

Managing Digital Information

**Issues regarding sharing of digital information
(Email, network etc)**

**Unlawful disclosure/consequence/disclosure
required by law**

**By Reza Mukoon
Data Protection Officer/Senior Data Protection Officer**

Applicability of the act



Section 1

- For the purposes of this Act, each Ministry or Government department will be treated as separate from any other Ministry or Government department.

Manual or Electronic Personal Data

- This Act applies to the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data forms part of a filing system or is intended to form part of a filing system..

Application of the Act (2)

The Act applies to a controller / processor who:



is established in Mauritius and processes personal data in the context of that establishment; and



is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.

Non - Application of the Act

The Act does not apply to:



the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis;



the processing of personal data by an individual in the course of a purely personal or household activity.

Special categories of Personal Data

Sections 29 of DPA

Special Categories of Personal Data

Personal data of data subject pertaining to:

- his racial or ethnic origin
- his political opinion or adherence
- his religious or philosophical beliefs
- his membership of a trade union
- his physical or mental health or condition
- his sexual orientation, practices or preferences
- his genetic data or biometric data uniquely identifying him
- the commission or alleged commission of an offence by him
- 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 or
- such other personal data as the Commissioner may determine to be sensitive personal data

Processing of special categories of personal data

- ▷ When processing special categories of personal data, controllers must still have a **lawful basis** for the processing under section 28, in exactly the same way as for any other personal data.
- ▷ The difference is that the controller will also need to satisfy a specific condition under section 29 of the Act. See section 29 for more information.
- ▷ Special categories of personal data are more sensitive, and so they need more protection.
- ▷ In particular, these types of data could cause more risk to a person's fundamental rights and freedoms. For example, unlawful discrimination.

Processing of special categories of personal data

▷ Special categories of personal data shall not be processed unless –

- section 28 applies to the processing; and
- The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes **OR**
- The processing relates to personal data which are manifestly made public by the data subject **OR**
- The processing is necessary for
 1. the establishment, exercise or defence of a legal claim;
 2. for a contract with a health professional subject to the obligation of professional secrecy (see S29 1 -d (ii) & S29 -2)
 3. the purpose of carrying out the obligations and exercising specific rights of the controller or the data subject
 4. protecting the vital interests of the data subjects or another person where the data subject is physically or legally incapable of giving consent.

Examples of special categories of personal data

- ▷ A trade union processes the personal data of its members in the context of its activities with appropriate security safeguards in place.
- ▷ A private Medical Specialist keeps medical records of his patients securely on his medical application computer for delivering health services to his patient.

Emails

▷ To;CC;BCC

▷ Risk of Data breach

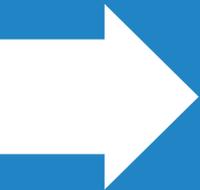
▷ Care must be taken using email

▷ Phishing

▷ Business Email Compromise

▷ Eg johnsmith@neworg.com

johnsmith@new_org.com

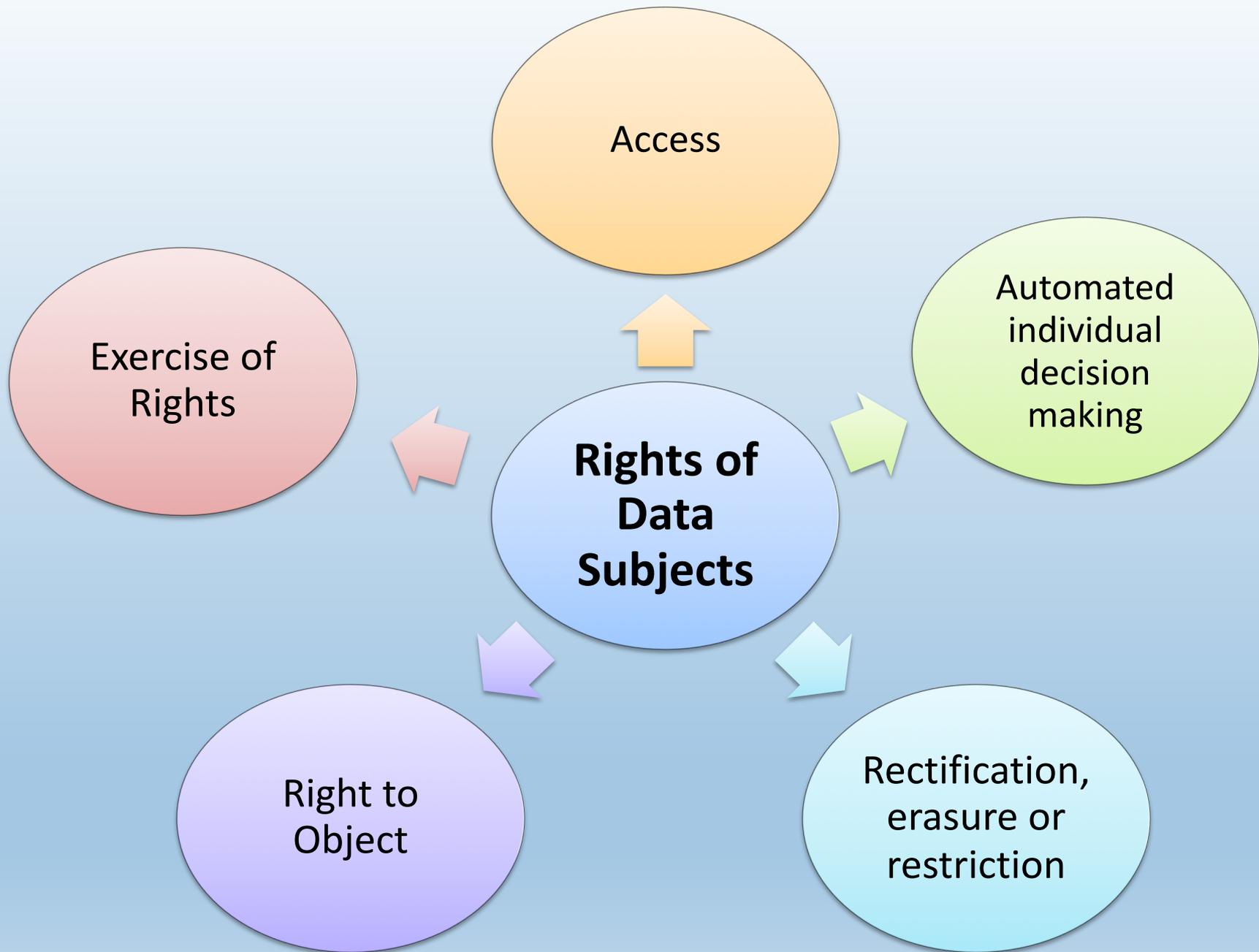


Rights of Data Subjects

Part VII

Rights of Data Subjects

- ▷ Part VII of the Act stipulates the rights of data subjects.
- ▷ The Act has enhanced the rights to access, rectify, erase and restrict the processing of personal data.
- ▷ New provisions have been made to cater for decisions which are based on automated processing and the right to object to the processing of personal data by individuals.



Right of access (Section 37)



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.

Right of access (Section 37)

▷ How to make a request of access?

- ❖ You should write to the controller or fill in the **new Rights of Data Subject Form** which is available on this office website.

▷ Can a controller charge a fee for dealing with a subject access request?

- ❖ The controller must provide a copy of the information **free of charge**.
- ❖ However, where the request is **manifestly excessive**, you may charge a fee for providing the information or taking the action requested, or you may not take the action requested.

Right of access (Section 37)

▷ **Case Study:**

Mrs B had concerns about her daughter Rosie's school performance and so made a request, on Rosie's behalf, for her education records. Rosie was aged eight and in grade three at primary school. The school asked for a fee of Rs 1000, which Mrs B paid. The school provided the records which consisted of 2 pages, 60 days later.

Right of access (Section 37)

▷ **This case is about:**

- access to education records; and
- timescales and fees for subject access requests.

▷ **What should be noted in this case?**

- As per section 37 (5), the school should have provided a reply within one month from the date of request but instead took 60 days.
- The information should have been given free of charge since the information is manifestly not excessive (only 2 pages provided)

Automated individual decision making (Section 38)

▷ When should a controller carry out an Automated individual decision making?

When:

- ❖ It is necessary for the entry into or performance of a contract; or
- ❖ It is authorised by law applicable to the controller; or
- ❖ It is based on the individual's explicit consent.
- ❖ Automated processing cannot be applied to special categories of personal data as specified in section 2 of the DPA.

Automated individual decision making (Section 38) - To DO

- ▷ If a controller is making automated decisions as described in Section 38 (1), it must:

Identify and record its lawful basis for the processing.

Inform the data subject that it is engaging in this type of activity and explain the significance/envisaged consequences of the processing.

Have processes in place for people to exercise their rights. Bring details of data subjects rights to their attention.

Secure personal data in a way that is in the interests and rights of the individual and that prevents discriminatory effects.

Rectification, erasure or restriction of processing (Section 39)

▷ **Data Subjects have the right to:**



Obtain from controller rectification of inaccurate or incomplete personal data concerning him/her without undue delay.



Request that his/her personal data are erased without undue delay if the continued processing of those data is not justified.



Request that the processing of his/her personal data is restricted where the accuracy of the data is contested or where he requires it for legal claim amongst others.



▷ **See the exceptions provided under section 39 (3) and (4) of the DPA.**

Rectification, erasure or restriction of processing (Section 39)

Example : Case for non-rectification

A medical record of an operation must not be changed, in other words 'updated', even if findings mentioned in the record later on turn out to have been wrong. In such circumstances, only additions to the remarks in the record may be made, as long as they are clearly marked as contributions made at a later stage.

Right to Object - Section 40

▷ What you need to know on right to object?

Data Subjects

- Data subjects have the right to object in writing, on grounds relating to their particular situation, to the processing of personal data.

Controllers

- Controllers must cease such processing unless they demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or requires the data in order to establish, exercise or defend legal claims.

Right to Object - Section 40

- ▷ **Example:** A controller has received an objection from a data subject regarding the use of his personal data for direct marketing. What should the company do?

Stop processing personal data for direct marketing purposes as soon as the controller receives an objection.

Deal with the objection to processing for direct marketing at any time and free of charge. If necessary, review the procedures of the organisation.

Inform individuals of their right to object “at the point of first communication” and in the organisation’s privacy notice.

Exercise of Rights (Section 41)

- ▷ Where a person is a minor or physically or mentally unfit, a person duly authorised (parents, guardian, legal administrator) can exercise their rights on their behalf under this part.

Unlawful disclosure of personal data

Section 42

Unlawful disclosure of personal data

Controller

Any controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected shall commit an offence.

Processor

Any processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the controller on whose behalf the data are being or have been processed shall commit an offence.

Unlawful disclosure of personal data

Case scenario - Disclosure

- In *Y v. Turkey*, the applicant was HIV positive.
- As he was unconscious during his arrival at the hospital, the ambulance crew informed the hospital staff that he was HIV positive.
- The applicant argued before the ECtHR that the disclosure of this information had violated his right to respect for private life.
- However, given the need to protect the safety of the hospital staff, sharing the information was not regarded as a breach of his rights.
- *Note: The European Court of Human Rights (ECtHR), Y v. Turkey, No. 648/10, 17 February 2015*

Offences and Penalties

Section 42

Offences and penalties

- ▷ 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.

Offences and penalties

Offences	Penalties
<p>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.</p>	<p> LIABLE to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.</p>
<p>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.</p>	<p> LIABLE to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.</p>
<p>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.</p>	<p> LIABLE to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.</p>
<p>Section 17: Change in particulars Any controller or processor who fails to notify a change in particulars.</p>	<p> LIABLE to a fine not exceeding 50, 000 rupees.</p>
<p>Section 28: Lawful processing Any person who process personal data unlawfully.</p>	<p> LIABLE to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.</p>

Investigation of complaints

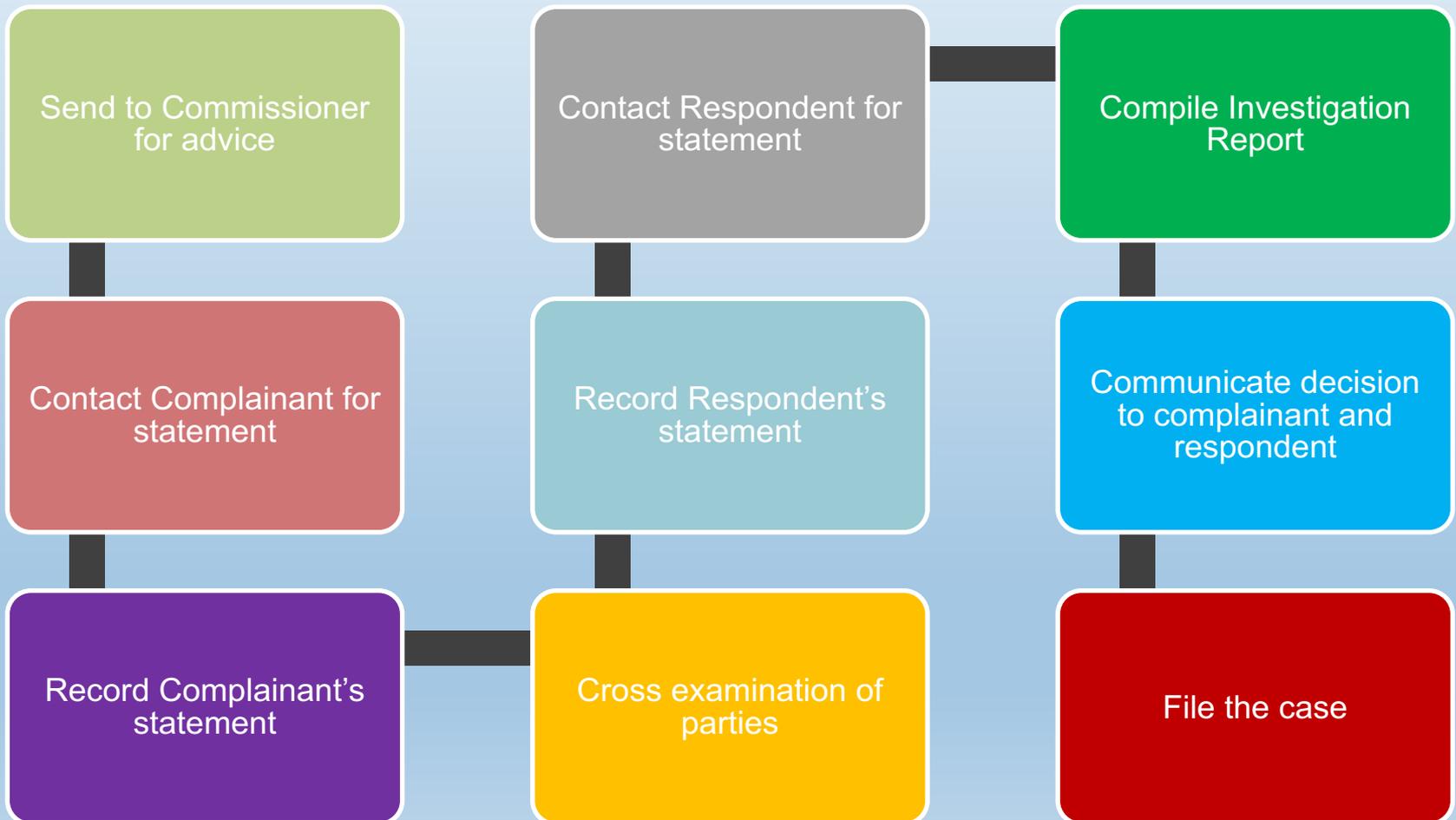
Section 6

Investigation of complaints

- ▷ The Commissioner is empowered to investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under the DPA or cause it to be investigated by an authorised officer, unless he is of the opinion that the complaint is frivolous or vexatious.
- ▷ Investigation of complaints has always been part of our previous functions but is now enhanced with the amicable resolution of disputes wherever possible.

Investigation of complaints

How is the investigation carried out?



Investigation of complaints

How long does the investigation take?

- ▷ Depending on the complexity of the cases, it may take 3 months to one year or more.
- ▷ It also depends on collaboration of all parties and availability/gathering of evidences.

Investigation of complaints

What can be the outcome of the investigation?

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

Is the Decision of the Commissioner appealable?

- ▷ Any person who feels aggrieved by the Commissioner'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.

Offences



For providing any false or misleading information in the particulars of information

A fine not exceeding 100,000 rupees

Imprisonment for a term not exceeding 5 years

Offences



**Failure to notify about
change in particulars**

**A fine not exceeding
50,000 rupees**

Questions