

African and International Perspective on Data Protection

Mrs. D. Madhub

Data Protection Commissioner
Data Protection Office

30 January 2023





Data Protection Office

Leadership is not about size



It's about knowledge & wisdom

Copyright Data Protection Office

Don't Look Now

The background is a dark blue field filled with a complex network of thin, light blue lines and small squares, creating a digital or circuit-like pattern. The lines and squares are scattered across the entire frame, with some areas appearing more densely populated than others.

10 Reasons *Why Privacy Rights are Important*

1 Privacy Rights prevent the government from spying on people (without cause)

2 Privacy Rights keep organisations from using personal data for their own goals

3 Privacy Rights help ensure those who steal or misuse data are held accountable

4 Privacy Rights help maintain social boundaries

5 Privacy Rights help build trust

6 Privacy Rights ensure we have control over our data

7 Privacy Rights protect freedom of speech and thought

8 Privacy Rights let you engage freely in politics

9 Privacy Rights protect reputations

10 Privacy Rights protect your finances

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>
<http://www.pptback.com/flowers-abstract-gradient-yellow-flowers-pptbackground.html>

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.

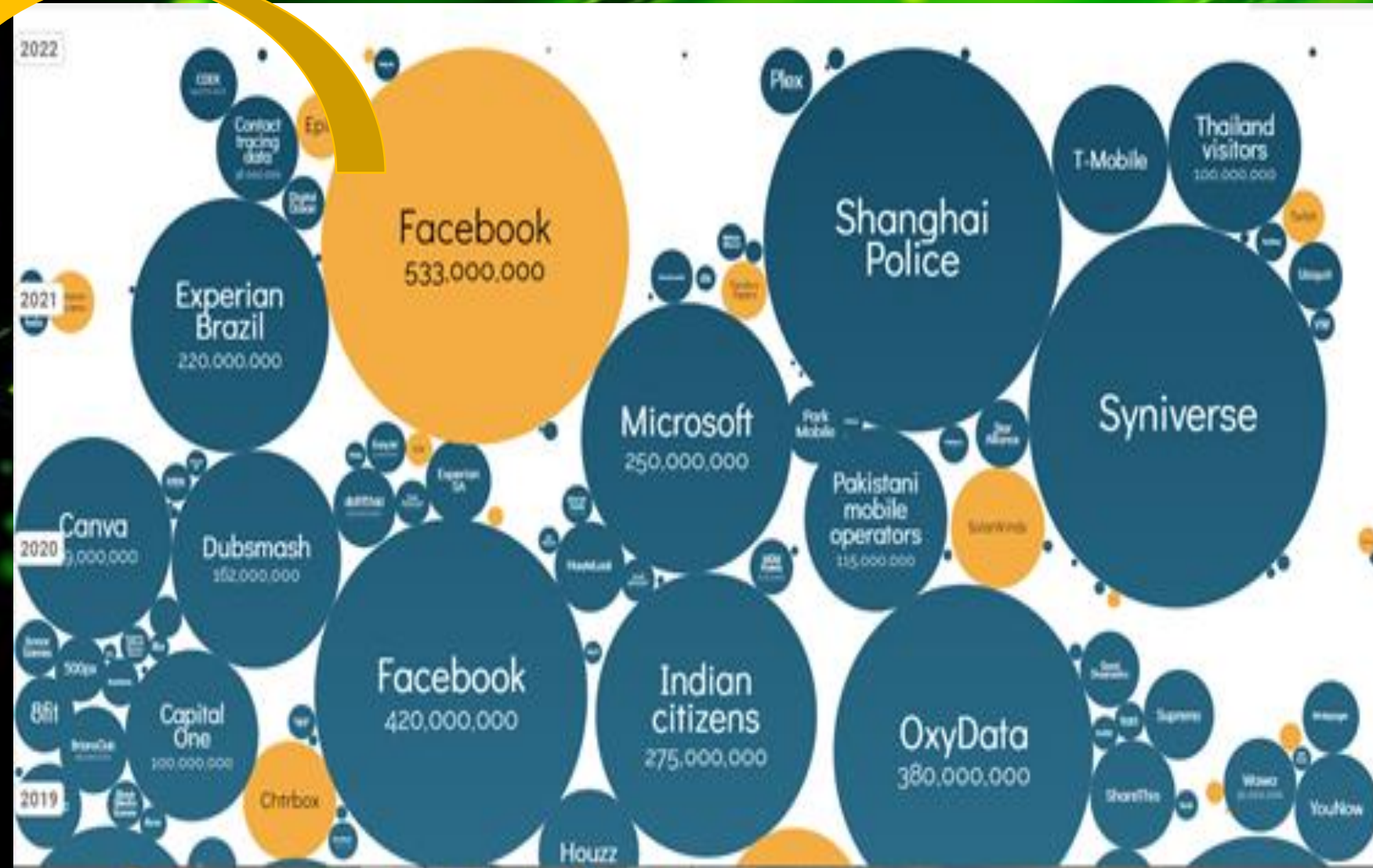
6. More data security and privacy job positions

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.

World's Biggest Data Breaches

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”

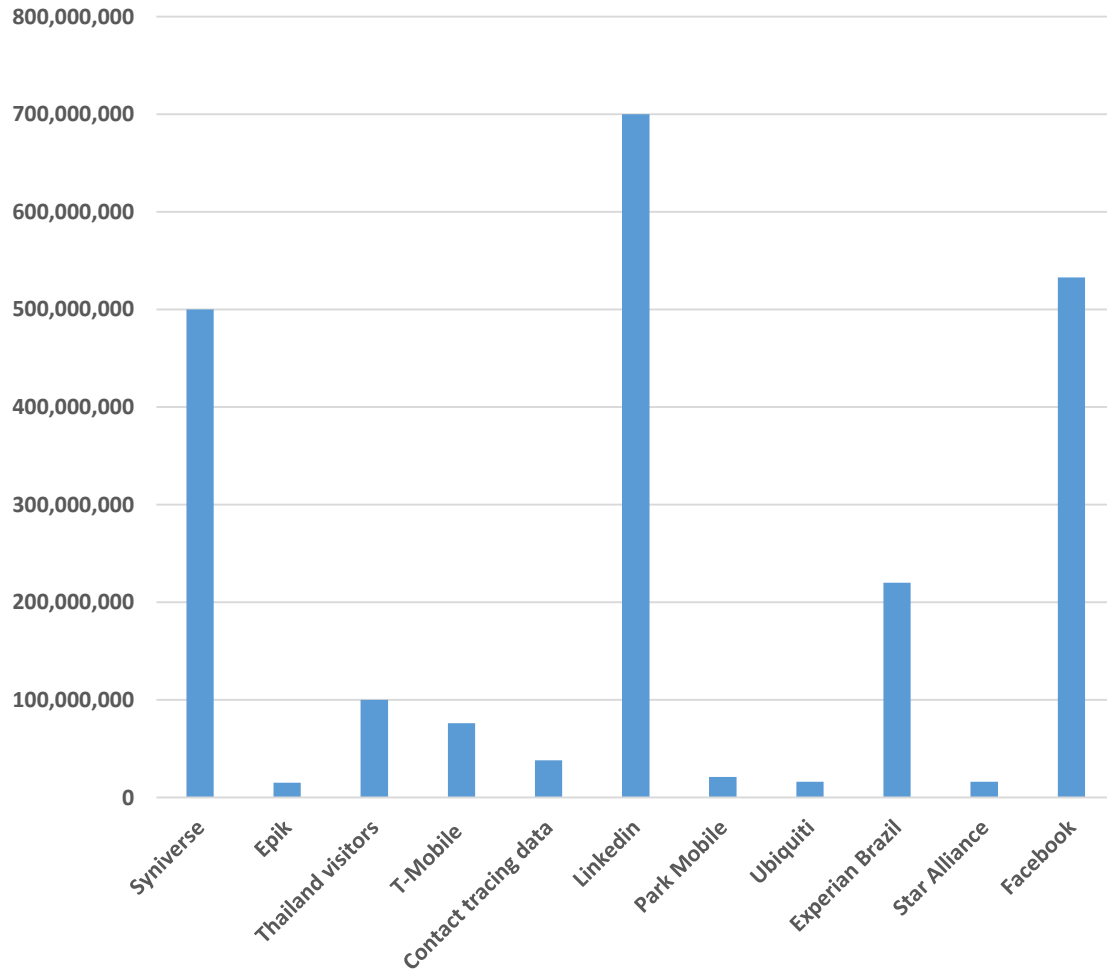


Source: <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Data Breaches exceeding 15,000,000 records lost

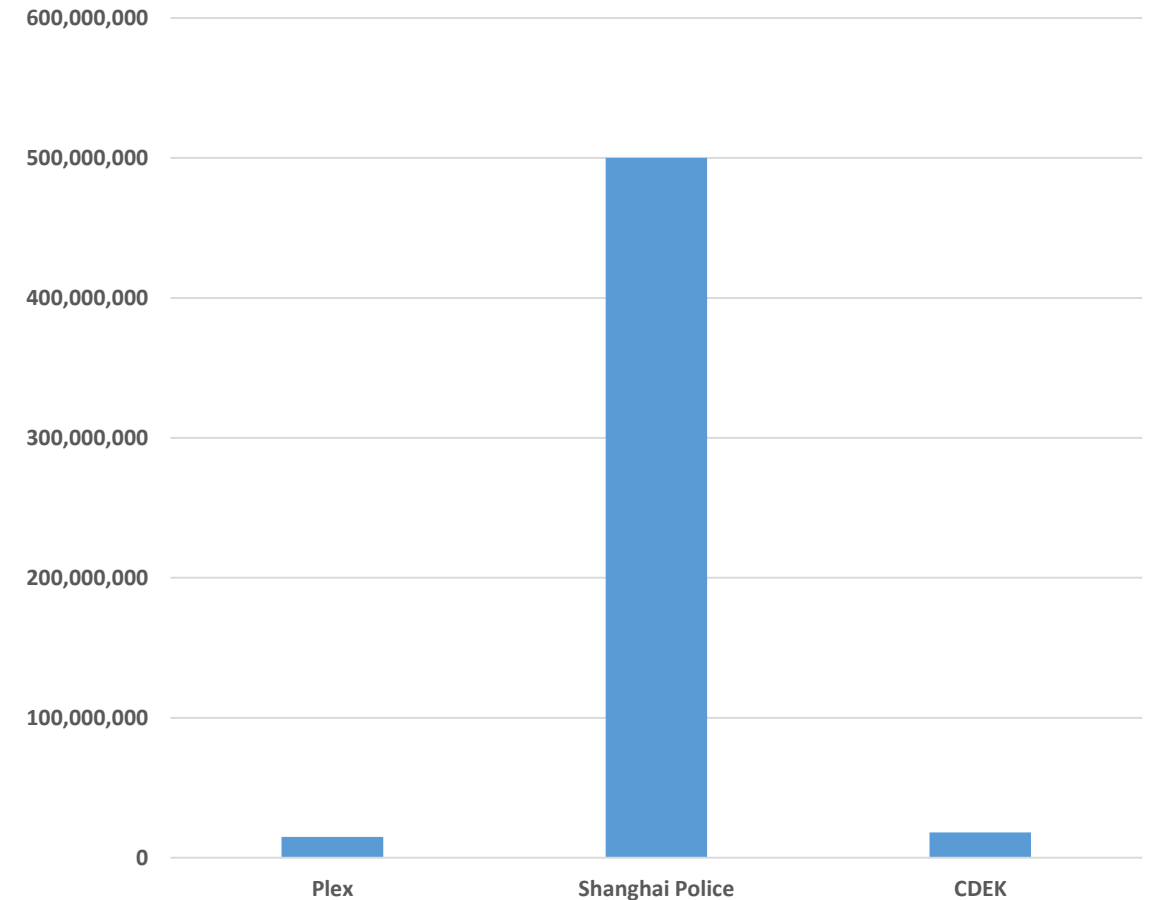
2021

2021



2022

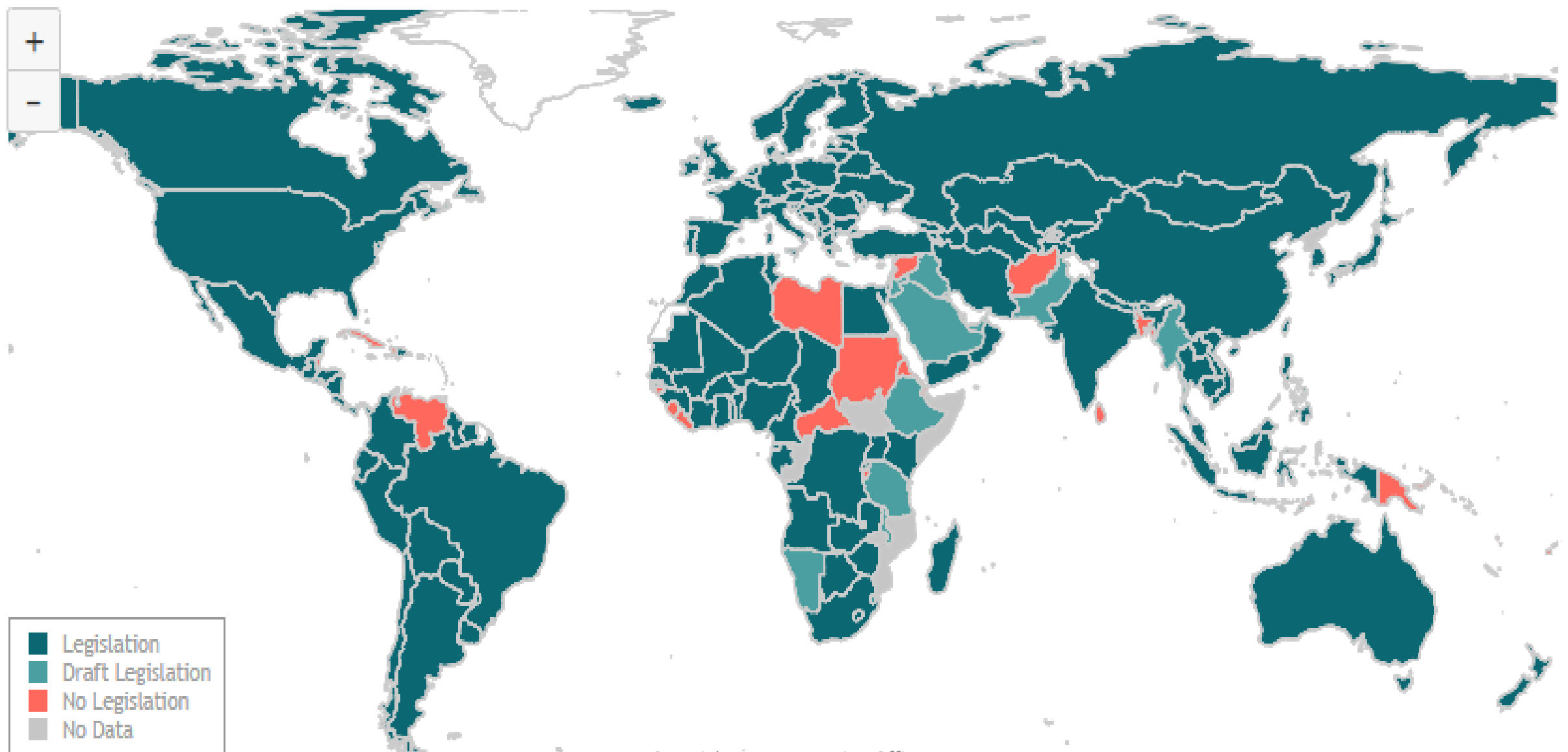
2022



Copyright Data Protection Office

Source: <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Data Protection and Privacy Legislation Worldwide



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.

Source: <https://www.videezy.com/>

Copyright Data Protection Office

<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

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

Key Considerations



Collection
Limitation

100100
101010
001001
01010



Data Quality



Purpose
Specification

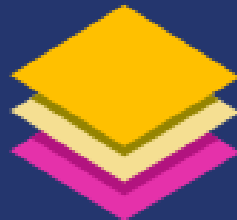


Use Limitation

Security
Safeguards



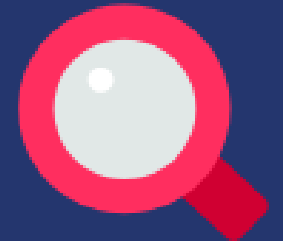
Openness



Individual
Participation



Accountability



AFRICA

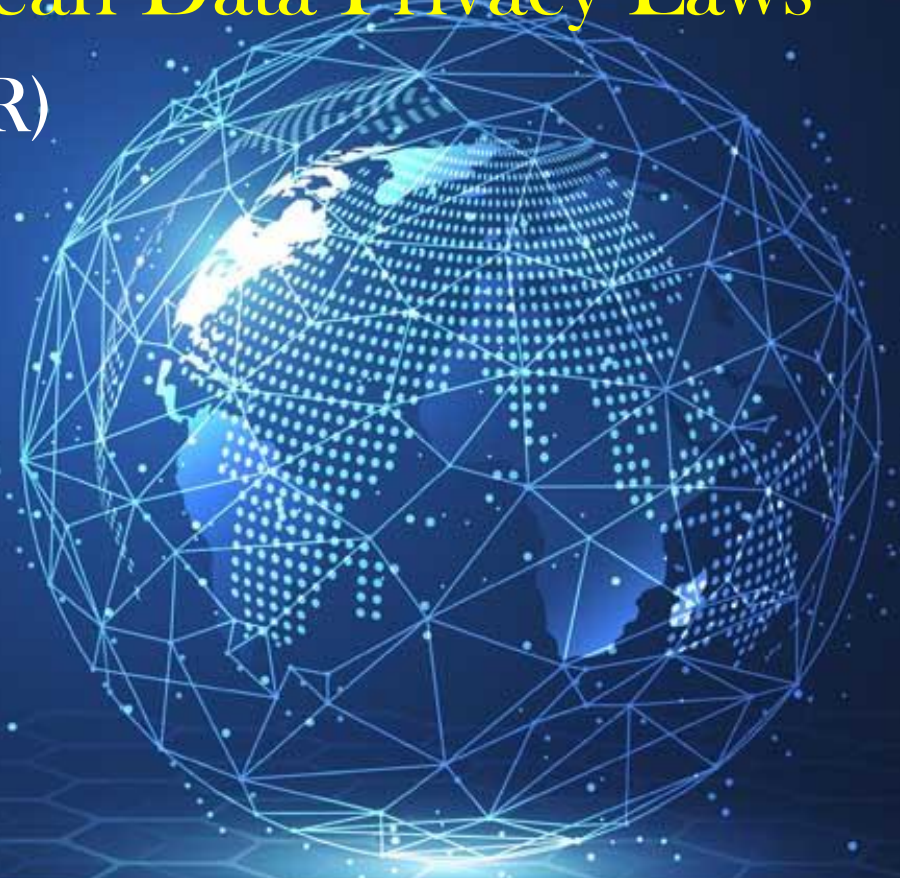
Existing Privacy Laws and Frameworks in Africa

- SADC Model Law on Data Protection (2010) – Under Review
- ECOWAS Supplementary Act A/SA.1/01/10 on personal data protection (2010)
- EAC Framework for Cyberlaws (2008)
- 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**.

United Nations

- 
- The United Nations emblem, featuring a world map surrounded by olive branches, is centered in the background of the slide.
- **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**

US

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

China

- Personal Information Protection Law (PIPL)

UK

- Data Protection Act 2018
- Online Safety Bill

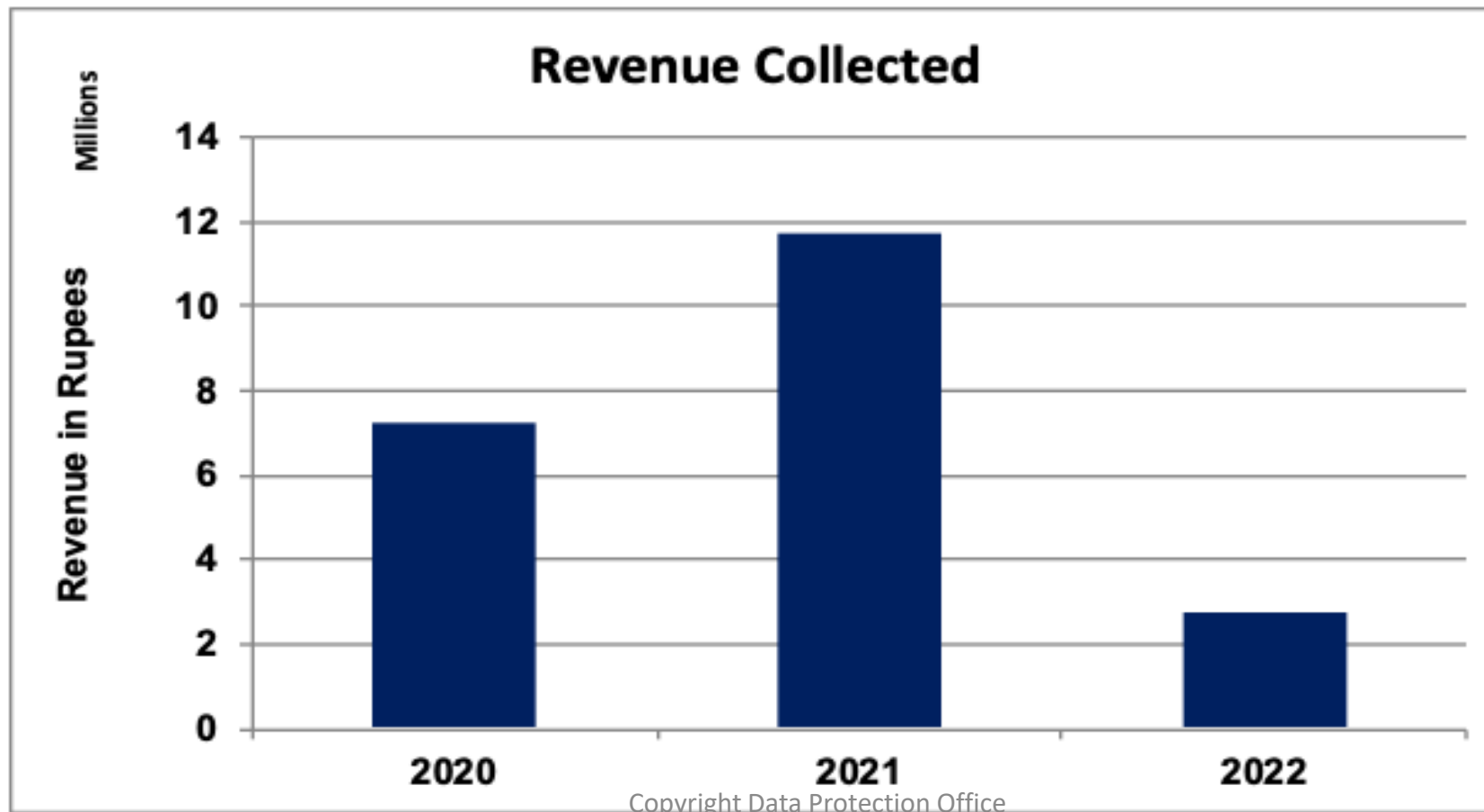
India

- Digital Personal Data Protection Bill 2022

Main Achievements of the Data Protection Office

Revenue Collected

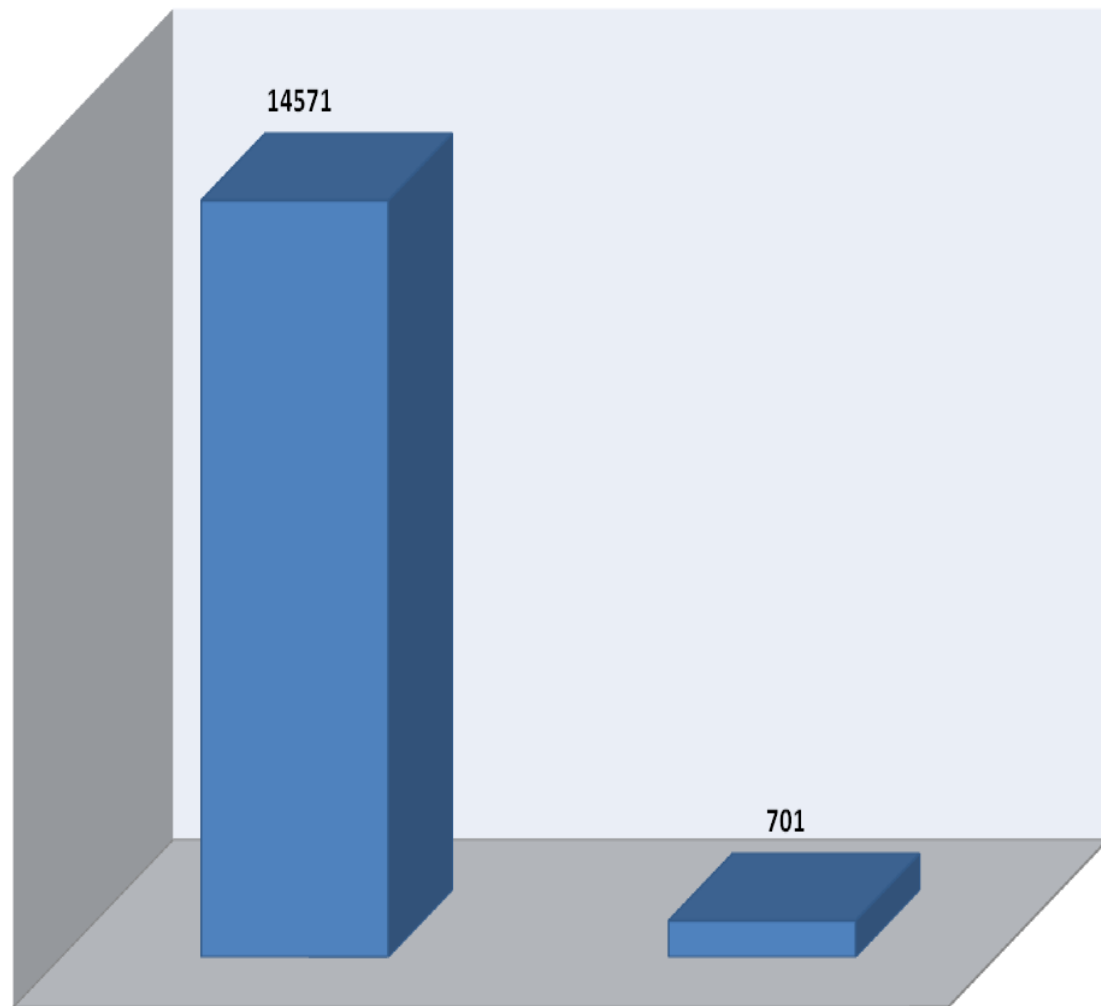
DPO collected a total revenue of **Rs 11,741,500** in 2021 and **Rs 2,736,500** for registration of controllers and processors in 2022.



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.

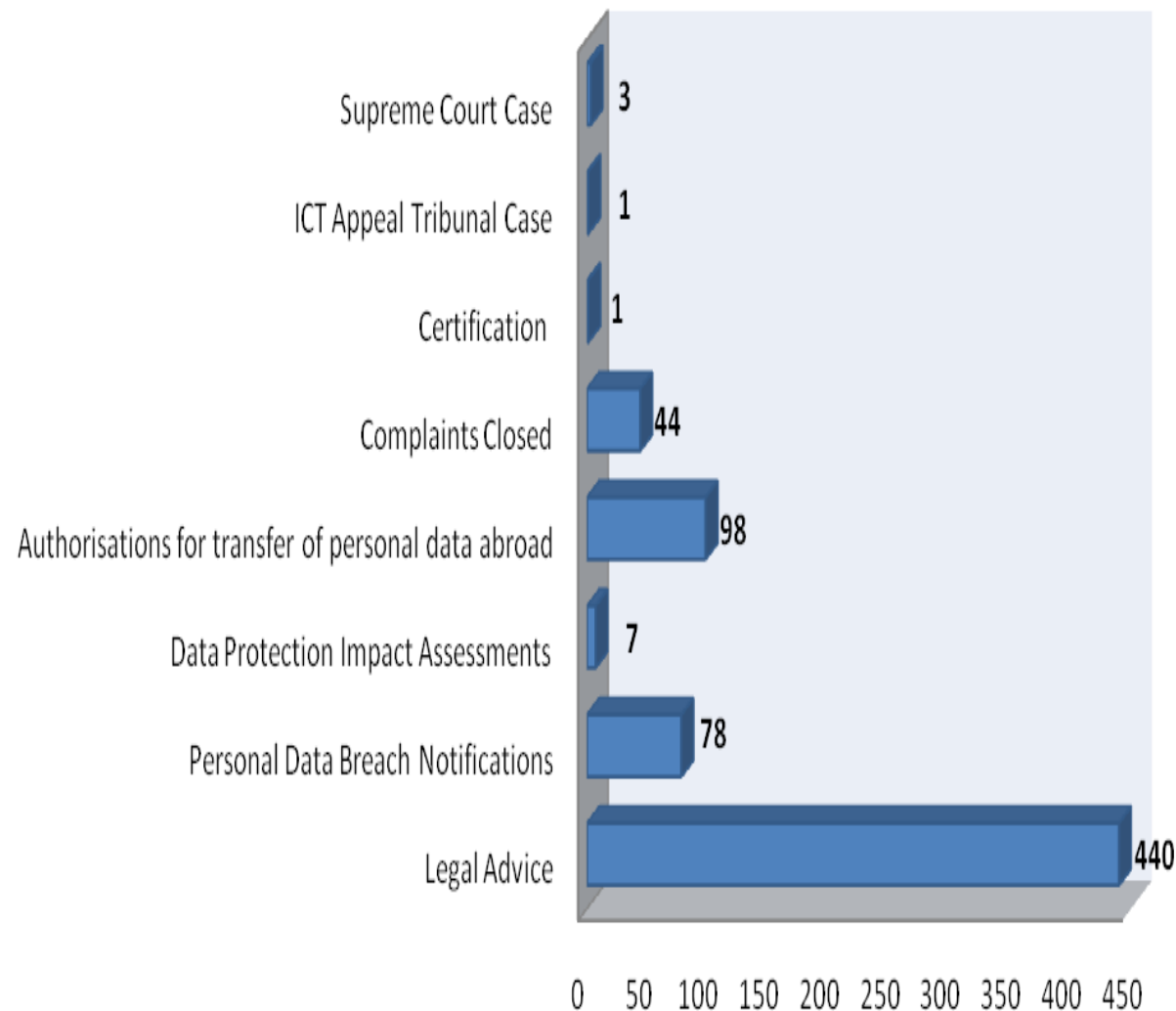
Enforcing Data Protection Statistics 2021 - 2022



Number of controllers registered

Number of processors registered

Copyright Data Protection Office



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:

Nature of Complaint	Total
CCTV Cameras	125
Fingerprints	1
Unlawful Disclosure of Personal Data	8
Rights of Data Subject Access	1

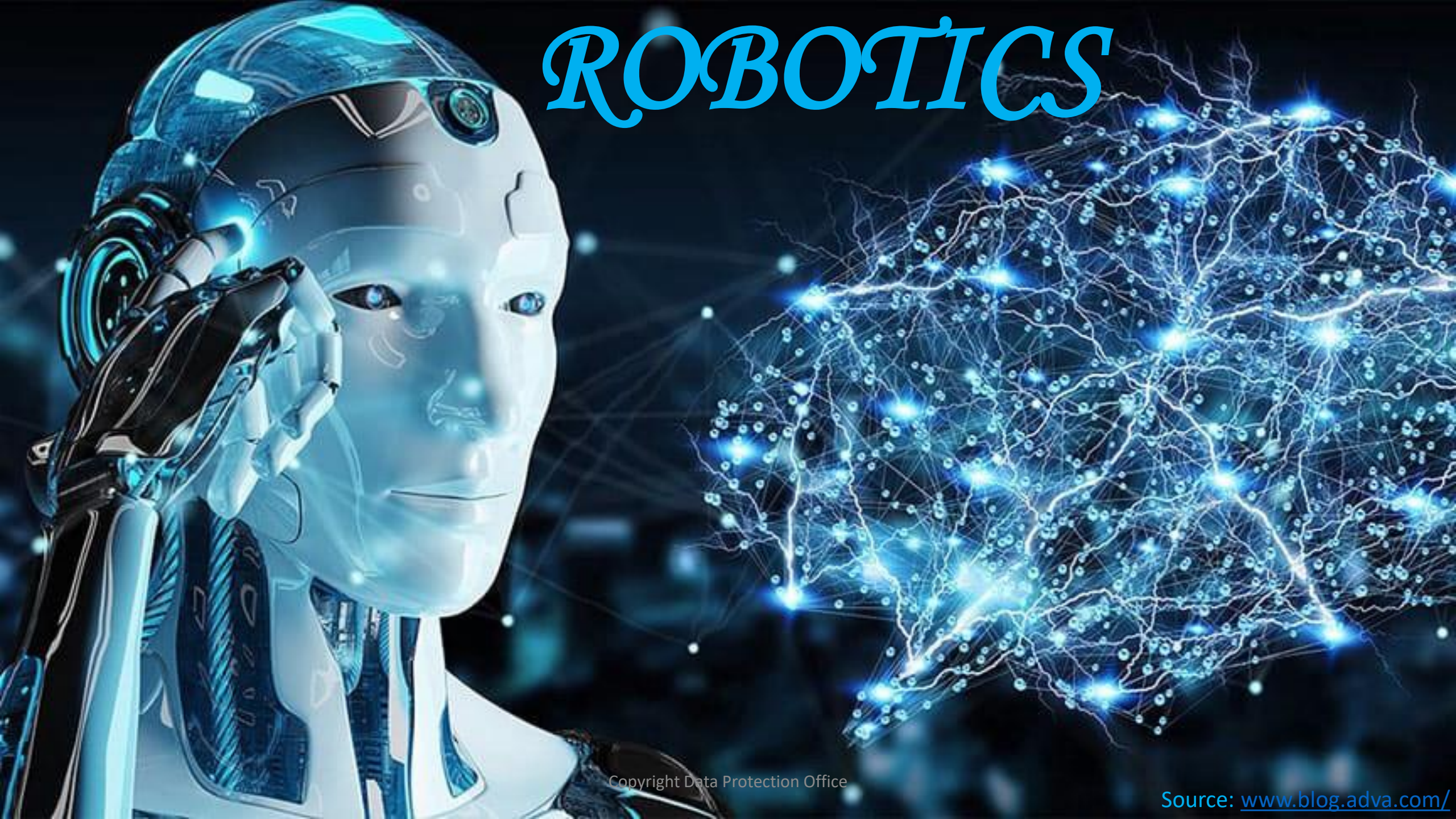
THE FUTURE

A call for Global Privacy Standards

Artificial Intelligence



ROBOTICS



PEOPLE AND PERSONAL DATA PROTECTION



Copyright Data Protection Office

Source: <https://www.dotmagazine.online/>

SETTING THE RIGHT EQUILIBRIUM





COOPERATION



*Thank You
For
Your Attention...*



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>



DPO Portal

Username

Password 

[Login](#)

[Create an account as DPO Administrator/User](#)

[Forgot Password?](#)

[Maupass Forgot Password?](#)

[Maupass Registration?](#)

[Register Anonymous Complaint](#)

Type of Administrators



1. Individual

Option 1

Individual with BRN
or no BRN.
Requires a Maupass
Account



2. Organisations

Option 2

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



3. Management
Companies

Option 3

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



4. Group of
Companies

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

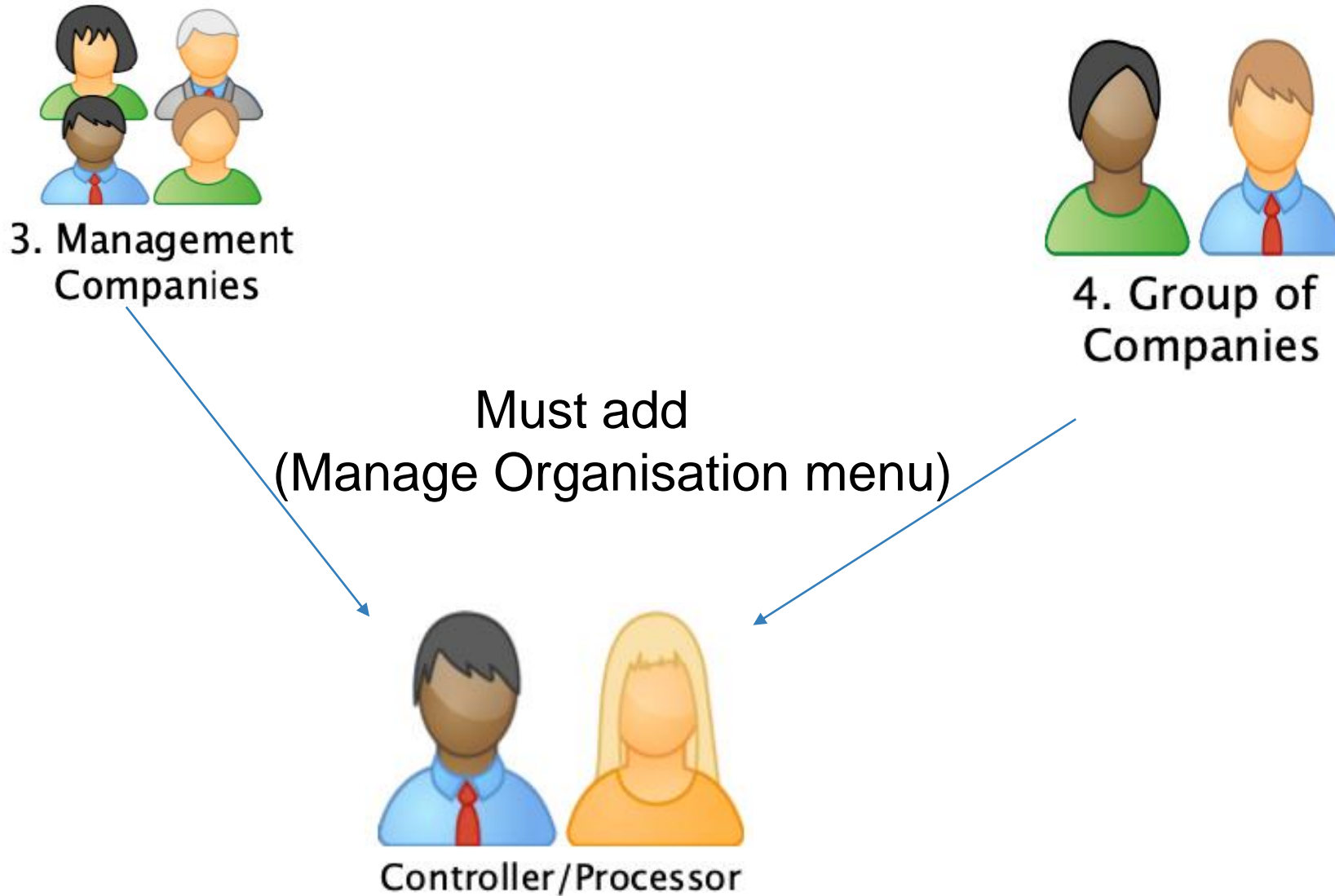
- Must log in with its Maupass Account
- It is the representative who register controller/processor on behalf of the Administrator (3 types)
- Submit the Eforms for a controller/processor

Concepts in eDPO Portal

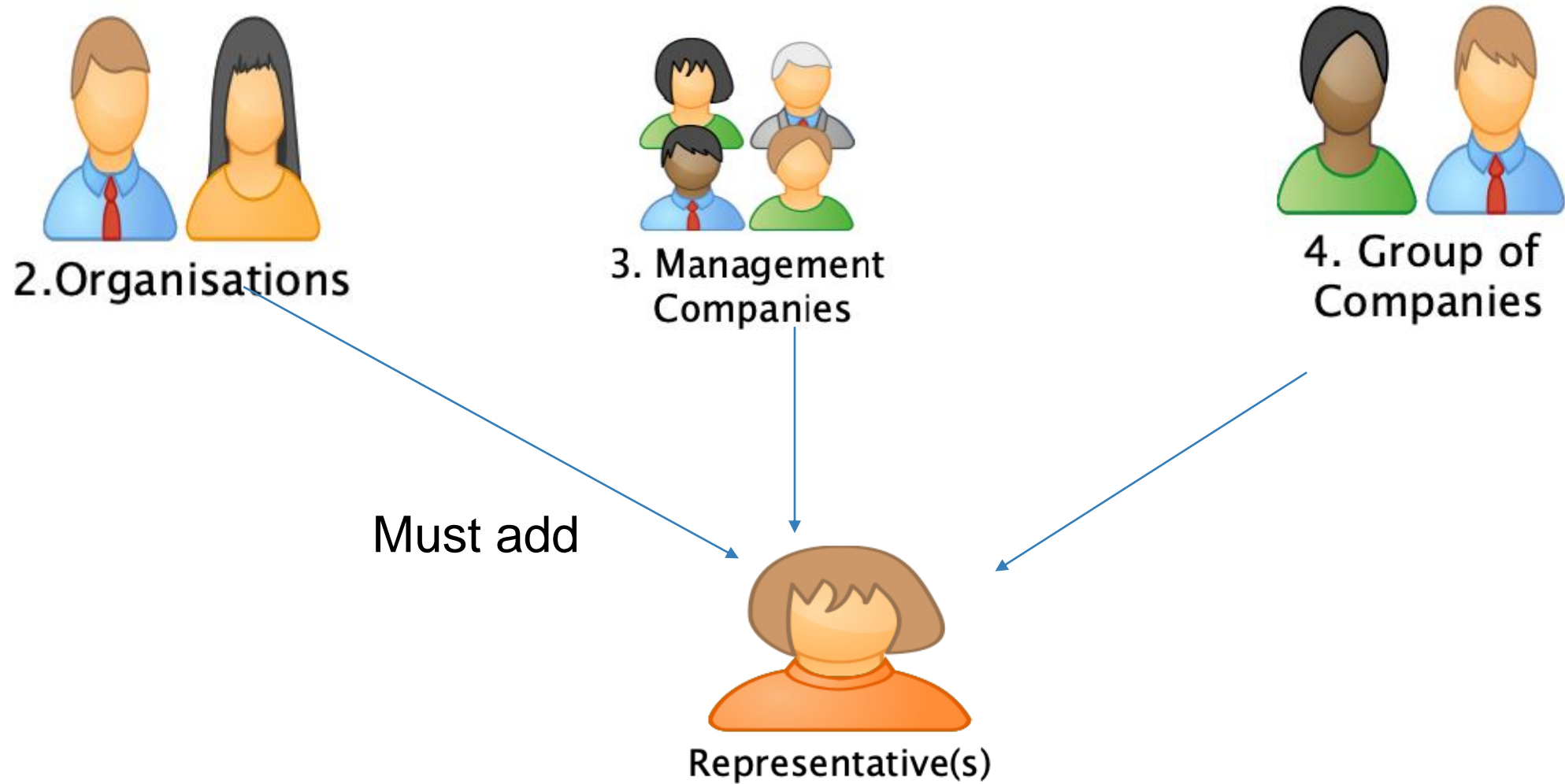
Administrator
account other
than Individual
(2 types)

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

Administrator and Companies(s)



Administrator and Representative(s)



Misconceptions in eDPO Portal

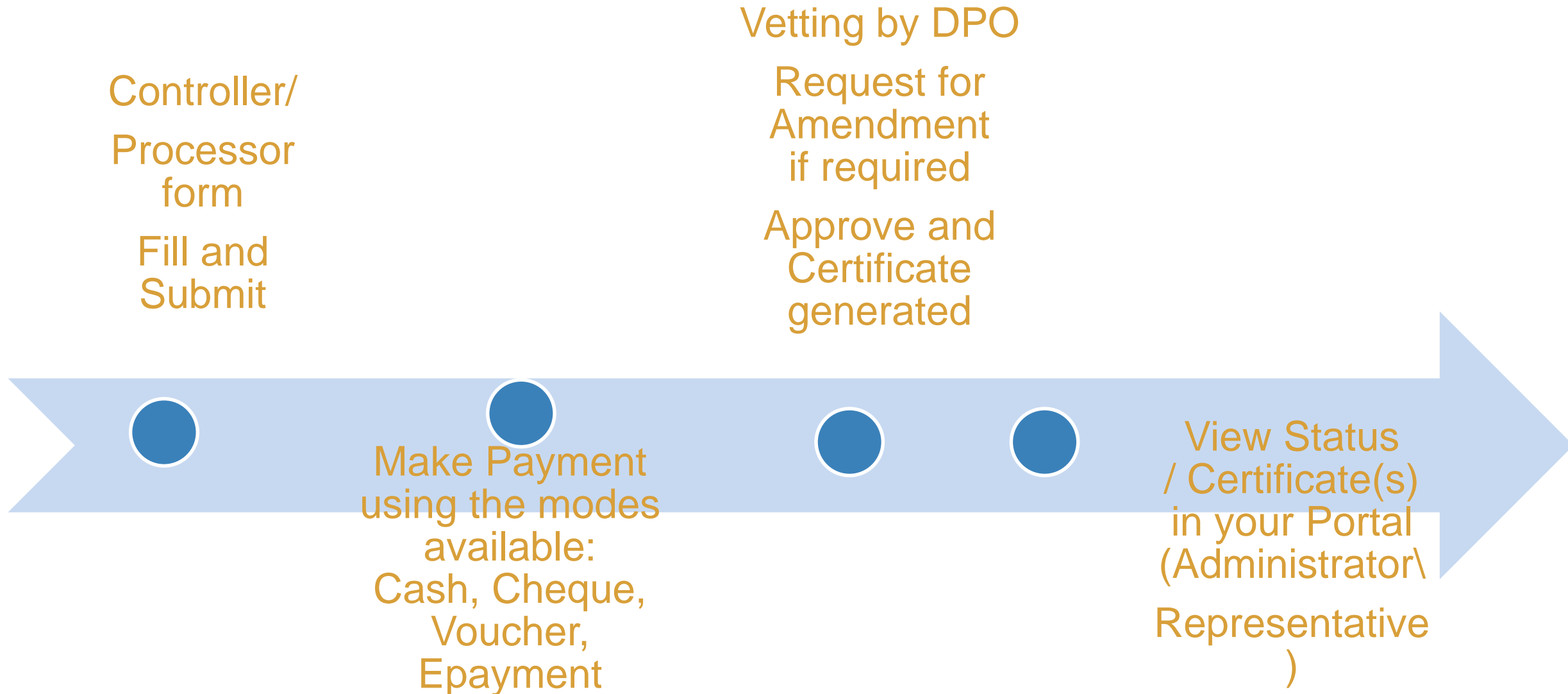
Log in
as
Administrator
account other
than Individual
(3 types)
Scenario

- 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 Application Process



Epayment



DATA PROTECTION OFFICE



Home

Register New Controller

Register New Processor

Renew Application

Controller

Processor


Query Complaints

Transactions

DRAFT APPLICATIONS

No records found.


PENDING FEES

 Click to Pay

DPO/2022/09/0091

New Controller for [Redacted] & CO LTD

Amount: 1000.00

 Click to Pay

DPO/2022/09/0082


New Controller for [Redacted] Ltd

Amount: 1000.00

REGISTERED CERTIFICATES


C10020

Controller for [Redacted] Limited

 View Certificate

C10021

Controller for [Redacted] CO LTD

 View Certificate

C10022

Sample Portal View (status/certificate)

Home

Manage Representatives

Register New Controller

Register New Processor

Renew Application

Controller

Processor

Query Complaints

Transactions


Controller Applications


Reference ↑↓	Application Type ↑↓	Controller Name ↑↓	Representative Name ↑↓	Status ↑↓	Edit Application	Application	Certificate
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>			
DPO/2022/08/0004	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/08/0001	Controller	[REDACTED]	[REDACTED]	Application Submitted			
DPO/2022/09/0031	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/10/0101	Controller	[REDACTED]	[REDACTED]	In Process			
DPO/2022/08/0019	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/09/0033	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/10/0105	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/10/0107	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/10/0106	Controller	[REDACTED]	[REDACTED]	Completed			
DPO/2022/10/0108	Controller	[REDACTED]	[REDACTED]	Completed			

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


Data Protection Office



[Home](#)

[Register New Controller](#)

[Register New Processor](#)

[Renew Application](#)

[EForms](#)

[Controller](#)

[Processor](#)

[Complaints](#)

[Transactions](#)

DPO PORTAL

LOGOUT

Registration of ONLINE Complaint

[Complainant](#) [Respondent](#) [Complaint Details](#) [Declaration](#) [Documents](#)

NID :

M0

First Name :

Mr X

Block / House No. :

Locality :

Select

District :

Select

Email Address :

dpoyep@govmu.org

Phone No :

Last Name :

YYYYYY

Street :

Town / Village :

Postcode :

Select

Occupation :


Mobile No :


[← Back](#) [Save as Draft](#) [Print](#)

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


Data Protection Office



[Home](#)

[Register New Controller](#)

[Register New Processor](#)

[Renew Application](#)

[EForms](#)

[Controller](#)

[Processor](#)

[Complaints](#)

[Transactions](#)

DPO PORTAL

LOGOUT

EForms

+ Transfer of Personal Data Abroad

+ Notification of Personal Data Breach

+ Data Protection Impact Assessment

+ Compliance Audit

+ Certification Form

Reference ↑↓

Category ↑↓

Submitted Date ↓

Status ↑↓

View

Letter

No records found.

<<

<

>

>>

10 ▾

Action Required and Response for Eforms

APPLICATION CERTIFICATION FORM

Ref Number: CERT/2022/1

Particulars of controller/processor Details Documents Action Required

Controller / Processor Certificate :

Name of controller/processor* :
(Please tick whether application is by controller/processor)

Name of controller :
(Please specify name of controller if application is being done by processor)

Block / House No. : Street* :

Locality* : Town / Village :

Action Required Notes

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 requested by DPO
- ▷ **Approved:** The eform is approved
- ▷ **Rejected:** The eform is rejected

Eform status in eDPO portal

EForms

+ Transfer of Personal Data Abroad		+ Notification of Personal Data Breach		+ Data Protection Impact Assessment	+ Compliance Audit	+ Certification Form
Reference ↑↓	Category ↑↓	Submitted Date ↓↕		Status ↑↓	View	Letter
DRAFT/2022/14	Certification Form			Draft		
DRAFT/2022/10	Data Protection Impact Assessment			Draft		
DRAFT/2022/15	Certification Form			Draft		
DRAFT/2022/16	Certification Form			Draft		
DRAFT/2022/19	Notification of Personal Data Breach			Draft		
DRAFT/2022/5	Transfer of Personal Data Abroad			Draft		
DRAFT/2022/25	Data Protection Impact Assessment			Draft		
DRAFT/2022/27	Data Protection Impact Assessment			Draft		
BREA/2022/7	Notification of Personal Data Breach	28/11/2022		Action Completed		
DPIA/2022/2	Data Protection Impact Assessment	28/11/2022		In Process		

DPO Portal User Guide

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.

Multistakeholder

- A multi-stakeholder body with representatives from key government agencies, private sector and civil society

Name	Organisation
Dr Viv Padayatchy	Chairperson
Mr R.Hawabhay	Chief Technical Officer, Ministry of Information Technology, Communication and Innovation
Mrs. D.Madhub	Data Protection Commissioner Data Protection Office
Mr C.Dawonauth	Superintendent of Police
Dr K.Usmani	Officer in Charge CERT-MU
Mr J.Louis	Officer in Charge Information and Communication Technology Authority
Mr. Q.A Ismael Ghanty	Chief Information Security Officer Bank of Mauritius
Mr. Arvind Jadoo	Chief Information Security Officer Financial Services Commission
Mr Pravesh Gaonjur	General Manager, Tylers
Mr Amreesh Phokeer	Internet Measurement and Data Expert Internet Society (Global) Mauritius
Mrs P.Sohun	Deputy Permanent Secretary, Prime Minister's Office
Mr A. Auckloo	Technical Security Analyst, Cyber Terrorism Unit
Mr M.Seetaram	Ag Senior Assistant Parliamentary Counsel State Law Office

The National Cybersecurity Committee

Additional Resources

- The Committee may co-opt any person who may be of assistance in relation to any matter before it



The National Cybersecurity Committee

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 Gov Policy

- 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 wish to bring such matters to the committee's attention

Critical Information Infrastructure

- 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;



MAUSHIELD

Mauritius Cyber Threat Information Sharing Platform

[Home](#)

[About Us](#)

[Membership](#)

[Cyber Threats](#) ▾

[Threat Alerts](#)

[Cybersecurity Trends](#)

[Threat Maps](#)

[Contact Us](#)

[Sign In](#)

MAUSHIELD Membership Programme

MAUSHIELD Membership Program is free and open to organisations in the public and private sectors, including critical sectors and academia. Register to become a member of MAUSHIELD

[Register Now](#)

Copyright Data Protection Office

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

Best Practices

- establish cybersecurity best practices and standards for critical information infrastructures;

CC work on selecting best practices such as ISO27001 protocols for CII





Capacity Building

- 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.

Work done

- 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

A large, solid orange circle occupies the left side of the slide, partially cut off by the edge.

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 (MloD)



30 January 2023

Safe City

Mr. Bholah
Superintendent of Police
Mauritius Police Force

30 January 2023





Police Main Command and Control Centre (PMCCC)

Welcome

“PROTECTING PERSONAL DATA ACROSS ALL ECONOMIC SECTORS”

Mr. A. BHOLAH
Superintendent of Police
OC PMCCC

Shri Atal Bihari Vajpayee Tower, Ebène

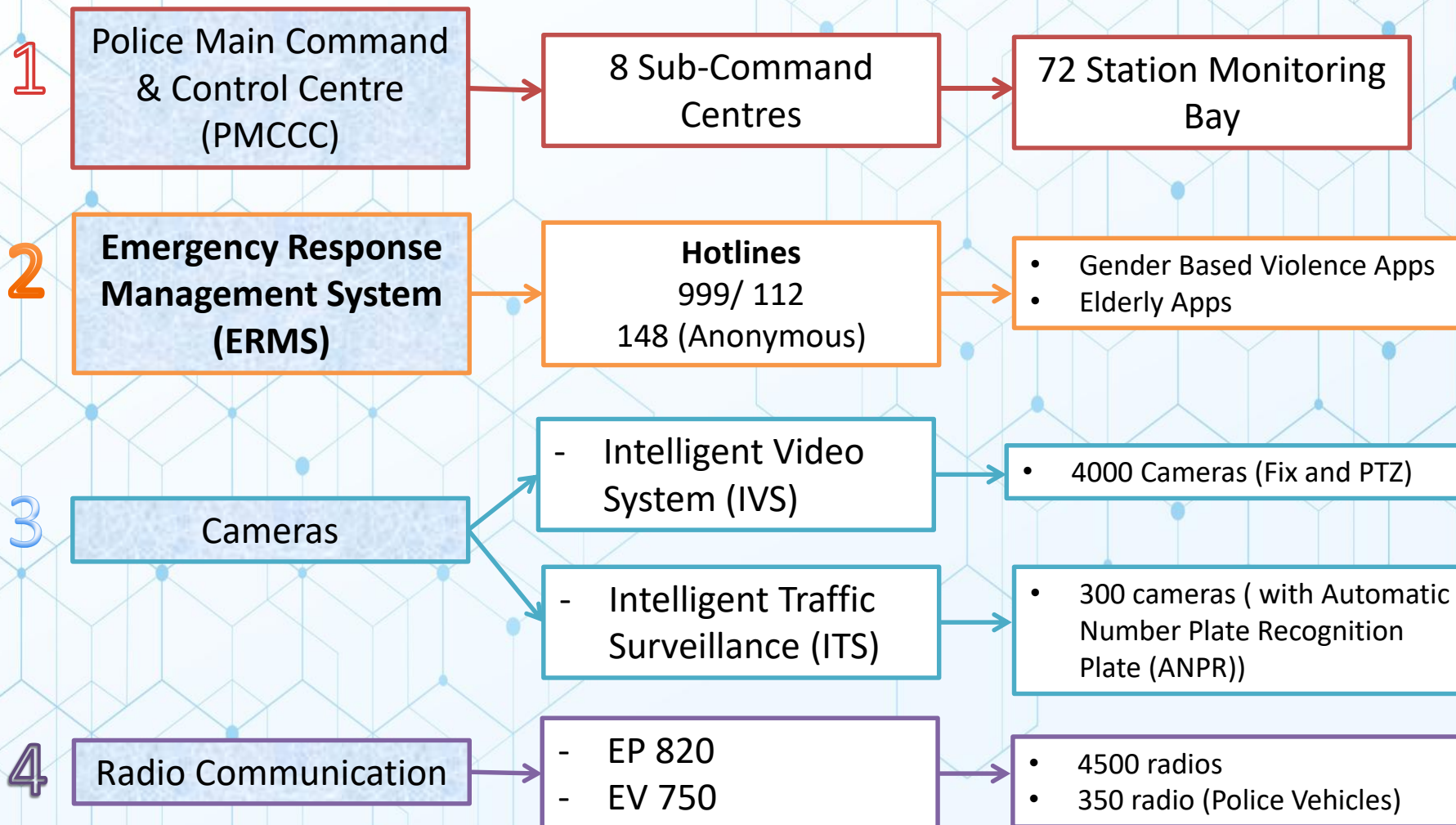
Safe City



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.

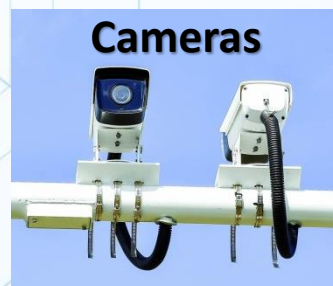
The Project consist of four components:



Personal Data are captured through ...



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



Cameras

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

Radio



- ✓ Voice
- ✓ Video
- ✓ Snapshot

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

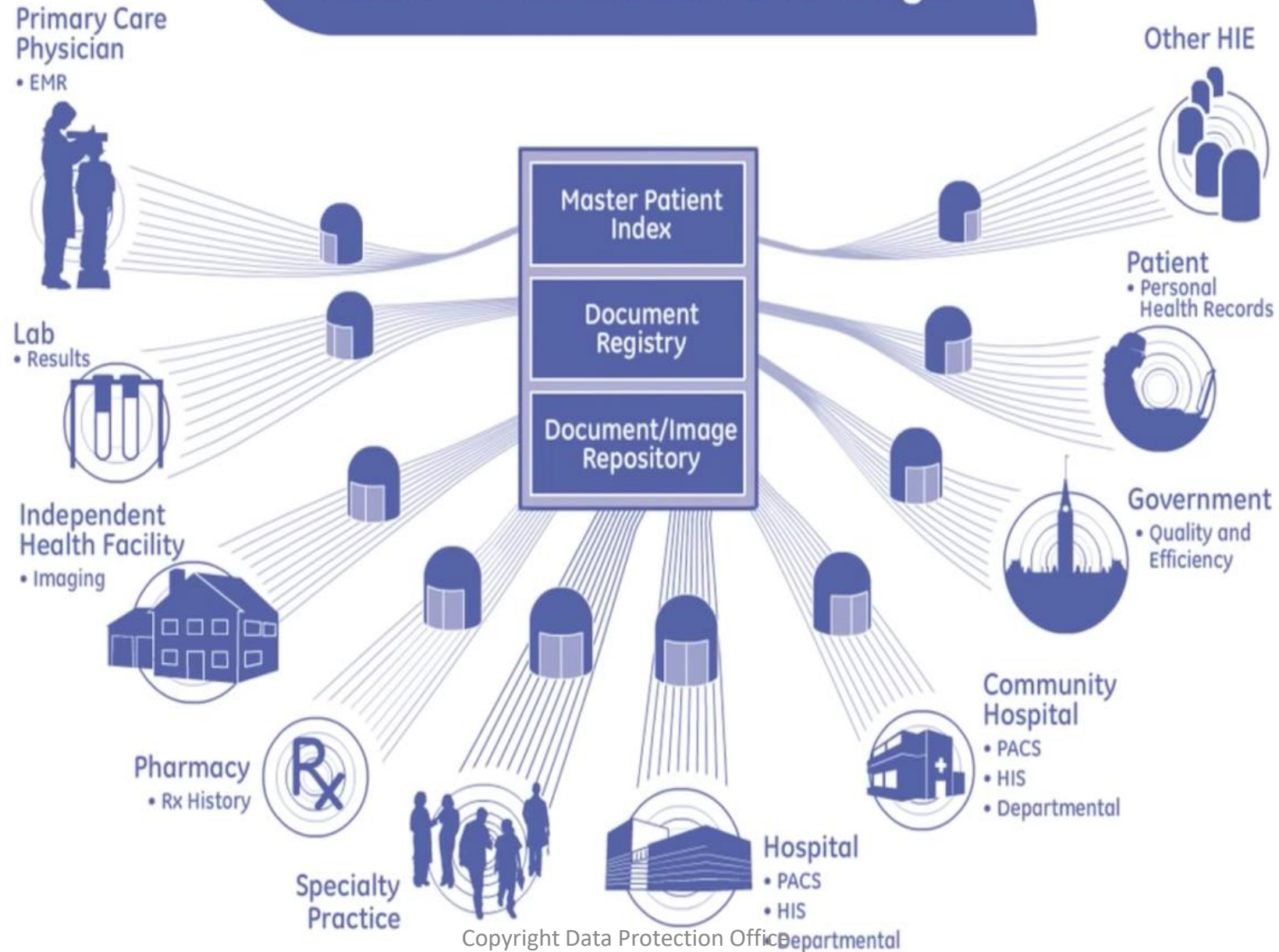
Dr. A. Bholah

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

30 January 2023



Health Information Exchange



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



Examples:

- Risk assessment
- Assigning a privacy official
- Staff training

Physical



Examples:

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

Technical



Examples:

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



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	[REDACTED]
User ID	[REDACTED]
Health	type 1 diabetes



Anonymous data

IDs removed & sensitive data randomised/generalised.

Sex	Male
Age	30-49
Health	type 1 diabetes

PSEUDONYMIZATION

Personal
information

Jane Doe



Key



Pseudonymized
data

De2b f1_

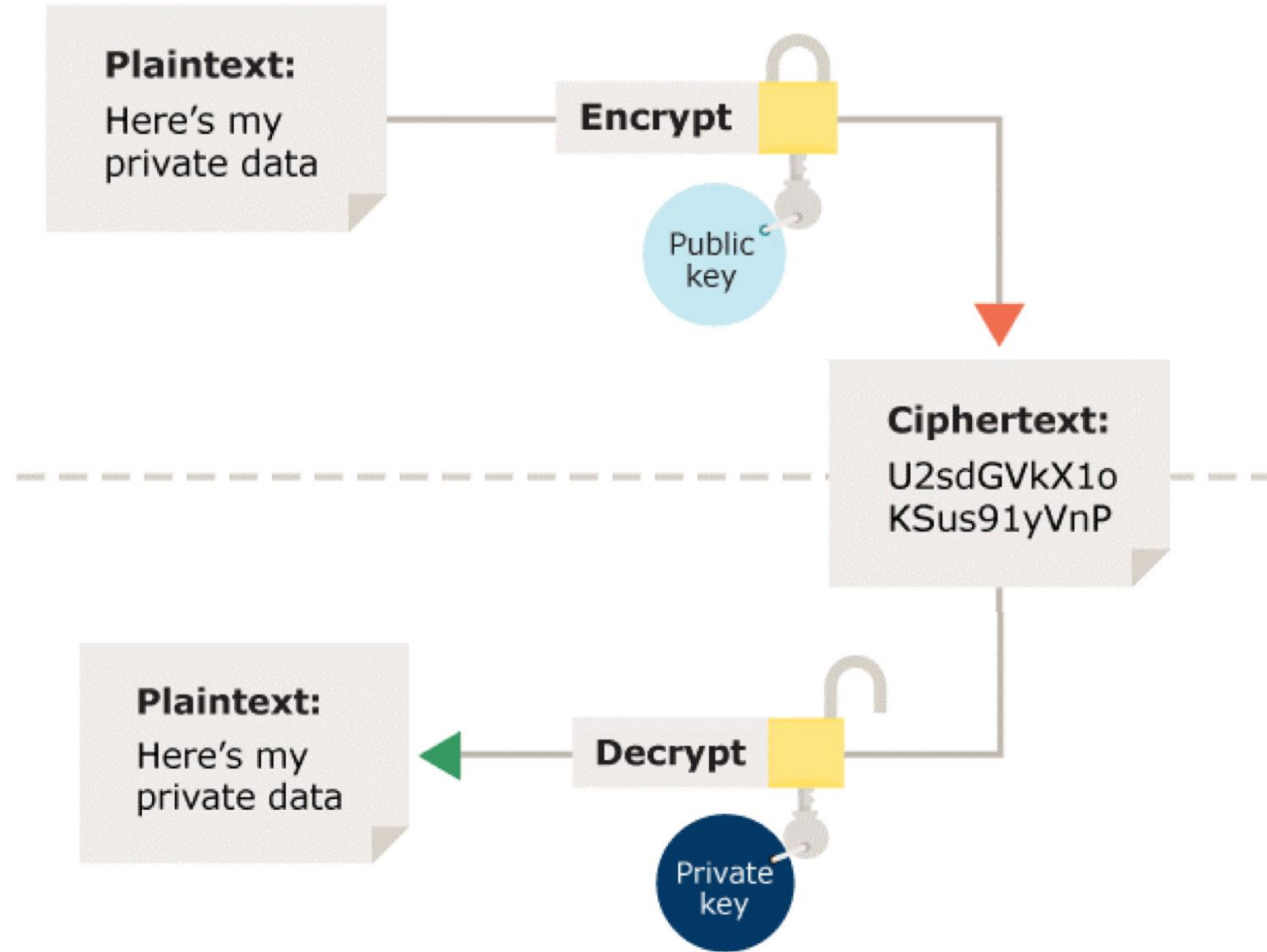
ANONYMIZATION

Personal
information

Jane Doe



Anonymized
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



Absa Bank Mauritius Limited

Bringing Possibilities to Life



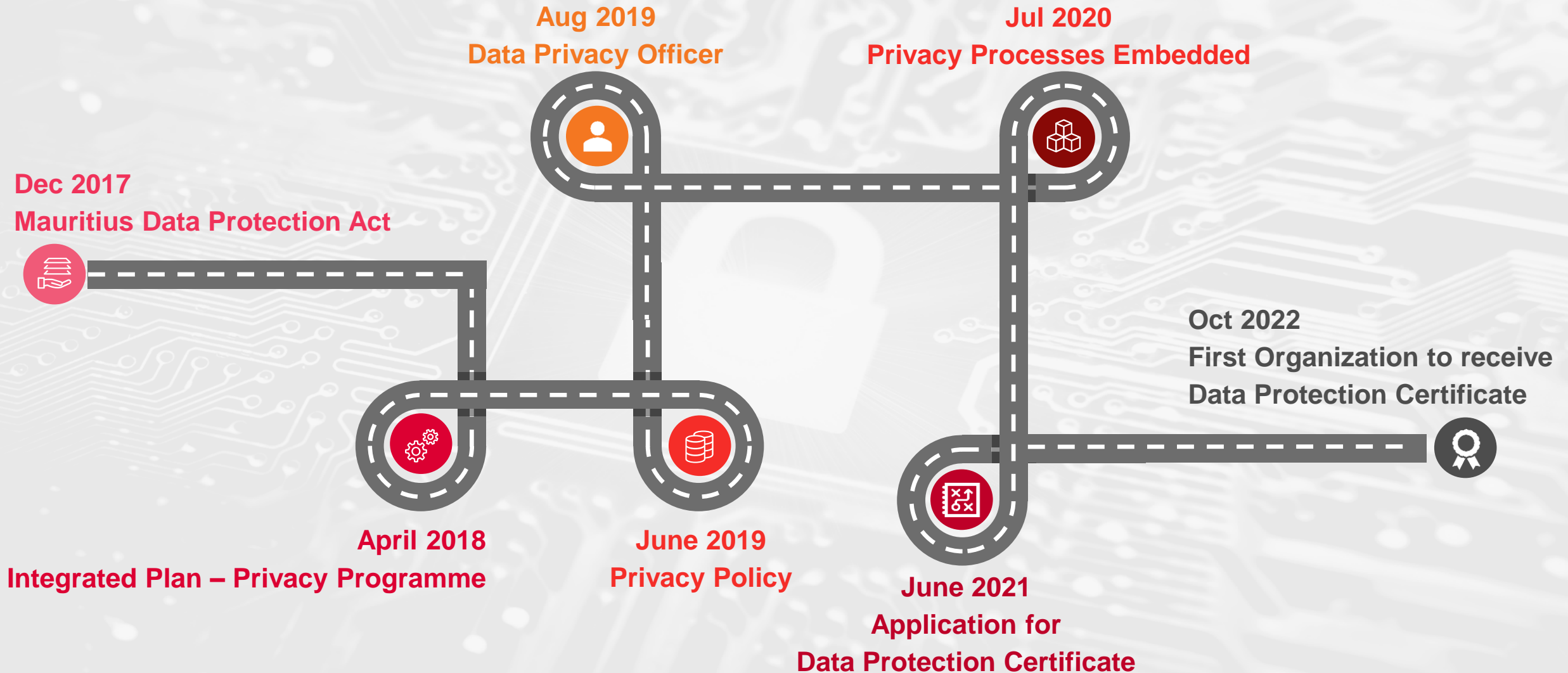
Our Journey to the Data Protection Certification

Kevin Sumputh

Chief Security Officer, Absa Bank Mauritius Limited

30 January 2023

The Data Protection Journey of Absa Bank Mauritius Limited



The Integrated Plan – Privacy Programme (2018- 2020)



Data Protection Certification (2021-2022)



Areas covered in the Application for Certification Form

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

Our Challenges...

Conditions for Consent <ul style="list-style-type: none">• Is consent verifiable?• Is consent easy to withdraw	Records of Processing <ul style="list-style-type: none">• Are records of all processing operations maintained?	Data Protection Impact Assessment <ul style="list-style-type: none">• Must be completed for high risk operations.	Rectification, erasure or restriction of processing <ul style="list-style-type: none">• Erasure or Restriction of processing?• Bank of Mauritius requirements (7 years)	Right to object <ul style="list-style-type: none">• Personal data should no longer be processed
--	---	--	---	--

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



IMPORTANCE OF DATA PROTECTION



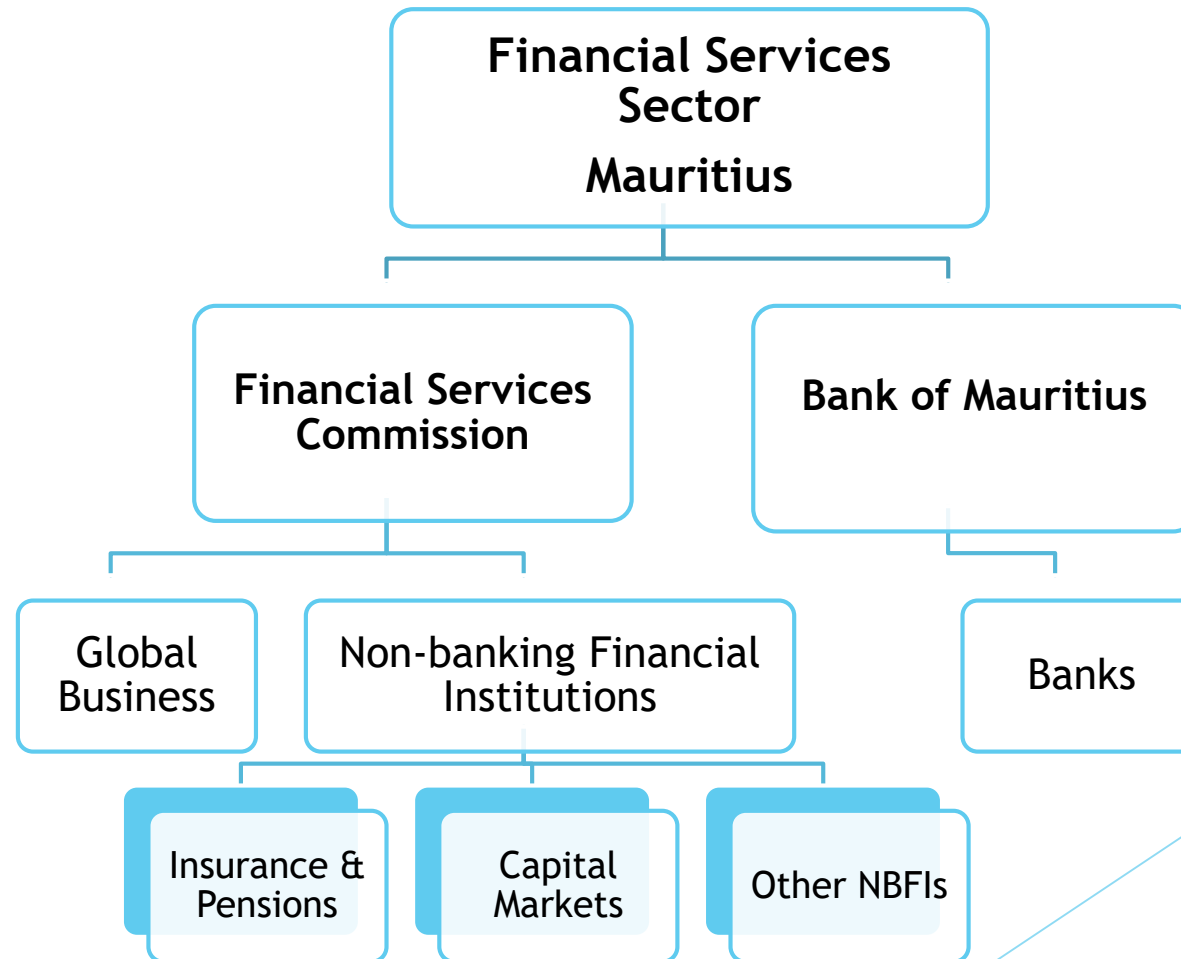
POWERPOINT PRESENTATION
ON
IMPORTANCE
OF
DATA PROTECTION IN the FINANCIAL SERVICES SECTOR

*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

Mixed legal system: civil and common law

Right of appeal to Judicial Committee of the Privy Council

Confidentiality (with transparency) for Global Business

- 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)

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 :

Long term Insurance , General Insurance Business ,External Insurance Business (non- Mauritian Policies) , professional reinsurer, insurance agent, broker, salesperson

- ▶ 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
- 6141 Authorised Companies
- 1318 domestic entities (excluding insurance salespersons)

Source : Statistics Mauritius - National Accounts - December 2022 Issue

- Contribution to the Consolidated Fund

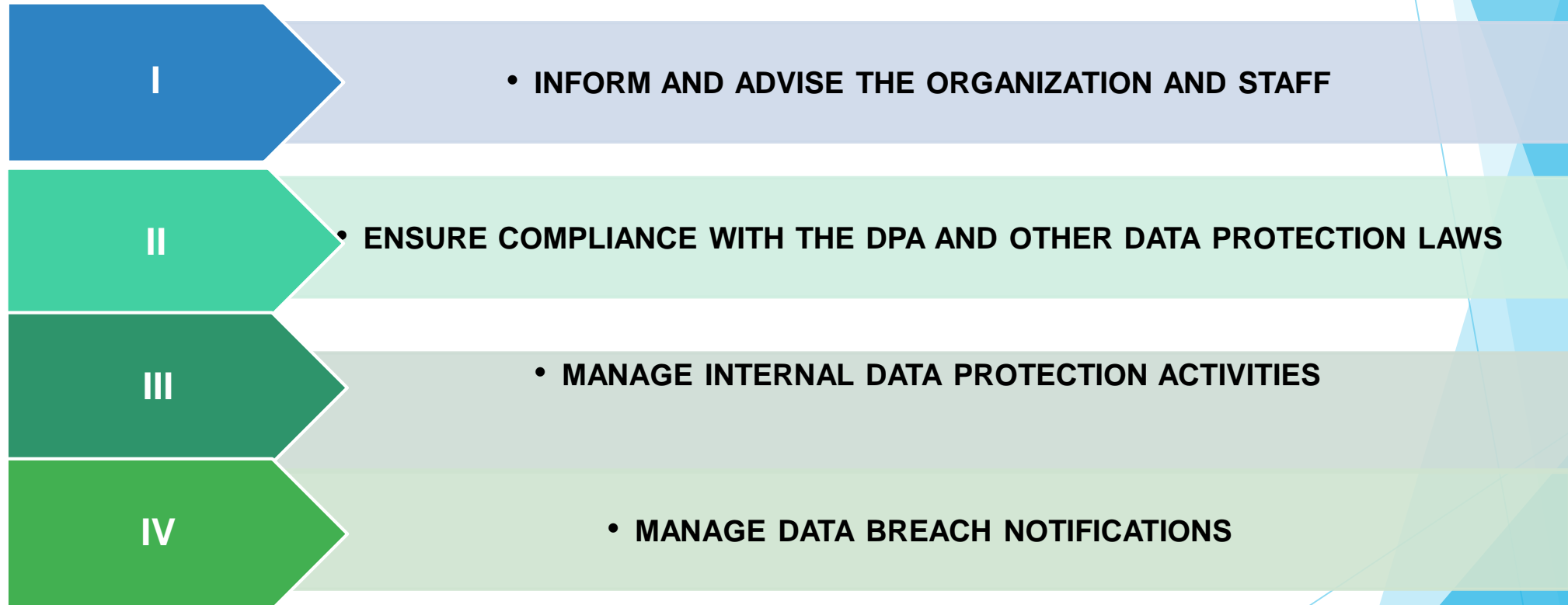
Challenges in the Financial Services sector

- 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.

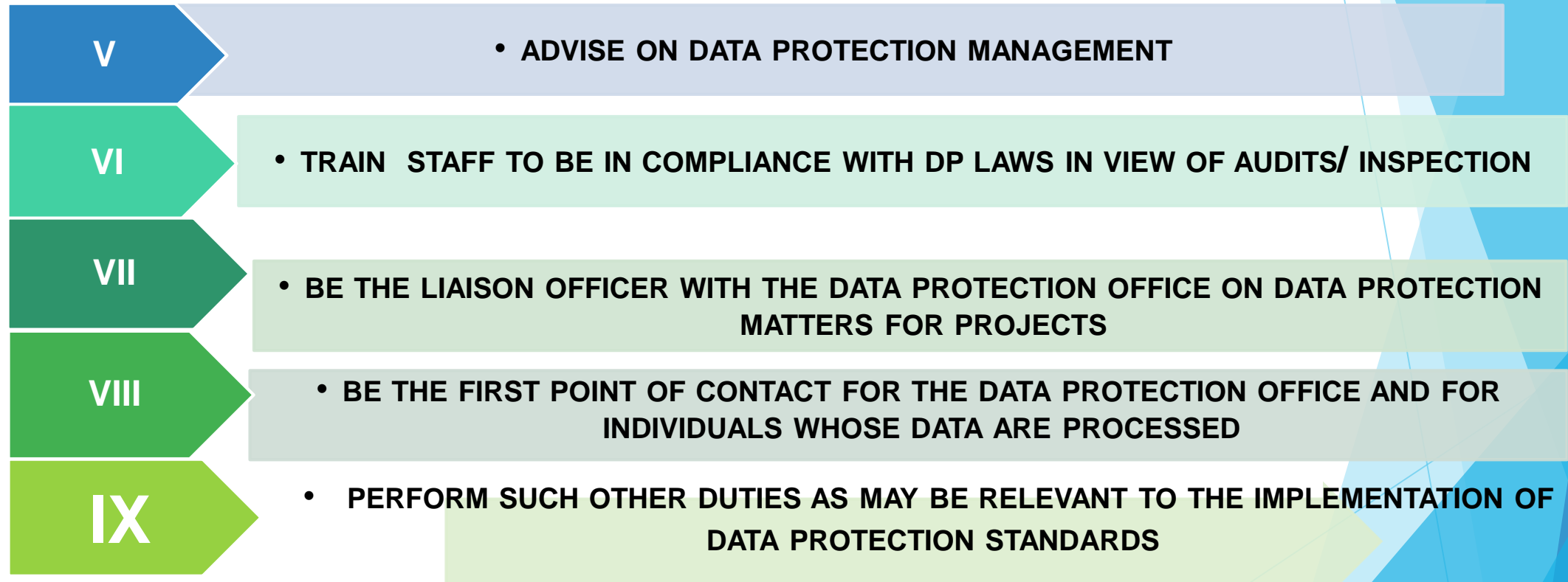
Impact of EU GDPR on the Financial Services sector

- ▶ **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



FUNCTIONS OF FSC DATA PROTECTION OFFICER



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 :**

Copyright Data Protection
“The Company shall adopt cyber security and data protection best practices as part of its ongoing obligations.”

FSC & Importance of Data Protection (2)

- 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/>
- 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

Copyright Data Protection Office

THINK TWICE AWARENESS CAMPAIGN



Data Protection Videos



Interview with the Data Protection
Commissioner



Screensaver



Posters

Copyright Data Protection Office



THINK TWICE VIDEOS

Copyright Data Protection Office



Interview with the Data Protection Commissioner



Copyright Data Protection Office





Breaches
have consequences

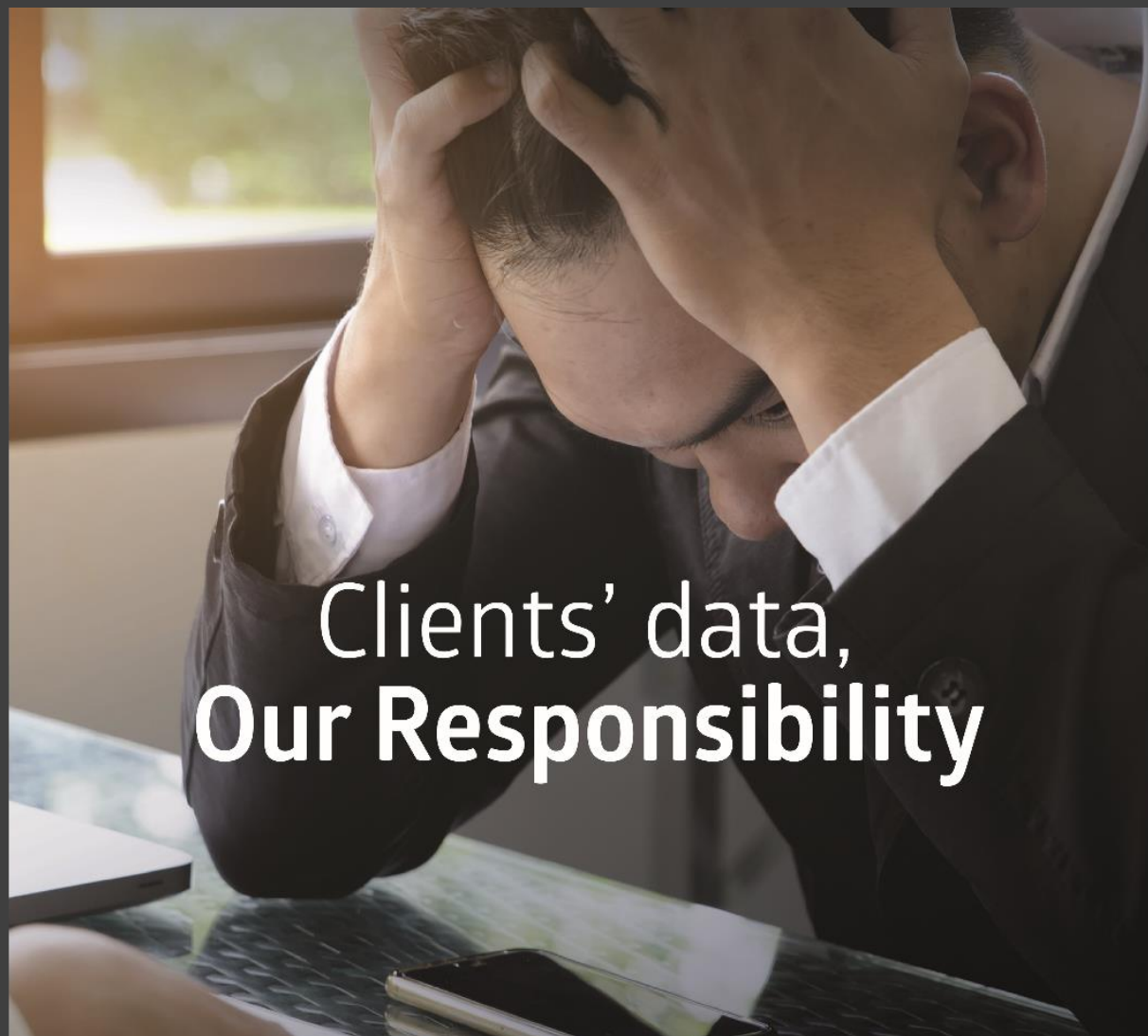


**think
twice**
by SWAN

Thumbs up for the wonderful job
you do for being **Compliant**

Together, let's protect **SWAN**

Copyright Data Protection Office



Clients' data,
Our Responsibility



Red Flags

Red flags are signs of danger or a problem. Protect yourself and your organization from cybercriminals by being aware of these warning signs and knowing actions to stay safe.



Common Red Flags

- Someone you don't know following you or your co-workers inside the office.
- Someone looking at your screen or watching what you type.
- Someone you don't recognise looking through a desk.
- Social media connection requests from someone you don't recognise.
- Receiving an unusual request from someone you know.
- Requests that offer you something in exchange for private organizational information.
- Unexpected emails, phone calls, and voice or text messages.
- Urgent requests to take an action.



Actions to Stay Safe

- Contact security about unknown individuals.
- Pay attention to your surroundings and safeguard organizational information.
- Keep confidential information and devices locked up/ secured when not in use.
- Don't accept unsolicited requests; report them to the service.
- Contact the person directly to verify it's legitimate.
- Be cautious before sharing any personal or organizational information.
- Follow your organization's security policies for handling suspicious correspondences.
- Never act on emotion and take the time to verify the request is legitimate.

Always stop, look, and think before you click on a link, open an attachment, or take any action!



Browser push notifications are small messages that deliver information to users. If the website requests it, web browsers will prompt the visitor to block or allow notifications. If allowed, the site will then be permitted to send messages directly to the user's computer, even when not visiting the site in question. Most often, these notifications can serve useful purposes, they're also abused by malicious hackers. Security researchers have identified that push notifications can be used to:

- Deliver excessive advertisements
- Display inappropriate content
- Send malicious advertisements, known as malvertising
- Trigger installation of unwanted software

How can you avoid falling victim to malicious browser notifications?

Click with Caution

Carefully review what any prompt or pop up is asking for, and only allow notifications for websites you trust. Think before you click!

Review Permissions

Most web browsers keep a list of the websites that have push notifications permitted. You can review and remove permissions in the privacy and security settings of your specific browser.

Disable Notifications

Depending on which browser you use, there may be an option to globally block push notifications. It's best to enable this option and manually add notifications as needed.

Stay Updated

Software updates are often used to fix bugs and patch security vulnerabilities. It's wise to enable automatic updates so your web browser is always on the latest version.

Follow Policy

Only use approved browsers and software. Never change settings or install extensions without asking. Doing so adds unnecessary risk and could lead to data theft.

Push notification may not come across as an alarming threat, but in a world where attackers are looking for every advantage, it's vital that we address every potential weakness in the security chain.

Always stop, look, and think before you click on a link, open an attachment, or take any action!



CYBER SECURITY AWARENESS

Copyright Data Protection Office