THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- "This presentation will offer to you a simplified understanding of the intricacies of the Data Protection Act and how the implementation of this legislation will affect your daily life."
- Presented by Mrs Drudeisha Caullychurn-Madhub , Data Protection Commissioner, Prime Minister's Office.
- pmo-dpo@mail.gov.mu
- 201-36-04
- 6th floor, New Government Centre

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

Data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues surrounding them.

Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as:

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

Healthcare records
Criminal justice investigations and proceedings
Financial institutions and transactions
Biological traits, such as genetic material
Residence and geographic records
Ethnicity
The challenge in data privacy is to share data while protecting personally identifiable information.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **Defining Privacy**
- Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information.
- Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. The lack of a single definition should not imply that the issue lacks importance. As one writer observed, "in one sense, all human rights are aspects of the right to privacy."

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **Aspects of Privacy**
- Privacy can be divided into the following separate but related concepts:
- **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
- **Privacy of communications**, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **Legality**
- The legal protection of the right to privacy in general - and of data privacy in particular - varies greatly around the world.
- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
- —*Universal Declaration of Human Rights, Article 12 , article 17 of the ICCPR and article 22 of the Code Civil Mauricien.*

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **Europe**
- The right to data privacy is heavily regulated and rigidly enforced in Europe. Article 8 of the European Convention on Human Rights (ECHR) provides a right to respect for one's *"private and family life, his home and his correspondence"*, subject to certain restrictions.
- The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence. According to the Court's case law the collection of information by officials of the state about an individual without his consent always falls within the scope of Article 8.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Thus, gathering information for the official census, recording fingerprints and photographs in a police register, collecting medical data or details of personal expenditures and implementing a system of personal identification have been judged to raise data privacy issues. Any state interference with a person's privacy is only acceptable for the Court if three conditions are fulfilled:
- The interference is in accordance with the law
- The interference pursues a legitimate goal
- The interference is necessary in a democratic society

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The government is not the only entity which may pose a threat to data privacy. Other citizens, and private companies most importantly, engage in far more threatening activities, especially since the automated processing of data became widespread;
- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was firstly concluded within the Council of Europe in 1981. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **The European Union Data Protection Directives**
- In 1995, the European Union enacted the Data Protection Directive in order to harmonize member states' laws in providing consistent levels of protections for citizens and ensuring the free flow of personal data within the European Union.
- The directive sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. It applies to the processing of personal information in electronic and manual files.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- A key concept in the European data protection model is "enforceability." Data subjects have rights established in explicit rules.
- Every European Union country has a data protection commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will need to provide a similar level of oversight.
- This explains why Mauritius has also opted for the creation of a data protection commission and why our legislation needs to be compliant with the norms established by the EU.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The basic principles established by the Directive are:
- the right to know where the data originated; the right to have inaccurate data rectified;
- a right of recourse in the event of unlawful processing; and the right to withhold permission to use data in some circumstances. For example, individuals have the right to opt-out free of charge from being sent direct marketing material.
- The Directive contains strengthened protections over the use of sensitive personal data relating, for example, to health, sex life or religious or philosophical beliefs.
-

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The commercial and government use of such information will generally require "explicit and unambiguous" consent of the data subject.
- The EU Directive on Data Protection contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable principles of good practice, i.e, the data must be:
- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to countries without adequate protection.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- These principles are also echoed in our legislation in the First Schedule since they represent the international norms on data protection and privacy.
- Definition of Personal Data:-
- Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', 'holding' and 'disclosing'.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The definition of personal data in the Data Protection Act reads as follows:
- "personal data" means data which relates to (a living) individual who can be identified from those data or the data or other information, including an opinion forming part of a database, whether or not recorded in material form, about an individual whose identity is apparent or can be reasonably ascertained from the data, information or opinion."

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

A similar definition is contained in the EU Data Protection Directive (95/46/EC):

"personal data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

- The definition is – deliberately - a very broad one. In principle, it covers any information that relates to an identifiable, living individual.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- There are different ways in which an individual can be considered 'identifiable'. A person's full name is an obvious likely identifier. But a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms occupation, address etc.
- The definition is also technology neutral. It does not matter how the personal data is stored - on paper, on an IT system, on a CCTV system etc.
- More extensive guidance on this topic is contained in Opinion 4/2007 of the EU Article 29 Working Party

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **DATA PROCESSING**
- **Data processing** is any computer process that converts data into information or knowledge. The processing is usually assumed to be automated and running on a computer.
- Because data are most useful when well-presented and actually *informative*, data-processing systems are often referred to as information systems to emphasize their practicality. Nevertheless, both terms are roughly synonymous, performing similar conversions; data-processing systems typically manipulate raw data into information, and likewise information systems typically take raw data as input to produce information as output.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- What is data protection?
- When you give your personal details to an organisation or individual, they have a duty to keep these details private and safe. This process is known as data protection. We refer to organisations or individuals who control the contents and use of your personal details as ‘data controllers’.
- Most of us give information about ourselves to groups such as government bodies, banks, insurance companies, medical professionals and telephone companies to use their services or meet certain conditions. Organisations or individuals can also get information about us from other sources. Under data protection law, you have rights regarding the use of these personal details and data controllers have certain responsibilities in how they handle this information.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- When do these rights apply?
- You have the right to data protection when your details are:
  - held on a computer;
  - held on paper or other manual forming part of a structured filing system; and
  - made up of photographs or video recordings of your image or recordings of your voice.
- What is the aim of these rights?
- Data protection rights will help you to make sure that the information stored about you is:
  - factually correct;
  - only available to those who should have it; and
  - only used for stated purposes.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- When should I contact the Data Protection Commissioner?
- If you are not happy with how your details are being used, you should contact the organisation in question. If you believe that the organisation or individual is still not respecting your data protection rights, you should contact the Office of the Data Protection Commissioner to ask for help.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 1. Right to have your details used in line with data protection regulations
- A data controller who holds information about you must:
  - get and use the information fairly;
  - keep it for only one or more clearly stated and lawful purposes;
  - use and make known this information only in ways that are in keeping with these purposes;
  - keep the information safe;
  - make sure that the information is factually correct, complete and up-to-date;
  - make sure that there is enough information – but not too much - and that it is relevant;
  - keep the information for no longer than is needed for the reason stated; and
  - give you a copy of your personal information when you ask for it.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 2. Right to information about your personal details
- Data controllers who obtain your personal information must give you:
  - the name of the organisation or person collecting the information or for whom they are collecting the information;
  - the reason why they want your details; and
  - any other information that you may need to make sure that they are handling your details fairly – for example the details of other organisations or people to whom they may give your personal details.
- If an organisation or individual gets your personal details from someone else and not directly from you, they must tell you which details they hold and give you the name of the original data controller.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 3. Right to access your personal details
- You can ask for a copy of all your personal details by filling in the request for access to personal data form to be sent to any organisation or person holding these details on a computer or in manual form.
- You can also ask the data controller to inform you of any opinions given about you, unless the data controller considers that the opinions are confidential. Even in such cases, your right to such information will usually be greater than the right of the person who gave this opinion in private. This right does not apply, however, in a small number of cases where it could harm certain interests – for example when someone is investigating an offence.
- You should also be informed of, and given the chance to object to, any decisions about you that are automatically generated by a computer without any human involvement.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 4. Right to know if your personal details are being held
- If you think that an organisation or individual may be holding some of your personal details, you can ask them to confirm this within 28 days. If they do have personal details about you, they must tell you which details they hold and the reason why they are holding this information.
- 5. Right to change or remove your details
- If you discover that a data controller has details about you that are not factually correct, you can ask them to change or, in some cases, remove these details.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Similarly, if you feel that the organisation or person does not have a valid reason for holding your personal details or that they have taken these details in an unfair way, you can ask them to change or remove these details.
- In both cases, you can fill in the form to be sent to the organisation or person, explaining your concerns or outlining which details are incorrect. Within 28 days, the organisation must do as you ask or explain why they will not do so.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 6. Right to prevent use of your personal details
- You can also ask a data controller not to use your personal details for purposes other than their main purpose – for example for marketing. You can do this by simply writing to the organisation or person holding your details and outlining your views. Within 28 days, they must do as you ask or explain why they will not do so.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- How do I request access to my details?
- You must fill in the request for access to personal data form which will be shortly available on the website of the office, www.dataprotection.gov.mu and on the government portal in the section "download forms" as well as in GN 22/09, i.e the Data Protection Regulations 09 which have come into force on the 16th of February 09.
- You must then send this form to the data controller who must comply with it within 28 days, subject to certain exceptions provided in the law.`

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 7. Right to remove your details from a direct marketing list
- If a data controller holds personal details about you for direct marketing purposes, you can ask them to remove your details. You can do this by writing to the organisation or person holding these details. They must let you know within 28 days if they have dealt with your request.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 8. Right to object
- A data controller may intend to use your details for official purposes, in the public interest or for their own interests. If you feel that doing so could cause you unnecessary damage or distress, you may ask the data controller not to use your personal details. This right does not apply if:
  - you have already agreed that the data controller can use your details;
  - a data controller needs your details under the terms of a contract to which you have agreed;
  - election candidates or political parties need your details for electoral purposes; or
  - a data controller needs your details for legal reasons.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- You can also object to use of your personal details for direct marketing purposes if these details are taken from the electoral register or from information made public by law, such as a shareholders' register. There is no charge for objecting.
- 9. Right to freedom from automated decision making
- Generally, important decisions about you based on your personal details should have a human input and must not be automatically generated by a computer, unless you agree to this. For example, such decisions may be about your work performance, creditworthiness or reliability.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 10. Right to refuse direct marketing calls or mail
- If you do not want to receive direct marketing telephone calls, you should contact your service provider. They will make a note of your request in the National Directory Database ('opt-out' register). If you have not included your phone number in this register, you can also refuse such calls by simply asking the caller not to phone you again. An organisation must get your permission before they contact you by fax machine or automated dialling for direct marketing purposes.
- An organisation must also get your permission before they send marketing emails to your computer or before they send marketing text messages to your mobile phone.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- *Are you a data controller?*
- If you, as an individual or an organisation, collect, store or process any data about living people on any type of computer or in a structured filing system, then you are a data controller. In practice, to establish whether or not you are a data controller, you should ask, do you decide what information is to be collected, stored, to what use it is put and when it should be deleted or altered.
- Because of the serious legal responsibilities attached to a data controller under the Act, you should seek the advice of the Commissioner if you have any doubts as to whether or not you are a data controller in any particular case.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- *What are your responsibilities as a data controller?*
- You have certain key responsibilities in relation to the information which you process. These may be summarised in terms of the eight fundamental rules which you must follow. These rules which are detailed in this guide apply to all data controllers. Certain categories of data controllers are also obliged to register with the Data Protection Commissioner. This is a separate legal requirement and in no way obviates the need to comply with the requirements of the Acts having so registered.
- There are some specific requirements on which more details can be found on our website, in various annual reports of the Data Protection Commissioner or by contacting this Office directly.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- These include:
- the obligatory requirement on certain categories of data controllers to register with the Data Protection Commissioner. Guidance notes of Registration for Data Controllers will also be made available shortly from this Office. If you are required to register and are not it is illegal to process personal data.
- the specific requirements for marketing by phone, e-mail, fax or other electronic means, including text message, are also covered.
- the processing of publicly available information for other purposes including direct marketing are also covered.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- *How do you as a data controller ensure compliance with the law?*
- You must make yourself aware of your data protection responsibilities, in particular, to process personal data fairly. You should ensure that your staff are made aware of their responsibilities through appropriate induction training with refresher training as necessary and the availability of an internal data protection policy that is relevant to the personal data held by you. An internal policy which reflects the eight fundamental data protection rules and applies them to your organisation, which is enforced through supervision and regular review and audit, is a valuable compliance tool.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- *How is the Act enforced?*
- The Commissioner's role is to ensure that those who keep personal data comply with the provisions of the Act. She has a wide range of enforcement powers to assist her in ensuring that the principles of data protection are being observed. These powers include the serving of legal notices compelling data controllers to provide information needed to assist his enquiries, and compelling a data controller to implement one or more provisions of the Act in a particular prescribed manner.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- She may investigate complaints made by the general public or carry out investigations proactively. She may, for example, authorise officers to inspect the type of personal information kept, how it is processed and the security measures in place in compliance with the power to carry out security checks and compliance audits. You and your staff are required to co-operate fully with such officers.
- A data controller found guilty of an offence under the Act is liable to imprisonment.
- The Commissioner also publishes an annual report which names, in certain cases, those data controllers that were the subject of investigation or action by his Office.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The Eight Rules of Data Protection
- **You must...**
- 1. Obtain and process information fairly
- 2. Keep it only for one or more specified, explicit and lawful purposes
- 3. Use and disclose it only in ways compatible with these purposes
- 4. Keep it safe and secure
- 5. Keep it accurate, complete and up-to-date
- 6. Ensure that it is adequate, relevant and not excessive
- 7. Retain it for no longer than is necessary for the purpose or purposes
- 8. Give a copy of his/her personal data to an individual, on request

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 1. Obtain and process information fairly
- To fairly obtain data the data subject must, at the time the personal data is being collected, be made aware of:
- the name and address of the data controller;
- the fact that the data is being collected;
- the purpose in collecting the data;
- the identity of any representative nominated for the purposes of the Act;
- the persons or categories of persons to whom the data may be disclosed;

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- whether replies to questions asked are voluntary or obligatory and the consequences of not providing replies to those questions;
- The consequences for the data subject if all or part of the requested data is not provided;
- the right to rectify their data if inaccurate or processed unfairly;
- In addition, where the personal data is not obtained from the data subject, either at the time their data is first processed or at the time of disclosure to a third party, all the above information must be provided to the data subject and they must also be informed of the identity of the original data controller from whom the information was obtained and the categories of data concerned.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- To fairly process personal data it must have been fairly obtained, and the data subject must have given consent to the processing; or
- the processing must be necessary for one of the following reasons -
- the performance of a contract to which the data subject is a party;
- in order to take steps at the request of the data subject prior to entering into a contract;
- to protect the vital interests of the data;
- for the administration of justice;
- In the public interest.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 2. Keep it only for one or more specified, explicit and lawful purposes
- You may only keep data for a purpose(s) that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with that purpose(s). An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose.
- To comply with this rule:
- In general a person should know the reason/s why you are collecting and retaining their data.
- The purpose for which the data is being collected should be a lawful one
- You should be aware of the different sets of data which you keep and specific purpose of each.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 3. Use and disclose it only in ways compatible with these purposes
- Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.
- A key test of compatibility is:
- do you use the data only in ways consistent with the purpose(s) for which they are kept?
- do you disclose the data only in ways consistent with that purpose(s)?

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The rule, that disclosures of information must always be compatible with the purpose(s) for which that information is kept, is lifted in certain restricted cases by Section 52 of the Act. Examples of such cases would include some obvious situations where disclosure of the information is required in connection with legal proceedings or for obtaining legal advice or for the purpose of defending legal rights.
- Any processing of personal data by a data processor on your behalf must also be undertaken in compliance with the Act. This requires that, as a minimum, any such processing takes place subject to a contract between the controller and the processor which specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data be deleted or returned upon completion or termination of the contract. The data controller is also required to take reasonable steps to ensure compliance by the data processor with these requirements.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 4. Keep it safe and secure
- Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of the data, and against their accidental loss or destruction. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure.
- High standards of security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.
-

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- A minimum standard of security would include the following:
- access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors;
- access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy;
- access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information;

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- There should be strict controls on the downloading of personal data from an organisation's IT system. Such downloading can easily be blocked by technical means (disabling drives etc)
- A logging and reporting system is an important tool in assisting the network administrator in identifying abuses and developing appropriate responses.
- Encryption
- Encrypting ("scrambling") data can add a further useful layer of security. It can be considered an essential measure where personal data is stored on a portable device. As with passwords, this measure is pointless unless the key to decrypt the data is kept secure.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Anti-Virus Software
- Anti-Virus software is not only required to prevent infection from the internet (either e-mail or web-sourced). Viruses may also be introduced from portable devices, such as memory sticks - a further reason for strictly limiting their use. No anti-virus package will prevent all infections, as they are only updated in response to infections. It is essential that users update such software on a regular basis, but also keep vigilant for potential threats. A policy of not opening e-mail attachments from unexpected sources can be a useful way of preventing infection.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Firewalls
- A firewall is essential where there is any external connectivity, either to other networks or to the internet. It is important that firewalls are properly configured, as they are a key weapon in combating unauthorised access attempts. The importance of firewalls has increased as organisations and individuals increasingly avail of "always-on" internet connections, exposing themselves to a greater possibility of attack.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Automatic screen savers
- Most systems allow for screensavers to activate after a period of inactivity, on the computer. This automatic activation is useful as the alternative manual locking of a workstation requires positive action by the user every time he/she leaves the computer unattended. Regardless of which method an organisation employs, computers should be locked when unattended. This not only applies to computers in public areas, but to all computers. It is pointless having an access control system in place if unattended computers may be accessed by any staff member.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Logs and Audit trails
- It is of course pointless having an access control system and security policy if the system cannot identify any potential abuses. Consequently, a system should be able to identify the user name that accessed a file, as well as the time of the access. A log of alterations made, along with author/editor, should also be created. Not only can this help in the effective administration of the security system, its existence should also act as a deterrent to those staff tempted to abuse the system.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The Human Factor
- No matter what technical or physical controls are placed on a system, the most important security measure is to ensure that staff are aware of their responsibilities. Passwords should not be written down and left in convenient places; passwords should not be shared amongst colleagues; unexpected e-mail attachments should not be opened unless first screened by anti-virus software.
- Certification
- ISO 27001 is an information management standard approved by the International Organisation for Standardisation. If a body is certified to be ISO 27001 compliant, it would demonstrate compliance with the security requirements of the Data Protection Act

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Portable Devices
- Laptops, personal organisers and other form of portable devices are especially vulnerable, as there is not only a higher risk of theft, but also a new risk of accidental loss. It would be a sensible precaution not only to have adequate security measures, but also to limit what data are placed on such machines in the first place.
- Where a data controller considers it essential to store personal data on a portable device, encryption of the device to a standard that makes it impossible to access the data without the encryption key should be the norm. Such personal data should be deleted from the portable device as soon as possible. .

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Back-up systems
- A back up system is an essential means of recovering from the loss or destruction of data. While some system should be in place, the frequency and nature of back up will depend, amongst other factors, on the organisation concerned and the nature of data being processed. The security standards for back-up data are the same as for live data.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Remote Access
- Where a worker is allowed to access the network from a remote location (e.g. From home or from an off-site visit), such access is creating a potential weakness in the system. Therefore, the need for such access should be properly assessed and security measures reassessed before remote access is granted.
- Wireless networks
- Access to a server by means of a wireless connection (such as infrared or radio signals) can expose the network to novel means of attack. The physical environment in which such systems are used may also be a factor in determining any weakness in the system security. As with remote access, wireless networks should be assessed on security grounds rather than solely on apparent ease of use.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Physical Security
- Physical security includes issues like perimeter security (office locked and alarmed when not in use); computer location (so that the screen may not be viewed by members of the public); and secure disposal of records (effective "wiping" of data stored electronically; secure disposal of paper records).

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The Data Protection Act does not detail specific security measures that a Data Controller or Data Processor must have in place. Rather section 27 of the Act places an obligation on persons to have appropriate security and organisational measures in place to prevent "unauthorised access to, alteration, disclosure of, accidental loss and destruction of the data in his control."
- However, when determining measures, a number of factors need be taken into account:
- The state of technological development;
- The cost of implementing measures;
- The harm that might result from unauthorised or unlawful processing;
- The nature of the data concerned;
- The special risks that exist in the processing of the data.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 5. Keep it accurate, complete and up-to-date
- Apart from ensuring compliance with the Act, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the duty of care provision in the Act applying to the handling of personal data which tends to arise substantially in relation to decisions or actions based on inaccurate data. In addition, it is also in the interests of your business to ensure accurate data for reasons of efficiency and effective decision making.
- To comply with this rule you should ensure that:
- your clerical and computer procedures are adequate with appropriate cross-checking to ensure high levels of data accuracy;

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- the general requirement to keep personal data up-to-date has been fully examined;
- appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.
- **Note:**
- The accuracy requirement does not apply to back-up data, that is, to data kept only for the specific and limited purpose of replacing other data in the event of their being lost, destroyed or damaged.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 6. Ensure that it is adequate, relevant and not excessive
- You can fulfil this requirement by making sure you are seeking and retaining only the minimum amount of personal data which you need to achieve your purpose(s). You should decide on specific criteria by which to assess what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose/s for which it is held.
- To comply with this rule you should ensure that the information sought and held is:

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- adequate in relation to the purpose/s for which you sought it;
- relevant in relation to the purpose/s for which you sought it;
- not excessive in relation to the purpose/s for which you sought it.
- A periodic review should be carried out of the relevance of the personal data sought from data subjects through the various channels by which information is collected, i.e. forms, website etc. In addition, a review should also be undertaken on the above basis of any personal information already held.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 7. Retain it for no longer than is necessary for the purpose or purposes
- This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the information is being retained. It is a key requirement of the Data Protection Act as personal data collected for one purpose cannot be retained once that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Act attach to it. If you don't hold it anymore then the Act does not apply.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- You should assign specific responsibility to someone for ensuring that files are regularly purged and that personal information is not retained any longer than necessary. This can include appropriate anonymisation of personal data after a defined period if there is a need to retain non-personal data.
- To comply with this rule you should have:
- a defined policy on retention periods for all items of personal data kept;
- management, clerical and computer procedures in place to implement such a policy.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- 8. Give a copy of his/her personal data to that individual, on request
- On making an access request any individual about whom you keep personal data is entitled to:
- a copy of the data you are keeping about him or her;
- know the categories of their data and your purpose/s for processing it;
- know the identity of those to whom you disclose the data;

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- know the source of the data, unless it is contrary to public interest;
- know the logic involved in automated decisions;
- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given.
- It is important that you have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- In response to an access request you must:
- supply the information to the individual promptly and within 28 days of receiving the request;
- provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained.
- If you do not keep any information about the individual making the request you should tell them so within the 28 days. However, the fee must be refunded if you do not comply with the request, or if you have to rectify, supplement or erase the personal data concerned.
- .

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- If you restrict the individual's right of access in accordance with one of the very limited restrictions set down in the Act, you must notify the data subject in writing within 28 days and you must include a statement of the reasons for refusal.
- Transferring Personal data Abroad
- An area of concern for many data controllers are the requirements necessary for the transfer of data abroad. There are special conditions that have to be met before transferring personal data outside Mauritius. This is termed a finding of adequacy. In such a case, one of the following conditions must be met if a transfer is to take place. Either the transfer must be:
- consented to by the data subject; or

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- necessary for the performance of a contract between the data controller and the data subject; or
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller; or
- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract; or

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- In the public interest, to safeguard public security or national security; or
- authorised by the Data Protection Commissioner, on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subjects, for instance, the approval of a contract which is based on EU model contracts or the transfer is by a US company which is certified as what is known as Safe Harbor compliant.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- Powers of the Data Protection Commissioner
- **Investigations by the Data Protection Commissioner**
- the Commissioner must investigate any complaints which she receives from individuals who feel that personal information about them is not being treated in accordance with the Act, unless she is of the opinion that such complaints are "frivolous or vexatious".
- The Commissioner's Decision can be appealed to the ICT Tribunal.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The Commissioner may also launch investigations on her own initiative, where she is of the opinion that there might be a breach of the Act, or where she considers it appropriate in order to ensure compliance with the Act. In practice, the investigations to ensure compliance take the form of privacy audits.
- The data controller gets advance notice and the aim of the privacy audit is to assist in improving data protection practices. It is only in the event of serious breaches being discovered or failure of the data controller to implement recommendations that further sanctions would be considered.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **The Commissioner's Power to Obtain Information**
- the Data Protection Commissioner may require any person to provide her with whatever information the Commissioner needs to carry out her functions, such as to pursue an investigation. The Commissioner exercises this power by providing a written notice, called an "information notice", to the person.
- A person who receives an information notice has the right to appeal it to ICT Tribunal.
- Failure to comply with an information notice without reasonable excuse is an offence. Knowingly to provide false information, or information that is misleading in a material respect, in response to an information notice is an offence. No legal prohibition may stand in the way of compliance with an information notice.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **The Commissioner's Power to Enforce Compliance with the Act**
- The Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Act. Such steps could include correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether.
- The Commissioner exercises this power by providing a written notice, called an "enforcement notice", to the data controller or data processor. A person who receives an enforcement notice has the right to appeal it to the ICT Tribunal.
- It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **The Commissioner's Power to Prohibit Overseas Transfer of Personal Data**
- As already mentioned before,the Data Protection Commissioner may prohibit the transfer of personal data from the State to a place outside the State.
- In considering whether to exercise this power, the Commissioner must have regard to the need to facilitate international transfers of information.
- It is an offence not to comply with the order of the Commisioner.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- **Power to prosecute offenders under Data Protection Act.**
- **Codes of Practice**
- The Commissioner can prepare and publish codes of practice for guidance in applying data protection law to particular areas. Codes of good practice, whether drawn up by the Commissioner or by other bodies as allowed by the law, may be enacted as regulations to have statutory effect.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

- The Commissioner has prepared four guidelines up to now which are currently in the process of publication, and will be made available to all data controllers very soon and a leaflet will also be circulated to the general public explaining the functions of the office. The fee charged for the purchase of the guidelines is Rs 350 each as provided as provided by the law whereas the leaflet will be free of charge.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

Thank You for your attention

Any Questions or Answers?

You are welcome