Data Protection Office

Workshop on DATA PROTECTION

Mauritius Police Force

Presented By:
Mrs. D. Madhub
Data Protection Commissioner
15 May 2019

Agenda

- The Data Protection Act (DPA)
- The Data Protection Office (DPO)
- Some definitions
- Functions and Powers of DPC
- Powers of authorised officers
- Delegation of powers
- Investigation and Conduct of hearings
- Obligations on Controllers and Processors
- Rights of data subjects
- Offences and penalties
- Exceptions and Restrictions
- Use of CCTV cameras
- Disclosure of personal data and sharing
- Questions raised by Police

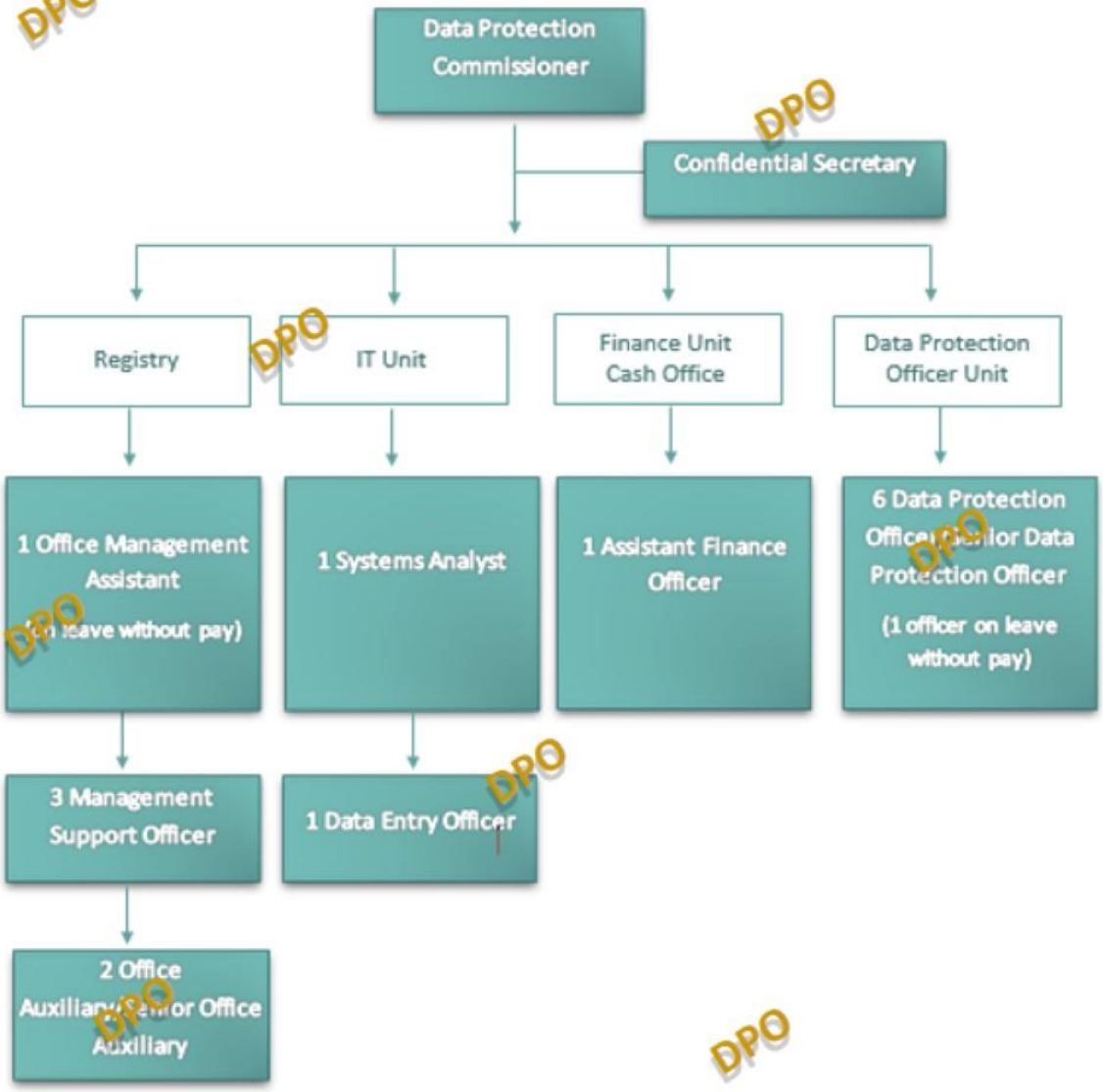
The Data Protection Act (DPA)

- First Enacted in 2004.
- Amended in 2017 to become a new and improved legislation namely, the Data Protection Act 2017 which came into force on 15 January 2018.
- Regulates the processing of personal data.
- Makes provisions also about the functions, powers of the office, enforcement and application of the legislation.

The Data Protection Office (DPO)

- Public office in operation since February 2009.
- Completely **independent** and **impartial** and not subject to the control or direction of any other person or authority in the discharge of its functions.
- Aim is to protect privacy rights of individuals.
- Head is the Data Protection Commissioner.

Structure of DPO



Some basic definitions

Section 2

Basic definitions

Personal data

- any information relating to a data subject.

Data Subject

- an identified or identifiable individual (any data which can identify an individual),
- in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Basic definitions

Processing

- an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction**.

Controller

- a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.

Processor

- a person who, or a public body which, processes personal data on behalf of a controller.

Functions and Powers of DPC

Sections 5 to 10

Functions and Powers of the DPC

The DPC is responsible for ensuring that people's rights are respected, and that the persons who keep personal information on computer or in manual format meet their responsibilities.

To assist the DPC in exercising these functions, she is assigned certain important powers under the DPA.

Functions of the DPC(s5)

Ensure compliance with DPA and the regulations
Issue or approve Codes of Practice or Guidelines
Maintain a register of controllers and processors
Exercise control on all data processing operations and verify whether they are done in accordance with DPA
Promote self-regulation among controllers and processors
Investigate any complaint
Undertake research into, and monitor developments in, data processing and ensure there is no risk or adverse effect to privacy of individuals
Examine any proposal for automated decision making or data linkage that may involve an interference or have an adverse effect with privacy of individuals

Investigation of complaints(s6)

Any data subject has the right to lodge a complaint if he thinks that a person or organisation is not meeting their data protection obligations, and the DPC has the legal power to enquire or delegate an authorised officer to look into the matter. The DPC may decide not to investigate a complaint if she thinks the complaint is frivolous or vexatious.

Following receipt of a complaint, this office initiates an enquiry, in the course of which concerned parties may be required to attend hearings or to produce a document or other material.

Investigation of complaints(s6)

An investigation can result in either :

- An amicable resolution between the parties concerned
- An offence being filed at the Office of the Director of Public Prosecution where the latter will decide if the offence has to be tried or not before a court.

Investigation of complaints(s6)

Is the Decision of the Commissioner appealable?

Yes, it is appealable at the ICT Appeal Tribunal set up under section 35 of the Information and Communication Technologies Act.

Any person who feels aggrieved by the DPC's decision has a right of appeal to the ICT Appeal Tribunal. He has to do so within 21 days from the date when the decision is made known to him.

Power to require information (s7)

The DPC may require any person to provide him with whatever information he needs to carry out his functions or exercise his powers by providing a written notice to the person.

Failure to comply with such a notice without reasonable excuse or knowingly to provide false information, or information that is misleading in a material respect, in response to the notice is an offence.

Preservation order(s8)

The DPC may apply to a Judge for a Preservation Order order for the expeditious preservation of data where he has reasonable grounds to believe that such information is vulnerable to loss or modification.

Where the Judge is satisfied that a Preservation Order may be made, it shall issue a preservation order specifying a period which shall not be more than 90 days during which the order shall remain in force.

The Judge may, on application made by the DPC extend the period specified for such time as the judge thinks fit.

Enforcement notice(s9)

The DPC may require a controller or processor to take whatever steps considered necessary to comply with the terms of the DPA. The DPC exercises this power by providing a written notice, called an "enforcement notice" to the controller or processor.

It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

E.g. Enforcement notices are sent to organisations or persons who fail to register as controller or renew their registration as required under s14.

Power to seek assistance(s10)

For the purpose of gathering information or for the proper conduct of any investigation under the DPA, the DPC may seek the assistance of such person or authority as he thinks fit and that person or authority may do such things as are reasonably necessary to assist him in the discharge of his functions.

Powers of Authorised Officers

Section 11 and 12

Power of entry and search(s11)

An authorized officer may enter and search premises to carry out his functions e.g. investigation by seeking a warrant from a Magistrate.

The authorized officer has the power to request the owner or occupier to produce document, record or data; examine any such document, record or data and take copies or extracts from them, to give all reasonable assistance and to answer all reasonable questions, orally or in writing.

Obstruction of Commissioner or authorised officer(s12)

It is an offence to:

a. obstruct or impede the Commissioner or an authorised officer in the exercise of such power;
b. fail to provide assistance or information requested by the Commissioner or authorized officer;
c. refuse to allow the Commissioner or an authorized officer to enter any premises or to take any person with him in the exercise of his functions;
d. give to the Commissioner or an authorized officer any information which is false or misleading in a material particular.

Delegation of powers

Section 13

Delegation of power by Commissioner(s13)

The Commissioner may delegate any investigating or enforcement power conferred on him by this Act to an officer of the Office or to a **police officer** designated for that purpose by the Commissioner of Police.

As such, police assistance is required:

- **To deal with controllers and processors who are contravening the DPA,**
- **To prepare and swear an information in respect of an offence under the DPA or any regulations made under it before a Magistrate and prosecute the case,**
- **To assist in search of premises in the conduct of investigations,**
- **To file warrants,**
- **To carry out site visits,**
- **To record statement.**

Obligations on controllers and processors

Sections 21 to 33

Obligations on controllers and processors

Registration and renewal as controller and/or processor (s 14)	1. Application forms available on DPO website. 2. Guidance on registration and renewal on DPO website.
Comply with the 6 principles for processing personal data (s 21)	1. Lawful, fair and transparent 2. Purpose limitation 3. Data minimisation 4. Data accuracy 5. Storage limitation 6. In accordance with the rights of data subjects.
Duties of controller (s 22)	1. Adopt policies and implement appropriate data security and organisational measures. 2. Designate a Data Protection Officer. 3. Verify the effectiveness of measures implemented.
Collection of personal data (s 23)	Done for a lawful purpose and is necessary.
Conditions for consent (s 24)	1. A controller bears the burden of proof for establishing consent. 2. An individual can withdraw his consent anytime. 3. Consent is presumed not freely-given if the performance of a contract/service is dependent on the consent which is not necessary for such execution of the contract/service.

Obligations on controllers and processors

Notification of personal data breach (s 25)	**1. To notify the Data Protection Office where feasible not later than 72 hours after becoming aware.** **2. Form available on DPO website.**
Communication of breach to data subject (s 26)	**Where it is likely to result in a high risk to the rights and freedoms of the data subject.**
Duty to destroy personal data (s 27)	**1. To destroy personal data as is reasonably practicable when the purpose has lapsed.** **2. To notify any processor holding the data for destruction.** **3. Retention period has to be determined by controllers taking into account the purpose and other applicable laws.**
Lawful processing (s 28)	**Must meet at least one criteria for lawful processing.** 9 criteria – (1) consent (2) contract (3) legal obligation (4) vital interest of data subject (5) official authority vested in the controller (6) a task carried out by a public authority (7) exercise, by any person in the public interest, of any functions of a public nature (8) legitimate interests of the controller which do no override the rights and freedoms of data subjects (9) historical/statistical or scientific research
Special Categories of personal data (s 29)	**Must implement specific protection and a stricter regime.**
Personal data of child (s 30)	**Parental or guardian consent must be obtained for processing the personal data of children under the age of 16.**

Obligations on controllers and processors

Security of processing (s 31)	**Implement appropriate security and organisational measures.**
Record of processing operations (s 33)	**Template available on DPO website.**
Processing operations likely to present risk to individuals (s 34&35)	**1. Guidance on how to evaluate high risk processing operations.** **2. Perform a DPIA.** **3. DPIA form available on DPO website.** **4. Comply with the requirements for prior authorisation from, or consultation with the Commissioner.**
Transfer of personal data outside Mauritius (s 36)	**If a controller or processor cannot provide proof of appropriate safeguards or cannot rely on any of the exceptions provided in section 36(1) (Consent from individual, Contract with individual, Public interest, Legal claim, Vital interest and Legitimate interest), then authorisation from the Data Protection Commissioner is required for the transfer.**

Rights of Data Subjects

Sections 37 to 40

Rights of Data Subjects

Right of access – s37

- A data subject has the right to obtain confirmation that his/her personal data is processed and a copy of the data free of charge within one month following a written request.

Automated individual decision making – s38

- A data subject has the right not to be subject to a measure which is based on profiling by means of automated processing.
- Can be carried out by controller if necessary for contract, authorised by law or based on explicit consent of the data subject.

Rectification –s39

- A data subject has the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her.

Rights of Data Subjects

Erasure – s39

- Data subject may request that his/her personal data are erased if the continued processing of those data is not justified

Restriction of Processing – s39

- A data subject may request that the processing of his/her personal data is restricted where the accuracy of the data is contested.

Object – s40

- A data subject has the right to object in writing at any time the processing of personal data relating to him/her free of charge.

Offences and Penalties

Section 43

Offences and Penalties (s43)

- There are various offences and criminal penalties under this Act which, in general if committed, are sanctioned by a court of law.

- Where no specific penalty is provided, any person who does not comply or contravenes this Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

Other Offences and Penalties

Offences	Penalties
Section 6: Investigation of Complaints Any person who fails to attend a hearing or to produce a document or other material when required to do so.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7: Power to require information Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 15: Application for registration Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular.	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 17: Change in particulars Any controller or processor who fails to notify a change in particulars.	Liable to a fine not exceeding 50, 000 rupees.
Section 28: Lawful processing Any person who process personal data unlawfully.	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

Exceptions and Restrictions

Section 44

Exceptions and Restrictions (s44)

- Processing of personal data by an individual in the course of a purely personal or household activity.
- For the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty.
- An objective of general public interest, including an economic or financial interest of the State.
- The protection of judicial independence and judicial proceedings.
- The protection of a data subject or the rights and freedoms of others
- Subject to section 44(4):
  - For the protection of national security, defence or public security

A certificate under the hand of the Prime Minister certifying that the non-application of the provision is required for the purpose of safeguarding national security, defence or public security shall be conclusive evidence of that fact.

Use of CCTV cameras

- CCTV recordings also fall within the scope of personal data since individuals can be identified from them.
- The DPO issued a code of practice under the Data Protection Act 2004 covering the use of CCTV in 2009.
- Conditions for using CCTV cameras:
  - there must be a genuine reason for installing the CCTV camera system (conditions under section 28 or 44 apply)
  - the purpose for its use must be displayed in a prominent position
  - signage must be used to inform the public of the location of cameras
  - CCTV footage must not be used for any purpose other than that stated
  - CCTV footage must not be accessed by or disclosed to unauthorised people

Case Law on CCTV cameras

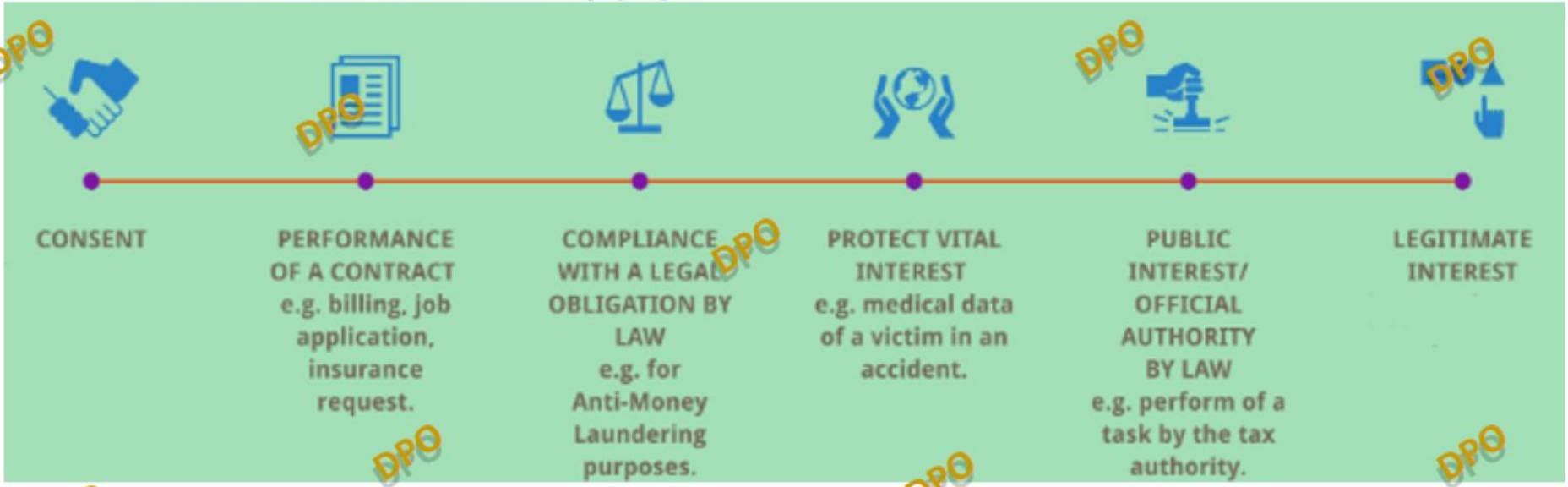
Ryneš v UPOOU

- Mr Rynes installed CCTV cameras as a result of numerous attacks on his property. The CCTV covered the entrance of his home, a public footpath and the neighbour's house opposite his property. On one occasion, Mr Rynes property was attacked and the CCTV captured the identity of the attackers. The CCTV recording was provided to the police for prosecution purposes.
- One of the attackers raised the question with the Czech Office for Personal Data Protection as to whether the use of the CCTV data was lawful as it recorded personal data of him on a public footpath which he had not consented to. The Czech Office found that Mr Rynes use of the CCTV was unlawful in accordance with the Data Protection Directive (Directive) and he was fined.
- Mr Rynes appealed to the Supreme Administrative Court arguing that his use of the CCTV fell within the 'domestic' exception provided by the Directive, namely that the recording was made by a natural person 'in the course of purely personal or household activities'. The Supreme Administrative Court turned to the ECJ to give a preliminary ruling on the issue.
- The ECJ ruled that a domestic CCTV installed for the protection of the property, health and life of the installer and his family which also monitors a public space does not fall within the 'domestic' exception and the obligations set out in the Directive would apply to the data controller. The ECJ briefly referred to point that the processing of data (e.g. by CCTV) could be lawful if the data controller had a 'legitimate interest' but this interest would be balanced against the privacy and data protection rights of the data subject.

Disclosure of personal data

- It is an offence to disclose personal data in any manner that is incompatible with the purpose for which such data has been collected.

- Personal data must not be disclosed unless condition(s) under section 28 apply:



Questions raised by police

1. Nowadays, many people are installing CCTV Cameras on their private premises for security purpose. These cameras at times also capture images of the movements of their neighbours. Very often the services of the Police are solicited to attend such requests. What is the correct course of actions?

- Inform concerned individual that cameras must cover his/her premises only and signage must be placed to notify people of camera surveillance
- Conduct a site visit to check position and coverage of cameras.
- Request the latter to adjust positions of cameras if capturing images outside his/her premises.

Questions raised by police

2. The Police have been issued with multi-media radios for better communication. These radios may be used for taking snaps and video recording. What are precautions that should be taken in order to avoid any breach of the Data Protection Act?

- Processing must be done in according with the DPA. There must be lawful grounds for processing personal data. (if any condition under sections 28 or 44 apply)
- The captured images/recordings must not be used for any purpose other than that stated.
- Security measures must be implemented to ensure confidentiality of personal data (section 31).The captured images/recordings must not be accessed by or disclosed to unauthorised people.

3. In the near future Police Officers will be equipped with body-worn cameras. Would they be allowed to use the images or voice recording captured by such body worn cameras to defend themselves in Court in case they are subject to unfounded or baseless allegations for corruption or malpractices?

- More intrusive than the more 'normal' CCTV style surveillance systems because of its mobility.
- It is important to justify its use and consider whether or not it is proportionate, necessary and addresses a pressing social need.
- Collection of both audio and video needs to be justifiable.
- Best approach is to purchase a system where video and audio recording can be controlled and turned on and off independently of each other.

- It is highly recommended to undertake a privacy impact assessment (PIA) before deciding to procure and deploy such a system.
- When using a BWV device, it is important to know when and when not to record.
- Continuous recording is not recommended without strong justification, as this can be highly intrusive and is likely to capture footage of everyday people going about their daily business, as well as the individual who is the focus of your attention.
- It is important that clear signage is displayed, e.g. on an individual's uniform, to show that recording is taking place and whether the recording includes audio.
- It is important to routinely monitor the use of BWV to ensure that it is still achieving its original purpose and if no more the case, to consider using less privacy-intrusive methods to address this need.

- In some countries, police officers may switch on their BWV camera when they believe an individual is being aggressive or there is potential for aggression. Devices help to reduce crime or the potential for crime by acting as a deterrent. In a case of actual bodily harm, recorded footage may be used as evidence in a court of law.
- However, in Mauritius advice must be sought from SLO regarding whether such evidence would be admissible in court.

Questions raised by police

4. Some Police Officers uses their personal mobile phones to take photographs at scene of crimes including dead body, exhibits and other physical evidence and use such photographs during investigation. Is such practice in order?

- Police must implement a policy regarding the use of mobile phones for police purposes.
- Ideally, police officers must not routinely use their personal mobile phone to capture an image or make a recording of an incident or crime scene.

Questions raised by police

5. Can the Police make use of photos on the social media for intelligence work or profiling?

- Publicly available information on social media may be used for intelligence work.
- However, accuracy of such information must be verified.
- Also, the information must not be used for any purpose other than that stated.

Thanks!

Any questions?

Contact us:

Website : http://dataprotection.govmu.org

Email: dpo@govmu.org

Tel: 4600251