.
- **Awaiting Payment**: Applicant need to pay the Registration or Renewal Fee for Application.
- **In Process**: Application is being processed at the DPO.
- **Awaiting Amendments**: Application was sent back to applicant on the portal to make necessary amendments. Applicant will receive a mail with all information that need to be amended, and have to re-submit application once completed.
- **Rejected**: Application has been rejected by the DPO and no certificate generated.
Complaint in eDPO portal
Complaint Status in eDPO portal

▷ **Draft:** The complaint is still at the level of complainant and not yet submitted.

▷ **Submitted:** Indicates that the complaint has been submitted to the DPO.

▷ **In Process:** The complaint is being processed at the DPO.

▷ **Closed:** The complaint is closed and the applicant has been notified.
Eforms in eDPO portal
Action Required from DPO

To submit Records of Processing report updated version.
Eforms Status in eDPO portal

▷ **Draft:** The Eform is still at the level of the applicant and is not yet submitted.

▷ **Submitted:** Indicates that the Eform has been submitted to the DPO.

▷ **In Process:** The Eform is being processed at the DPO.

▷ **Action Required:** as explained previously

▷ **Action Completed:** the required action action requested by DPO

▷ **Approved:** The eform is approved

▷ **Rejected:** The eform is rejected
## Eform status in eDPO portal

<table>
<thead>
<tr>
<th>Reference</th>
<th>Category</th>
<th>Submitted Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT/2022/14</td>
<td>Certification Form</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/10</td>
<td>Data Protection Impact Assessment</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/15</td>
<td>Certification Form</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/16</td>
<td>Certification Form</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/19</td>
<td>Notification of Personal Data Breach</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/5</td>
<td>Transfer of Personal Data Abroad</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/25</td>
<td>Data Protection Impact Assessment</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>DRAFT/2022/27</td>
<td>Data Protection Impact Assessment</td>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td>BREA/2022/7</td>
<td>Notification of Personal Data Breach</td>
<td>28/11/2022</td>
<td>Action Completed</td>
</tr>
<tr>
<td>DPIA/2022/2</td>
<td>Data Protection Impact Assessment</td>
<td>28/11/2022</td>
<td>In Process</td>
</tr>
</tbody>
</table>
User Guide

for

Dpo Portal

for the

Data Protection Office

(Version No. 5.0)
Data Protection in the Telecommunications Sector

Mr. D. C. NG Sui Wa

Chairperson
Information and Communication Technologies Authority

30 January 2023
The role and mandate of the National Cybersecurity Committee

Dr. V. Padayatchy
Chairman
National Cybersecurity Committee

30 January 2023
CONFERENCE ON
“PROTECTING PERSONAL DATA ACROSS ALL ECONOMIC SECTORS”

30TH January 2023

The role and mandate of the National Cybersecurity Committee

*Presented by: Dr Viv Padayatchy*

*Chairman, National Cybersecurity Committee*
The new legislation in place

LEGAL SUPPLEMENT

567

to the Government Gazette of Mauritius No. 173 of 24 November 2021

THE CYBERSECURITY AND CYBERCRIME ACT 2021

Act No. 16 of 2021

54. Repeal

The Computer Misuse and Cybercrime Act is repealed.
• A multi-stakeholder body with representatives from key government agencies, private sector and civil society

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr Viv Padayatchy</td>
<td>Chairperson</td>
</tr>
<tr>
<td>Mr R.Howabhay</td>
<td>Chief Technical Officer, Ministry of Information Technology, Communication and Innovation</td>
</tr>
<tr>
<td>Mrs. D.Madhub</td>
<td>Data Protection Commissioner</td>
</tr>
<tr>
<td>Mr C.Dawonauth</td>
<td>Superintendent of Police</td>
</tr>
<tr>
<td>Dr K.Usmani</td>
<td>Officer in Charge</td>
</tr>
<tr>
<td>Mr J.Louis</td>
<td>Officer in Charge</td>
</tr>
<tr>
<td>Mr J.A Ismael Ghanty</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>Mr Arvind Jadoo</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>Mr Pravesh Gaonjur</td>
<td>General Manager, Tylers</td>
</tr>
<tr>
<td>Mr Amreesh Phokeer</td>
<td>Internet Measurement and Data Expert</td>
</tr>
<tr>
<td>Mrs P.Sohun</td>
<td>Deputy Permanent Secretary, Prime Minister's Office</td>
</tr>
<tr>
<td>Mr A. Auckloo</td>
<td>Technical Security Analyst, Cyber Terrorism Unit</td>
</tr>
<tr>
<td>Mr M.Seetaram</td>
<td>Ag Senior Assistant Parliamentary Counsel</td>
</tr>
</tbody>
</table>

Copyright Data Protection Office
The Committee may co-opt any person who may be of assistance in relation to any matter before it.
Advisory

(a) advise the Government on cybersecurity and cybercrime;

The committee draws on its pool of resources and discuss cybersecurity matters. Government may refer matters for consideration by the committee or the committee may bring matters to the government’s attention via the Minister of ICT.
• implement Government policy relating to cybersecurity and cybercrime;

The committee may implement policy via its constituent agencies. However, the committee does not itself have any human or material resources outside its committee members.
Coordination

• coordinate all matters relating to cybersecurity and cybercrime;

Coordination is achieved by concertation between members either during a meeting or online discussions
Reporting

• receive and act on reports relating to cybersecurity and cybercrime;

The committee may receive reports either via its members or any other party who which to bring such matters to the committee’s attention
• coordinate and facilitate the implementation of a critical information infrastructure protection framework;

A critical information structure, from a cybersecurity viewpoint, is a set of information assets, systems, and processes that are considered essential to the operation and survival of the country.

This includes sensitive data, intellectual property, key infrastructure, and systems that are necessary to meet business objectives. In the context of cybersecurity, protecting the critical information structure is a top priority to prevent data breaches, unauthorized access, and other types of cyber attacks.

Examples:
- Telecommunication
- Port & Airport
- Health services
- Power Generation and Distribution
- Water collection, treatment and distribution
- etc
Information Aggregation

• coordinate the collection and analysis of internal and external cyber threats, and response to cyber incidents that threaten the Mauritian cyberspace;
Local and International Collaboration

• cooperate with computer incident response teams and other relevant bodies, locally and internationally, on response to cyber threats and cybersecurity incidents;

CERT-MU is a key member of CC and is an active participant.

The CC actively seek collaboration with other local and international bodies to fight Cyber Crime.
• establish cybersecurity best practices and standards for critical information infrastructures;

CC work on selecting best practices such as ISO27001 protocols for CII
• promote capacity building on the prevention, detection and mitigation of cyber threats;

CC aim to promote the development of local Cybersecurity expertise via collaboration with training institutions and local organisations involved in the field of cybersecurity.
The Committee starting its work in September 2022
Meeting every 2-3 weeks
4 meetings held
Excluding confidential matters discussed, the committee has:
  • Reviewed and gave its input on the national cybersecurity strategy
  • Reviewed the Maushield Platform
  • Reviewed the National Cyber incident response plan and simulation exercises
  • Started work on the CII Framework
  • Planning an event on Cybersecurity
The end

Thank you!
Data Protection in the Mauritian Business Community

Ms. A. Radhakeesoon
Chairperson
National Committee on Corporate Governance (NCCG)

Mrs. S. Ujoodha
CEO Mauritius Institute of Directors (MIoD)

30 January 2023
Safe City

Mr. Bholah
Superintendent of Police
Mauritius Police Force

30 January 2023
“PROTECTING PERSONAL DATA ACROSS ALL ECONOMIC SECTORS”

Mr. A. BHOLAH
Superintendent of Police
OC PMCCC

Shri Atal Bihari Vajpayee Tower, Ebène
The Mauritius Police Force (MPF) is responsible for State Security. The duties of the MPF are prescribed under Sec. 9 of the Police Act.

The MPF has adopted the “Safe City Solution” to enhance the safety of Mauritian Citizens and visitors in line with our Prime Minister’s vision.
The Project consists of four components:

1. Police Main Command & Control Centre (PMCCC)
2. Emergency Response Management System (ERMS)
3. Cameras
4. Radio Communication

- **PMCCC**
  - 8 Sub-Command Centres
  - 72 Station Monitoring Bay

- **ERMS**
  - Hotlines
    - 999/112
    - 148 (Anonymous)
    - Gender Based Violence Apps
    - Elderly Apps

- **Cameras**
  - Intelligent Video System (IVS)
  - Intelligent Traffic Surveillance (ITS)
    - 4000 Cameras (Fix and PTZ)
    - 300 cameras (with Automatic Number Plate Recognition Plate (ANPR))

- **Radio Communication**
  - EP 820
  - EV 750
  - 4500 radios
  - 350 radio (Police Vehicles)
Personal Data are captured through ...

- Name of Caller
- Phone Number,
- Address
- Location (GPS)

- Images of data subject
- Registration Number Plate
- Images are stored for 30 days

- Voice
- Video
- Snapshot

PROTECTING PERSONAL DATA ACROSS ALL ECONOMIC SECTORS

Copyright Data Protection Office
Protecting Personal Data

Code of Practice
(issued by the Data Protection Office)

The Mauritius Police Force is adhering to the Code of Practice for Safe City which sets out the basic conditions for the use of Safe City Systems in accordance with the provisions of the Data Protection Act 2017 (DPA).

• All Cameras are sited at strategic location (such as public places, beaches, public road, larceny prone areas)

• The PMCCC is to ensure the proper running of the Safe City system(s) under its control and also ensure that all its personnel operating or monitoring the system(s) are trained and work under the legal framework.

• Recorded material are processed in accordance with the DPA, i.e. footages should be relevant, authentic and impartial.
Protecting Personal Data

- All **Data** are stored on a server housed at the **Government Online Centre (GOC)**, Ebene
  - Access to GOC is controlled. Only Engineer / Technician from MT/Huawei under the supervision of Police are granted access for maintenance

- Access to PMCCC/ SCC are restricted areas
- Stations Monitoring Bays have been placed out of Public view.

- **Disclosure of Personal Data to third party is done:**
  - On issue of a Court Order,
  - Upon request from Attorney General’s Office, or
  - From a Police Officer not below of the rank of an ASP, for investigation or advice from DPP

- **Retrieval of Footages:**
  - Two copies are retrieved:
    - One as ‘**Master Copy**’ is sealed in a plastic evidence bag, authenticated by the Enquiring Officer and is kept as exhibit for court production.
    - A second one as ‘**working copy**’ is handed over to the Enquiring Officer for investigation
Safe Guard

• Laws
  – **Constitution** :- Sec 3 (c) the right of the individual to protection for the privacy of his house
  – **Data Protection Act** :- Sec. 44 (1)
    - Protect the privacy of individuals. The exception allowed:
      – 1. for public security
      – 2. prevention, investigation and detection of an offence
  – **Information & Communication Technologies Act / Official Secret Act**

*If an officer has breached the above acts, legal actions will be taken against him*

• Training
  – PMCCC Personnel, SCC and those at Police Station are trained on relevant Laws and Code of Practice
  – Issuing of personal account number

• Compliance Audit
  – PMCCC is subject to compliance audits by the DPO for
    • How the PMCCC collects and processes the personal data?
    • Policies implemented in compliance with the DPA e.g. Privacy Policy, Retention Policy
    • Procedures for handling personal data breaches and rights of data subjects.
Data Protection in Health Sector

Dr. A. Bholah

MSc Global eHealth (University of Edinburgh)
MBBS (SSRMC)
Digital Health Office
Ministry of Health & Wellness

30 January 2023
Health Information Exchange

Primary Care Physician
- EMR

Lab
- Results

Independent Health Facility
- Imaging

Pharmacy
- Rx History

Specialty Practice

Hospital
- PACS
- HIS
- Departmental

DocumentRegistry

Document/Image Repository

Other HIE

Patient
- Personal Health Records

Government
- Quality and Efficiency

Community Hospital
- PACS
- HIS
- Departmental

Copyright Data Protection Office
What is HIPAA Compliance?

HIPAA compliance is adherence to the physical, administrative, and technical safeguards outlined in HIPAA, which covered entities and business associates must uphold to protect the integrity of Protected Health Information (PHI).
The 3 Types of HIPAA Safeguards

**Administrative**
- Risk assessment
- Assigning a privacy official
- Staff training

**Physical**
- Alarm systems
- Security systems
- Locking areas where PHI is stored

**Technical**
- Data encryption
- Antivirus software
- Automatic log-off
- Audit controls

Copyright Data Protection Office
**Personal sensitive data**
This is the full data including personal and special* data.

- **Name**: John Briggs
- **Date of birth**: 14.04.87
- **Email**: jb89@mail.com
- **User ID**: john_briggs_89
- **Health**: type 1 diabetes

**Pseudonymous data**
IDs are replaced with pseudonyms. Sensitive data is encrypted.

- **Names**: User-78463
- **Date of birth**: 14.04.87
- **Email**: "" (blurred)
- **User ID**: "" (blurred)
- **Health**: type 1 diabetes

**Anonymous data**
IDs removed & sensitive data randomised/generalised.

- **Sex**: Male
- **Age**: 30-49
- **Health**: type 1 diabetes
Plaintext: Here’s my private data

Encrypt

Public key

Ciphertext: U2sdGVkJ1oKSus91yVnP

Decrypt

Private key

Plaintext: Here’s my private data
Digital Health Law

- Provide a general framework for the digital health sector;
- Data sharing between health institutions and practitioners, including private clinics and medical practitioners, and medical insurances;
- Data privacy and data protection;
- Incorporate national policies and long-term objectives of the health sector;
- Define clearly the roles, functions and powers of the Ministry and relevant Departments falling under its aegis;
- Comply with international conventions and commitments ratified by the Government of Mauritius;
• Propose any repealing of existing Acts (or parts thereof) and enactment of the New Digital Health Act;

• Propose appropriate legal mechanisms for the prevention of illegal Digital Health Services;

• Develop regulations as follows for implementation of the Digital Health Bill, but not limited to:
  • Digital Prescription
  • Digital Signatures
  • Digital Medical Certificates
  • Digital Laboratory Results
  • Digital Medical Reports

• Advise on the human resources, institutional set-up and logistics required for implementing the Digital Health Bill.
Dr. Bholah Amal

MSc Global eHealth (University of Edinburgh)
MBBS (SSRMC)
digitalhealth@govmu.org
214 8850
Sharing the Data Protection Certification journey

Mr. K. Sumputh
Chief Security Officer
ABSA

30 January 2023
Our Journey to the Data Protection Certification

Kevin Sumputh
Chief Security Officer, Absa Bank Mauritius Limited
30 January 2023
The Data Protection Journey of Absa Bank Mauritius Limited

- **Dec 2017**
  - Mauritius Data Protection Act

- **April 2018**
  - Integrated Plan – Privacy Programme

- **Aug 2019**
  - Data Privacy Officer

- **Jun 2019**
  - Privacy Policy

- **Jul 2020**
  - Privacy Processes Embedded

- **Jun 2021**
  - Application for Data Protection Certificate

- **Oct 2022**
  - First Organization to receive Data Protection Certificate
## The Integrated Plan – Privacy Programme (2018-2020)

### Governance
- Gap assessments & Legislative reviews (incl. GDPR)
- Publish Privacy Policy and Standards

### Target Operating Model
- Roles and Responsibilities of the Data Protection Officer
- Recruitment of the Data Protection Officer

### Privacy Processes
- Data Subject Rights – Define processes
- Privacy Notice and Terms & Conditions Reviews
- Data collection and Lawful processing

### Privacy Impact Assessment
- Define requirements of the Privacy Impact Assessment
- Mandatory for all New/Amended Projects (Cloud Projects)

### Complaints Process
- Define process in line with DPA and Banking Act
- Internal breach escalation process

### Information Breach Management Process
- Implement process in adherence to DPA and Banking Act
- Internal breach escalation process

### Repository of Personal Data
- Customer Data Flows, Touchpoints & Repository
- Retention of Personal Data

### Supplier Contract Review
- Define a Privacy Due Diligence for Suppliers
- Include Data Privacy Clauses in contracts

### Data Transfer & Sharing
- Security Controls in place (including Suppliers)
- Data Leakage Prevention Tool (DLP)

### Flagging Functionality
- Marketing Opt Out process and functionality
- Data Subject Requests

### Training and Awareness
- Devise induction and refresher trainings
- Assign Departmental Privacy Champions

### Annual Reviews
- Define list of annual reviews
- Define scope of reviews

### Assurance Reviews
- Compliance to review and approve the Integrated Plan
- Independent reviews

### Management Information
- Define processes of reporting (Board, Group)
- Develop platform for automated MIs
### Data Protection Certification (2021-2022)

#### Areas covered in the Application for Certification Form

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration and Renewal</td>
<td></td>
</tr>
<tr>
<td>Lawfulness, fairness and transparency</td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td></td>
</tr>
<tr>
<td>Purpose limitation</td>
<td></td>
</tr>
<tr>
<td>Data minimization</td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
</tr>
<tr>
<td>Storage limitation</td>
<td></td>
</tr>
<tr>
<td>Duty to destroy data</td>
<td></td>
</tr>
<tr>
<td>Duties of controller</td>
<td></td>
</tr>
<tr>
<td>Collection of personal data</td>
<td></td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td></td>
</tr>
<tr>
<td>Security of processing</td>
<td></td>
</tr>
<tr>
<td>Record of processing</td>
<td></td>
</tr>
<tr>
<td>Data Impact Assessment</td>
<td></td>
</tr>
<tr>
<td>Prior authorization and consultation</td>
<td></td>
</tr>
<tr>
<td>Transfer of personal data</td>
<td></td>
</tr>
<tr>
<td>Right of access</td>
<td></td>
</tr>
<tr>
<td>Automated individual decision making</td>
<td></td>
</tr>
<tr>
<td>Rectification, erasure or restriction of processing</td>
<td></td>
</tr>
<tr>
<td>Right to object</td>
<td></td>
</tr>
<tr>
<td>ISO-IEC</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
</tr>
</tbody>
</table>

#### Our Challenges…

<table>
<thead>
<tr>
<th>Conditions for Consent</th>
<th>Records of Processing</th>
<th>Data Protection Impact Assessment</th>
<th>Rectification, erasure or restriction of processing</th>
<th>Right to object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is consent verifiable?</td>
<td>Are records of all processing operations maintained?</td>
<td>Must be completed for high risk operations.</td>
<td>Erasure or Restriction of processing?</td>
<td>Personal data should no longer be processed</td>
</tr>
<tr>
<td>Is consent easy to withdraw</td>
<td></td>
<td></td>
<td>Bank of Mauritius requirements (7 years)</td>
<td></td>
</tr>
</tbody>
</table>
Data Protection Certification (2022)

- First Organization and Bank in Mauritius to receive a Certificate of Compliance
- Commendable support received from Data Protection Office

What it meant for us?
- Re-enforces trust and confidence with our stakeholders (Customers, Suppliers, Regulators, Absa Group)
- Opportunity for the marketing of the Absa brand
- Recognition and Pride to the Absa team
) Thank you (}
Panel Discussion

Data Protection in the financial sector

Mrs. K. Hurdowar
Barrister-at-law, Senior Manager
&
Data Protection Officer
Financial Services Commission

Miss. C. Domingue
Manager Compliance
Swan

30 January 2023
IMPORTANCE OF DATA PROTECTION
POWERPOINT PRESENTATION
ON
IMPORTANCE
OF
DATA PROTECTION IN the FINANCIAL SERVICES SECTOR

Presented by: Mrs Khemalini Hurdowar
Senior Manager /Data Protection Officer
Office of the Chief Executive
Financial Services Commission

30 January 2023
THE FINANCIAL SERVICES SECTOR

- Regulation of financial services include the regulation of banking and non-banking activities
Legal & Regulatory Framework

- Compliance with International norms and standards
  - IOSCO principles
  - IAIS principles
  - IOPS principles
  - OECD Principles
  - FATF recommendations (AML-CFT)
  - Signatory to IOSCO Administrative Arrangement on Exchange of Information / Privacy Notice (personal data)

- Mixed legal system: civil and common law

- Right of appeal to Judicial Committee of the Privy Council

- Confidentiality (with transparency) for Global Business

Legislation (Relevant Acts)
- Financial Services Act
- Insurance Act
- Securities Act
- Private Pension Schemes Act
- Captive Insurance Act
- Protected Cell Companies Act
- Trust Act
- Variable Capital Companies Act
- Virtual Asset and Initial Token Offering Services Act

- Companies Act
- Limited Partnerships Act
- Foundations Act
- Financial Reporting Act
- FIAMLA
- Asset Recovery Act
- Limited Liability Partnership Act
- Prevention of Corruption Act / Prevention of Terrorism Act

- A flexible legal and regulatory framework for the financial services industry
- The right balance between regulation and business development
Activities regulated by the FSC

- FSC has several objects & functions: licensing, supervision, enforcement, financial literacy & developmental role for the country.

- The Financial Services Act (FSA) of 2007, simplifies the regulatory regime and consolidates the legislative framework of the global business sector.

  In monitoring the conduct of business activities of its licensees, the FSC focuses inter alia on market conduct, Anti-Money Laundering and Combating the Financing of Terrorism requirements, good corporate governance principles and international norms and standards.

Management Companies (MCs) are service providers which act as intermediaries between their clients and the FSC (applications for Global Business Licence). MCs are licensed by the FSC under Section 77 of the FSA.

An applicant for a Global Business Licence has to pass the test of a resident corporation conducting business outside Mauritius. An applicant for a Global Business Licence is required to submit the appropriate application to the FSC, channelled through a Management Company of its choice.

Under the Financial Services Act, corporations are also allowed to operate as Global Legal Advisers and Investment Bankers.

There is also the concept of Authorised Companies.
Activities regulated by the FSC (part 2)

- There are other financial services activities, regulated under other relevant acts (e.g. the **Insurance Act**, the **Securities Act**, **Trust Act**, and the **Private Pension Schemes Act**).

**Indicative list:**


- Qualified trustee, enforcer, successor to enforcer / Funds – CIS / CEF / CIS functionaries / foreign schemes

- Pension scheme, Foreign Pension scheme, External Pension scheme

- Captive insurer, Captive insurance agent / Virtual Asset Service Providers / VCC Fund

- Providers of market infrastructure like Securities Exchange, Clearing & Settlement Facility

- Securities or Capital Market Intermediaries (e.g. investment dealer/adviser etc) / representatives
Activities regulated by the FSC (part 3)

- Some of the financial business activities, other than those under the relevant acts (e.g. the Insurance Act, the Securities Act and the Private Pension Schemes Act), as listed in the Second Schedule of the Financial Services Act are:
  - Assets Management, Crowdfunding, Credit Finance, Custodian Services (non-CIS), Distribution of Financial Products, Factoring, Leasing, Pension Scheme Administrator, Registrar and Transfer Agent, Treasury Management, Peer-to-Peer Lending
  - Credit Rating Agencies/Rating Agencies, Global headquarters administration, Global treasury activities
  - Representative Office (for financial services provided by a person established in a foreign jurisdiction)
  - Actuarial services, Payment intermediary services (outside Mauritius), Family office (single), Family office (multiple)

- This list is not exhaustive and the FSC Rules may provide for other financial business activities.
Statistics

- Contribution of the Financial Services Sector to the GDP
  - 14% for year 2021
- Number of licensees
  - As at December 2022
  - 12,813 GBCs
  - 6,141 Authorised Companies
  - 1,318 domestic entities (excluding insurance salespersons)

Source: Statistics Mauritius - National Accounts - December 2022 Issue

- Contribution to the Consolidated Fund
Challenges in the Financial Services sector

- Data valuable (like oil in previous century) & needs to be protected - several types of personal data e.g. trusts information, payslips, beneficial owner information
- Constitution – Right to privacy / Article 22 of the Code Civil Mauricien provides that: "Chacun a droit au respect de sa vie privée« / Data Protection Act 2017
- The need for data protection laws is derived from this general principle that everyone has the right to the protection of his private life
- Globalisation, coupled with the rapid technological developments pose new challenges to the protection of personal data in the Financial Services sector
- The scale of collection and sharing of personal data has increased exponentially / online platforms
- Both private companies and public authorities make use of personal data on an unprecedented scale in their day to day activities - corresponding need for safeguards
- Whilst technology has transformed both the economy and social life of people and further facilitate the free flow of personal data whether onshore or offshore, ensuring a high level of protection of personal data is essential.
Impact of EU GDPR on the Financial Services sector

- EU GDPR incorporated into national legislation - The Data Protection Act 2017
- The updated regulatory framework strengthens the ties between Mauritius and Europe. It thus helps to attract Foreign Direct Investment and fosters a more business friendly environment.
- There are wide-scale privacy changes in all organizations and companies in Mauritius. The regulator (DPO) has unprecedented powers to initiate action for fines in case of non-compliance.
- Companies and organizations must notify the national supervisory authority, namely the Mauritius DPO, of data breaches which put individuals at risk and communicate all high risk breaches as soon as possible to the data subject.
- Data controllers and processors must conduct a Data Protection Impact Assessment prior to any processing of sensitive data that likely involves high risks to the privacy of data subjects.
FUNCTIONS OF THE FSC DATA PROTECTION OFFICER

I. INFORM AND ADVISE THE ORGANIZATION AND STAFF

II. ENSURE COMPLIANCE WITH THE DPA AND OTHER DATA PROTECTION LAWS

III. MANAGE INTERNAL DATA PROTECTION ACTIVITIES

IV. MANAGE DATA BREACH NOTIFICATIONS
FUNCTIONS OF FSC DATA PROTECTION OFFICER

- Advise on data protection management
- Train staff to be in compliance with DP laws in view of audits/inspection
- Be the first point of contact for the data protection office and for individuals whose data are processed
- Be the liaison officer with the data protection office on data protection matters for projects
- Perform such other duties as may be relevant to the implementation of data protection standards
Compliance of FSC as Data Controller (1)

- **Registration** – work with several clusters / Committees / Secretariat to encompass & disclose the types of data processed by FSC (employees and non-employees like officers in licensees like directors, applicants for licences, shareholders, trustees, beneficial owners, suppliers, whistleblowers etc) & the uses of the data (elaborate and extensive Data Controller form)

- Importance of identifying & keeping personal data e.g even children data in Financial Literacy campaigns

- Appointment of **Data Protection Champions** across the organization

- **Training & Awareness sessions to staff** and Committees on key concepts, risks of breaches of data e.g human error / computer systems & Consequences of Non-Compliance – offences in Mauritius– risk of delisting internationally

- **Staff should protect personal data** (data on employees and non-employees e.g licensees, suppliers, students, speakers and whistleblowers)

- Precautions for staff to take to avoid leakage of Personal Data (e.g careful to rename and check scanned documents prior to sending emails, check the correct emails before sending, correct use of fax numbers, use of hard copies, use of printer, discretion when talking about personal data matters in the course of work, careful when inserting documents in envelope)

- What happens in case of a personal data breach?

- Crucial that personal data of licensees data properly safeguarded (+ confidentiality under FSA)

- Consequences of **unlawful disclosure / offences & reputational damage** to the institution and the country
Compliance of FSC as Data Controller (2)

- Crucial that personal data of licensees data properly safeguarded (+ confidentiality under FSA )
- Documents posted on the Intranet for information on Data Protection issues
- Principles in handling Personal Data
- Security of Personal Data- IT Policy for Data Security
- Safeguards against IT risks e.g use of passwords / risks of hacking / disaster recovery
- High Risk Data Assessment for high risk data, such as large scale data and sensitive data (e.g health details) -guidance provided
- Special Categories of Data ( Section 2 and Section 29 of DPA )
- Data Protection laws and Communiques e.g Social media and the Internet ( FSC We Connect )
Compliance of FSC as Data Controller (3)

- Appropriate security measures be taken for unauthorised processing of personal data and against accidental loss, destruction or damage / IT Security measures
- The FSC has also appointed a Chief Information Security Officer ("CISO") who has helped to enhance the security systems at the FSC.
- CYBERSECURITY viewed as very important
- Convention on Cybercrime /The Cybersecurity & Cybercrime Act 2021
- Our staff continue to work to enhance FSC’s cyber security posture, while supporting our digital transformation initiative.
- FSC requests confirmation of IT security measures / disaster recovery etc from some licensees
- FSC is aligned with the Government’s efforts to improve the nation’s cybersecurity.
- FSC is vigilant to the evolving threat landscape and continuously maintain the highest level of resilience. This focus cannot be compromised. Although the monetary cost of improving cyber resilience may seem high, the costs of successful attacks – in terms of both financial damage and reputational impact – are far higher.
- In addition, we continue to evaluate our data footprint and improve our data collection processes so that we collect only the data we need to fulfill our mission.
Compliance of FSC as Data Controller (4)

- Investors from EU - Extra-territorial application of EU GDPR (data belonging to EU citizens and residents)

The law, therefore, applies to organizations that handle such data whether they are EU-based organizations or not, known as “extra-territorial effect.”

- Similarities between provisions of the DPA and EU GDPR
- Prompt advice on any matters arising to ensure compliance e.g. Contracts (local / international – procurement / Online Platform / other projects)
- Consent issues – pictures / bio-data / recordings / Annual Reports / calendar/ Projects with other institutions like the bonus malus system
- Transfer of data abroad – list of countries - personal data can only be transferred to a third country which ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.
- Outsourcing – only to EU –GDPR compliant countries
- Change in particulars to Data Controller form reported to MRU DPO e.g data wrt vaccination , information wrt Covid cases, new type of data kept at RCE
- Can notify data breach to Data Protection Commissioner & communicate to data subject
FSC & Importance of Data Protection (1)

- **International Financial Centre**, the Mauritius jurisdiction maintains an environment of transparency, stability, and predictability providing the right platform to investors for doing business. Reputation of the sector important

- Financial Services sector - High number of Licensees, huge amount of data

- Foreign Investors look for a jurisdiction which safeguards their personal data

- **FSC measures**: 
  - **DPOs of licensees regarded as officers under the Financial Services Act** (and require Fitness and propriety assessments)
  - The FSC expects licensees to comply with the all relevant laws and take measures to enforce compliance with laws / data protection best practices
  - An example in the Fintech space is the following **licensing condition for one activity**: 
    “The Company shall adopt cyber security and data protection best practices as part of its ongoing obligations.”
Individual rights to protection of data should be upheld at all times

FSC signatory to IOSCO Administrative Arrangement for the transfer of personal data between each of European Economic Area ("EEA") – Appendix A and each of the non-EEA Authorities – Appendix B ("the "AA") - Exchange of Information – 1st September 2021

This is a mechanism under Art 46 of the EU-GDPR for transfer of personal data with appropriate safeguards (in case of repeated exchanges)

Importance of protection of personal data & robust data protection regimes in place

Any sharing in a controlled manner – Data Protection Principles applied & Safeguards in place

Privacy notice posted on Website

Need to comply with safeguards – A breach can entail delisting from the AA

Signature of the AA – good sign internationally for upgrading of standards and modernization of the Financial Services sector
FSC & Importance of Data Protection (3)

- Financial Services sector - High number of Licensees, huge amount of data
- **CERTIFICATION** – FSC encourages Certification by licensees
- Data Breaches – consequences locally and internationally
- EU-GDPR – heavy fines in the world [https://www.enforcementtracker.com/](https://www.enforcementtracker.com/)
- So many cases - Insufficient legal basis for data processing / Insufficient technical and organisational measures to ensure information security / Non-compliance with general data processing principles
- Growth of **CYBERINSURANCE** to protect against cyberisks & data breaches
- But ! Reinsurers limit their underwriting – need for appropriate IT security systems/
  Cyberhygiene & Data Protection mechanisms
CONCLUSION

• Financial services – a continuously changing sector
• Flexibility & innovation required to boost the sector with appropriate safeguards
• Duty for FSC to administer the relevant Acts judiciously and to protect the consumers of financial services – Data protection measures
• Accountability to data subjects (locally & internationally)
• Need to take measures to be in line with international standards & best practices including data protection – EU GDPR
• Need to benchmark our practices with renowned jurisdictions
• Personal data standards to be kept - FSC to maintain its reputation as an internationally recognised/ respected regulator e.g. being on Appendix A of the IOSCO MMOU
• Need to constantly update with developments in Data Protection
• Consistently help to increase the competitiveness of Mauritius as an international financial centre
THANK YOU!
DATA PROTECTION in the INSURANCE SECTOR

Presented by Clotilde Domingue
Data Protection Officer
THINK TWICE VIDEOS

Copyright Data Protection Office
Interview with the Data Protection Commissioner
Breaches have consequences

Clients' data, Our Responsibility

Thumbs up for the wonderful job you do for being Compliant

Together, let's protect SWAN

Copyright Data Protection Office
CYBER SECURITY AWARENESS

Copyright Data Protection Office