

Data



Collection, Types, Accuracy,
Processing, Use & Security

By Mrs Pravina Dodah
Data Protection Officer/Senior Data Protection Officer

What is data?

- Information in raw or unorganised form such as:

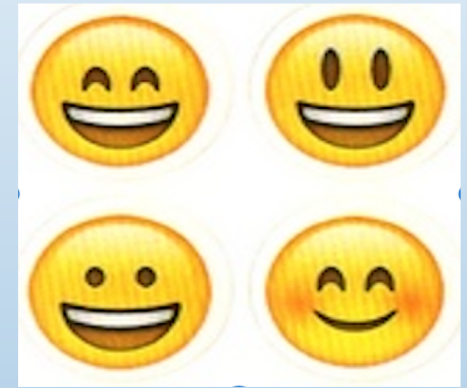
Alphabets



Numbers



Symbols



that represent conditions, ideas, or objects.

- Data is limitless and present everywhere.

What is personal data?

- ▷ **Personal data is any information relating to an identified or identifiable individual by reference to identifiers.**



- ▷ **Identification thus requires elements which describe a person in such a way that he/she is distinguishable from all other persons and recognisable as an individual (singling out).**

Example:

80 people are participating in a training at the Local Government Services Commission.



Can you identify someone?

<Name of participant> is participating in a training at the Local Government Services Commission.



Can you now identify someone?

Data



80 people

Identifier



Name

Personal
Data



Actual
<Name of
participant>

Examples of identifiers are:



Name of a person

National Identity Card no.

Social security no.

Bank account no.

Even one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual.

**What is special categories
of personal data?**

➤ Personal data of an individual pertaining to

- 1) his racial or ethnic origin;
- 2) his political opinion or adherence;
- 3) his religious or philosophical beliefs;
- 4) his membership of a trade union;
- 5) his physical or mental health or condition;
- 6) his sexual orientation, practices or preferences;
- 7) his genetic data or biometric data uniquely identifying him;
- 8) the commission or alleged commission of an offence by him;
- 9) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings.



Processing and use of personal data

➤ **Processing of personal data must be made in accordance with the Data Protection Act 2017.**

➤ **Imposes a number of obligations on controllers and processors.**

A **controller** can be an organisation/department/professional, amongst others, who processes personal data and has decision making power over the processing.

A **processor** processes personal data on behalf of a controller.

➤ **Provides enhanced rights to individuals.**



Obligations on controllers and processors

Registration and renewal as controller and/or processor (s14)	<ol style="list-style-type: none">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)	<ol style="list-style-type: none">1. Lawful, fair and transparent2. Purpose limitation3. Data minimisation4. Data accuracy5. Storage limitation6. In accordance with the rights of data subjects.
Duties of controller (s 22)	<ol style="list-style-type: none">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)	<ol style="list-style-type: none">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

<p>Notification of personal data breach (s 25)</p>	<p>1. To notify the Data Protection Office where feasible not later than 72 hours after becoming aware. 2. Form available on DPO website.</p>
<p>Communication of breach to data subject (s 26)</p>	<p>Where it is likely to result in a high risk to the rights and freedoms of the data subject.</p>
<p>Duty to destroy personal data (s 27)</p>	<p>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.</p>
<p>Lawful processing (s 28)</p>	<p>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 not override the rights and freedoms of data subjects (9) historical/statistical or scientific research.</p>
<p>Special Categories of personal data (s 29)</p>	<p>Must implement specific protection and a stricter regime.</p>
<p>Personal data of child (s 30)</p>	<p>Parental or guardian consent must be obtained for processing the personal data of children under the age of 16.</p>

Obligations on controllers and processors

<p>Security of processing (s 31)</p>	<p>Implement appropriate security and organisational measures.</p>
<p>Record of processing operations (s 33)</p>	<p>Template available on DPO website.</p>
<p>Processing operations likely to present risk to individuals (s 34&35)</p>	<ol style="list-style-type: none"> 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.
<p>Transfer of personal data outside Mauritius (s 36)</p>	<p>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.</p>

Collection of personal data

- **Controllers and processors often collect personal information (e.g. through application forms and/or websites).**
- **Must abide with section 23 of the Data Protection Act 2017.**




▷ **Collect personal data for a lawful purpose.**

▷ **Details to be provided to individuals:**

- **The organisation's contact details and where applicable its representative and any Data Protection Officer;**
- **Purpose(s) for which you are collecting the data;**
- **To whom you intend to disclose the data;**
- **Whether the collection is voluntary or mandatory;**
- **Right to withdraw consent at any time;**
- **Rights of individuals: Access, Rectification, Erasure, Object to processing;**
- **Existence of automated decision making, and the consequences of such processing;**
- **Period for storing the data;**
- **Right to lodge a complaint with the Commissioner;**
- **To which countries you intend to transfer the data.**

Lawful Processing

Criteria for lawful processing




There are 9 criteria for processing personal data lawfully under the Data Protection Act 2017.

You must meet at least one of them to satisfy your requirements for lawful processing.

1st Criteria for lawful processing



Consent of the data subject.



Example: A company which processes job application forms submitted by candidates for recruitment.

2nd Criteria for lawful processing

A contractual relationship requires the processing of personal data.

You made an online purchase.

The controller processes your name and address in order to deliver the goods.

This is necessary in order to perform the contract.

You will enter into a life insurance contract.

The controller requires some medical test of you before entering into the contract.

This is necessary prior to entering into the life insurance contract.

3rd Criteria for lawful processing

The processing is necessary for compliance with a legal obligation of the controller.

Example: An employer needs to disclose employee emolument details to Mauritius Revenue Authority (MRA).


Example: A court order may require you to process personal data for a particular purpose and this qualifies as a legal obligation.

4th Criteria for lawful processing

To protect the vital interests of the data subject or another person



An individual is admitted to the ICU department of a hospital and that person is unable to communicate to doctors. The disclosure of the individual's medical history to the hospital is necessary in order to protect his/her vital interests.



Note : This criterion may be invoked where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person.

5th Criteria for lawful processing

Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Example: The Financial Services Commission (FSC) processes personal data for the administration of financial services in Mauritius.

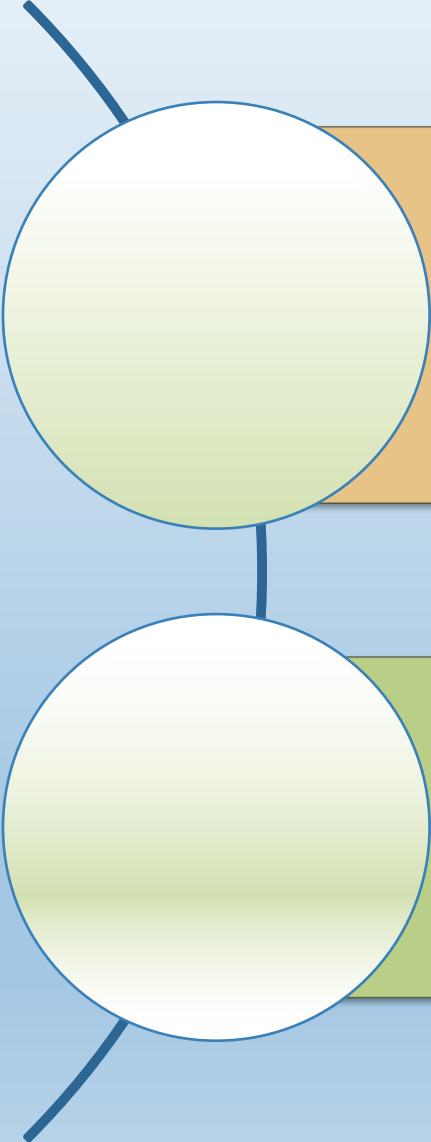
6th Criteria for lawful processing



Performance of any task carried out by a public authority.

Example: The Central Water Authority processes personal data for the distribution of water to households.

7th Criteria for lawful processing



For the exercise, by any person in the public interest, of any other functions of a public nature.

Example: A court hearing or judgment where the names of individuals are cited.

8th Criteria for lawful processing

The processing of personal data is necessary for the legitimate interests of the controller or a third party to whom the data are disclosed.

This requires a 3 parts test to be carried out by the controller:

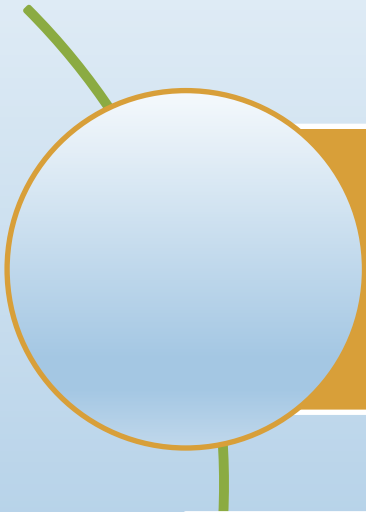
Purpose test: Are you pursuing a legitimate interest?

Necessity test: Is the processing necessary for that purpose?

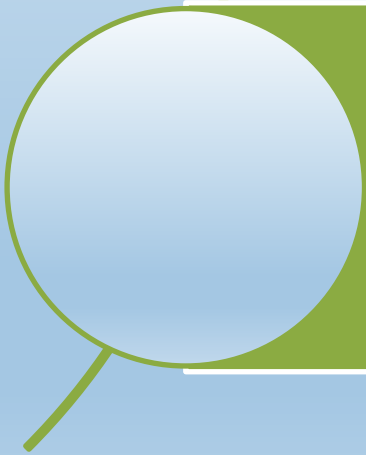
Balancing test: Do the individual's interests override the legitimate interests of the controller?

Example: The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the controller.

9th Criteria for lawful processing



The processing is necessary for historical, statistical or scientific research.

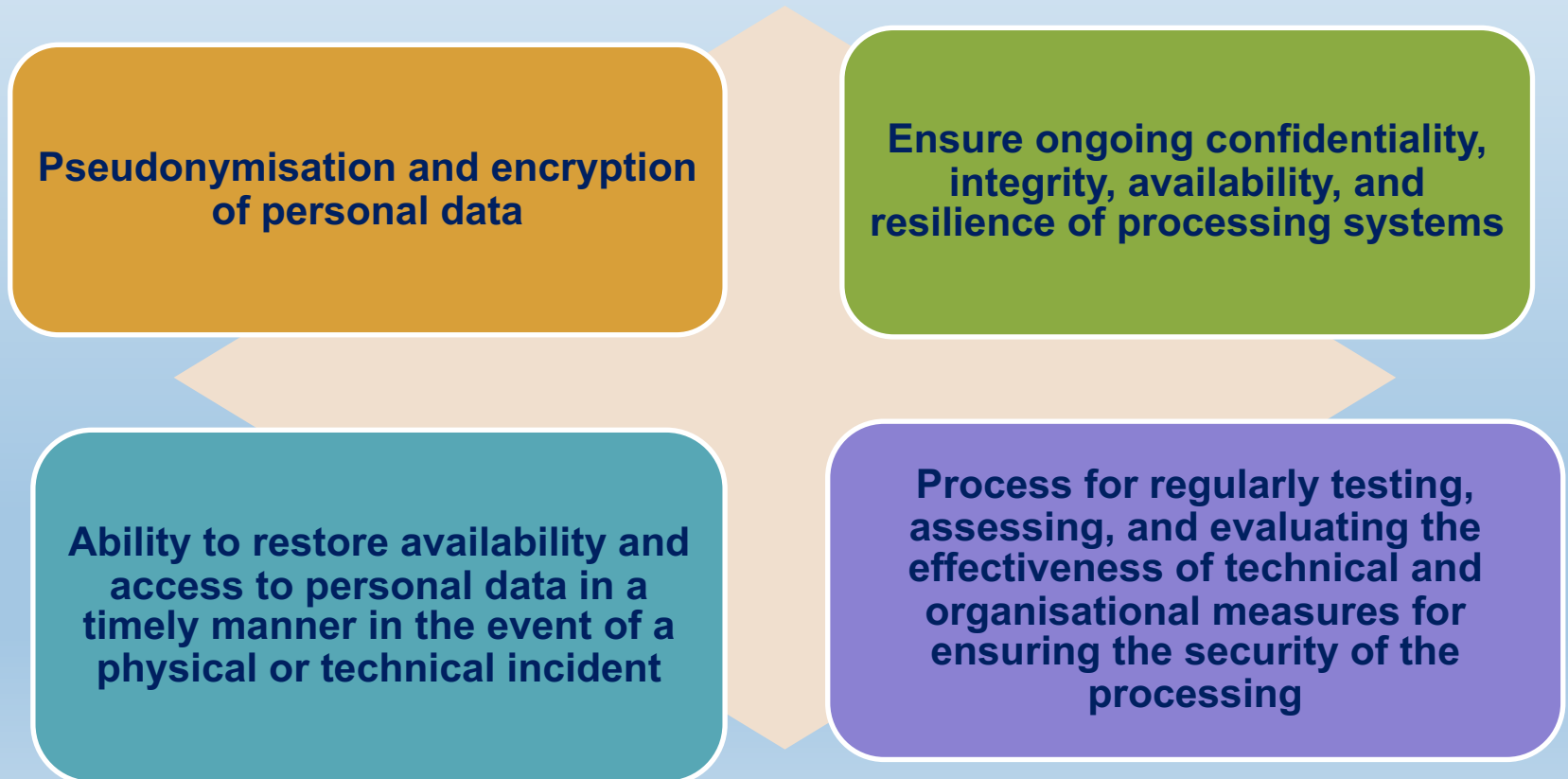


The Ministry of Health is using historical health data for forecasting of health services to be provided by public authorities.

Security of processing

Appropriate technical and organisational measures

- ▷ must be implemented to prevent unauthorised access to, alteration, disclosure, accidental loss and destruction of personal data. Such measures include:



Pseudonymisation

- ▷ Pseudonymisation is a process by which personal data cannot be attributed to an individual without additional information.
- ▷ The ‘key’/additional information that enables re-identification of the data subjects must be kept separate and secure.

Example:

“**Charles Spencer** is the father of a family of four children.”



can be pseudonymised as

“**324** is the father of a family of four children.”

Measures

- ❑ will vary from organisation to organisation but you have to take the following into consideration:



the state of technological development available

the cost of implementing any of the measures

the special risks that exist in the processing of the data and

the nature of the data being processed

Example:

A bank will have greater security measures such as ISO 27001 standards as compared to a pre primary school.

Using the services of a processor

If the controller is using the services of a processor, the controller is still responsible under the DPA for data protection and so must ensure through a written contract that the processor

acts only on instructions received from the controller and

implements appropriate security measures for protecting any personal data processed.

Employees of controller or processor

A controller must also ensure that employees have received appropriate security training and that they are taking all reasonable steps to comply with the relevant security measures.

Thank you

Data Protection Office
5th Floor, Sicom Tower,
Wall Street, Ebene
Email: dpo@govmu.org
Tel: 4600251