DATA PROTECTION OFFICE

- DATA PROTECTION REQUIREMENTS FOR THE ITES/BPO/KPO/LPO SECTOR
- PRESENTED BY THE DATA PROTECTION COMMISSIONER (MRS DRUDEISHA C-MADHUB)
- DATA PROTECTION OFFICE
- DEFENCE AND HOME AFFAIRS DEPARTMENT
- PRIME MINISTER'S OFFICE
- TEL:- 201 36 04
- EMAIL:- dmadhub@mail.gov.mu, pmo-dpo@mail.gov.mu
- Website:- http://dataprotection.gov.mu

DATA PROTECTION OFFICE

- *"There is no security on this earth, there is only opportunity."*

  – General Douglas MacArthur (1880-1964)

  Taking a cue from Gen MacArthur's quotation, BPO industry is just about opportunity and innovation. BPO has moved beyond being a mere 'buzzword' in corporate parlance. Today, it is not only a business necessity but a recipe for global reach and success.

DATA PROTECTION OFFICE

- The two key issues on which the success of the outsourcing sector hinges are confidentiality and data security since the biggest challenge of the sector is winning clients' confidence.
- Developing a culture of privacy and data protection is very important for the fitness and survival of the sector. People should also be trained on security issues and data handling.

DATA PROTECTION OFFICE

- New forms of crime such as e-commerce frauds through wrongful use of digital signatures and impersonation, phishing, identity theft, data theft, etc are not an uncommon feature in this sector.
- The world has witnessed the sale of confidential bank account details representing personal customer data and transfers of personal data by employees of BPO companies without the consent of their clients.
- The Data Protection Act represents the weapon in our legal armour against such data attacks in complementarity with:-

DATA PROTECTION OFFICE

- international data protection standards such as ISO 27001, SAS 70, ISO 17799, the signing of service level agreements contracted between offshore providers and the companies incorporating strict confidentiality and security clauses etc, which provide a well defined framework of dos and don’ts that ought to be followed by the outsourcing sector.
- This is to ensure that the use of safe software, techniques such as data encryption, copy protection, intrusion detection systems, firewalls, anti-virus tools, network security, system security systems and monitoring systems should also be favoured.

DATA PROTECTION OFFICE

- There are certain prerequisites for a safe, secure and reliable outsourcing sector:-
- Security of Data over Internet :

➢ To prevent data being lost to hackers on the Internet, you must deploy best firewalls available in the market.

➢ You must use data encrypting systems while receiving the data from clients and also sending back. This ensures that no one even in middle path of the Internet will be able to access the data.

➢ Only selected desktops and employees may have internet access whenever this is feasible within your sector or company for security reasons. You may also maintain separate networks for minimizing the risk of hacking into networks

DATA PROTECTION OFFICE

- **Security and Confidentiality from Employees :**
  - **You must have full trust on your expert and reliable manpower and know that they will never misuse their position in the organization as far as the security of the data is concerned.**
  - **You must perform security checks on the employees, general workforce and visitors to avoid any leakage of data through employees.**
  - **You must restrict the use of internet and emails to prevent transfer of data to any internal or external sources.**
  - **All of your staff, vendors, contractors and partners must sign strict confidentiality agreements with your company.**

DATA PROTECTION OFFICE

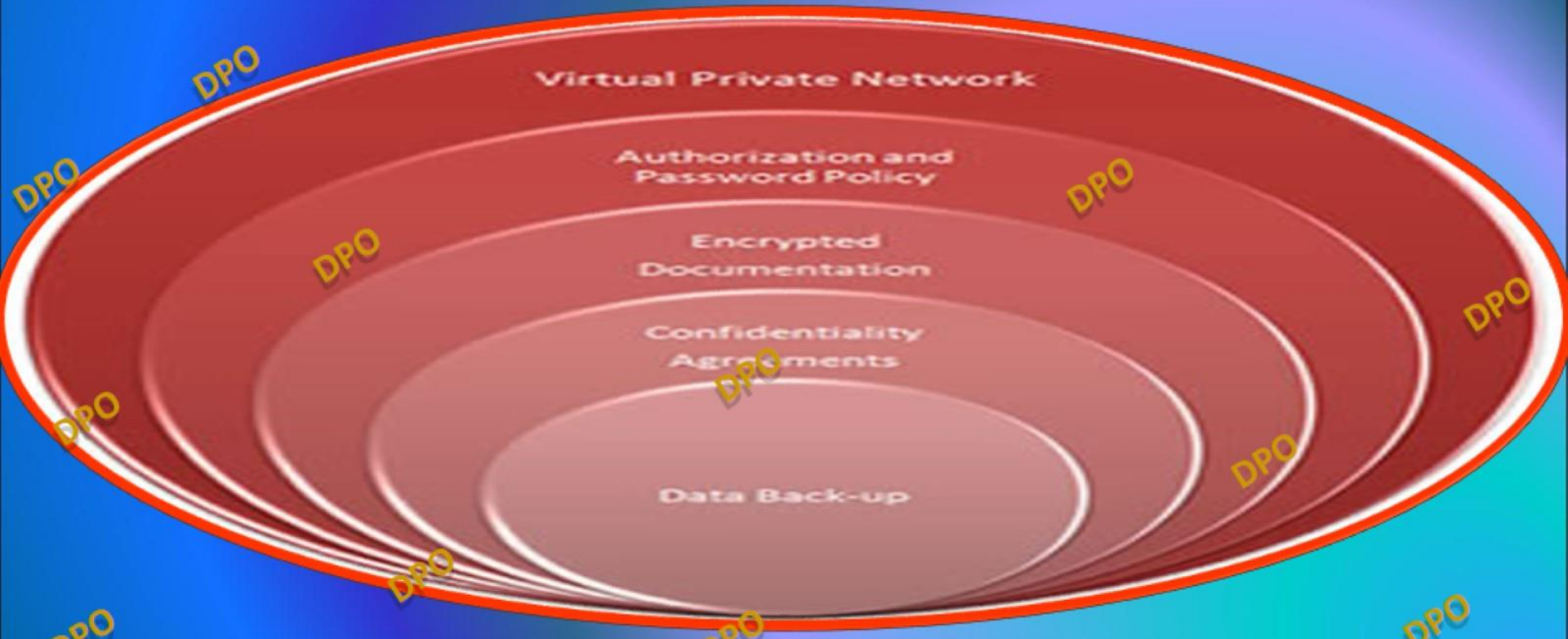
- You may sign confidentiality agreements with your employees prior to engaging them.
- You also need a well-maintained hardware :

  Your system engineers must protect your systems with Anti Virus programs to ensure continuity of work without technical disruptions
- You need Data Back-up and Recovery :

  Properly maintained Data backup and Recovery System for the employees and client reference.

DATA PROTECTION OFFICE

The following principles are thus to be followed to ensure data is tamper-proof:-



DATA PROTECTION OFFICE

- The Data Protection Act 2004 (DPA) gives individuals the right to know what information is held about them. It provides the legal framework to ensure that personal information is handled properly.

- The Eight Data Protection Principles which may be termed the mantras of data protection are as follows-

  - Personal data shall be processed fairly and lawfully.

  - Personal data shall be obtained only for a specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose.

  - Personal data shall be accurate and, where necessary, kept up to date.

DATA PROTECTION OFFICE

- Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of the data subjects under the Data Protection Act.

- Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

DATA PROTECTION OFFICE

- **What does processing, legally speaking, mean?**

"processing" means any operation or set of operations which is performed on the data wholly or partly by automatic means, or otherwise than by automatic means, and includes -

- collecting, organising or altering the data;
- retrieving, consulting, using, storing or adapting the data;
- disclosing the data by transmitting, disseminating or otherwise making it available; or
- aligning, combining, blocking, erasing or destroying the data;

DATA PROTECTION OFFICE

- For the purpose of the DPA, the data controller is the person who processes personal information of individuals and in our context, the data controller is the BPO company.

- Personal data is defined under the DPA as data, whether recorded electronically or otherwise, which relates to an identified or identifiable living individual, i.e, whose identity is apparent or can reasonably be ascertained from the data.

DATA PROTECTION OFFICE

- **What does sensitive personal data mean?**

  - It means personal information of a data subject which consists of information as to his/her -
  - racial or ethnic origin;
  - political opinion or adherence;
  - religious belief or other belief of a similar nature;
  - membership to a trade union;
  - physical or mental health;
  - sexual preferences or practices;
  - the commission of an offence; or
  - 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 such proceeding.

DATA PROTECTION OFFICE

Can sensitive data be processed by a data controller ?

- No sensitive data can be processed without the consent of the data subject or where the latter has made the data public, subject to certain further exceptions as provided in the Act.
- The data processor is the person, other than an employee of the data controller, who is required to register under the DPA.

DATA PROTECTION OFFICE

- Data controllers are the natural or legal persons, who determine the purposes and the means of the processing of personal data, both in the public and in the private sector.
- A medical practitioner would usually be the controller of the data processed on his clients; a company would be the controller of the data processed on its clients and employees; a sports club would control the data processed on its members and a public library controls the data processed on its users.

DATA PROTECTION OFFICE

- Where the data controller is not established in Mauritius, he must nominate a representative who resides in Mauritius to carry out his data processing activities through an office in Mauritius.

  Each data controller must adhere to the Data Protection Act where he is established in Mauritius and where he is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purposes of transit through Mauritius.

DATA PROTECTION OFFICE

How is an application made to the Data Protection Office for registration?

- It must be made in writing to the Commissioner by filling in the registration form for data controllers which contain the following information as required by the DPA:-
  - His/her name and address and that of his/her representative.
  - A description of the personal data being processed, the purpose for which it is being processed and the category and class of data subjects targetted, where possible their names.

DATA PROTECTION OFFICE

- A statement as to whether he/she holds sensitive personal data
- A description of the intended recipients to whom the data controller intend to disclose the personal data in his possession.
- A description of the country to which the data controller intends to transfer the data, directly or indirectly.

DATA PROTECTION OFFICE

- After the form is duly filled in and approved by the Commissioner and upon payment of the relevant fee, it will then be included in the public register which will be available at the DPO for viewing by the public and a copy may be also made available on request upon the payment of a fee of Rs 100. A list of registered controllers is also be available on the website.
- Remember to use a separate application form for each purpose for which you process personal data.

DATA PROTECTION OFFICE

- The types of personal data to be provided on the registration form may range from contact , financial, income, employment, medical, marital details to property owned, qualifications, amount of debt, transaction details.
- The purposes for their processing are actually the nature of the business being carried out.

DATA PROTECTION OFFICE

What if the data controller supplies false information to the Commissioner?

- It is an offence and the penalty is a fine not exceeding Rs 100,000 and imprisonment not exceeding 2 years.

For how long does the registration remain valid?

- It remains valid for a period of one year and if registration is not renewed, it will be cancelled.

Is it an offence not to register or to renew registration?

- Yes, the penalty is a fine not exceeding Rs 200,000 and imprisonment not exceeding 5 years.

DATA PROTECTION OFFICE

- Any change in address is to be notified in writing to the Commissioner within 15 days of the change. Otherwise, it is an offence.
- You may also request the Commissioner to remove your name from where it is contained in the register.
- An amendment has been brought to the DPA to include changes in particulars of the data controller to be notified in writing within 14 days to the Commissioner.

DATA PROTECTION OFFICE

- Remember it is an offence not to register if you are a data controller!
- The Commissioner may refuse an application for registration where:-
  - she reasonably believes that the details supplied to her by the applicant are insufficient or simply not furnished; or
  - appropriate safeguards for the protection of the privacy of the data subjects have not been provided by the data controller; or

DATA PROTECTION OFFICE

- the applicant is not a proper and fit person.

- The Commissioner must as soon as is reasonably practicable, notify in writing, the applicant of the reasons for refusal and of the fact that he may appeal to the ICT Tribunal.

DATA PROTECTION OFFICE

- **What can the Data Protection Office do when a data controller or a data processor contravenes the Data Protection Act?**

- Where the Commissioner finds that a data controller or a data processor is acting in violation of the Data Protection Act, she may serve an *enforcement notice* on the data controller or the data processor requiring him/her to take such steps within the period of time specified in the notice which must not be less than 21 days, to remedy the matter and implement the measures recommended by the Commissioner in the *enforcement notice*.

DATA PROTECTION OFFICE

- The data controller or the data processor must then notify the data subject of his compliance with the enforcement notice, not later than 21 days after such compliance.
- **Is it an offence not to comply with the enforcement notice?**

  Yes. Any person who does not comply with the enforcement notice and does not have a reasonable excuse for not complying will commit an offence, the penalty of which will be a fine not exceeding Rs 50,000 and imprisonment not exceeding 2 years.

DATA PROTECTION OFFICE

- Where the data controller is using the services of a data processor , he must ensure that the data processor is providing sufficient guarantees in respect of security and organisational measures.
- A data processor is also required to take all reasonable steps to ensure that any person employed by him is aware of and complies with relevant security measures.
- The written contract must provide that the data processor will act only on the instructions received from the data controller and the data processor will be bound by the obligations devolving on the data controller.

DATA PROTECTION OFFICE

- Minimum security arrangements would normally include the following physical and technical safeguards:-
- Physical safeguards- Access to computers should be restricted to authorised personnel only, premises alarmed and secure when not occupied.
- Technical Safeguards- Access to computers to be password-protected, PC workstation is subject to password-protected lock-out after period of inactivity, anti-virus software is in use, a firewall is used to protect systems connected to the internet.
- For sensitive data, it is recommended to use additional safeguards such as routine encryption of files and multi-level access control.

DATA PROTECTION OFFICE

- In determining the appropriate security measures, in particular, where the processing involves the transmission of personal data over an information and communication network, a data controller must consider the:-
- State of technological development;
- The cost of implementing any of the security measures;
- The special risks that exist in the processing of the data; and
- The nature of the personal data being processed;

as they are elaborated in section 27 of the DPA.

DATA PROTECTION OFFICE

- Under section 28 of the DPA, the data controller must notify the data processor holding data , where the purpose for keeping which has lapsed, to destroy it as soon as is reasonably practicable.
- Under section 29 of the DPA, any data processor, who without lawful excuse, discloses personal data processed by him without the prior authority of the data controller shall commit an offence, the penalty of which is a fine not exceeding Rs 200, 000 and imprisonment for a term not exceeding 5 years.

DATA PROTECTION OFFICE

- Under section 31 of the DPA, no data controller is allowed to transfer personal data to another country, except with the authorisation of the Commissioner. The word “transfer” is not defined in the DPA. The ordinary dictionary meaning of this word is transmission from one place, person, etc. to another. Transfer does not bear the same meaning as mere transit which refers for example, to data originating from Mauritius and routed through a server in Dubai on its way to Europe.

DATA PROTECTION OFFICE

- Before making a transfer, a data controller must consider whether it is possible for it to achieve its objectives without processing personal data at all and examine such options such as anonymisation of such data.
- Derogations from the Eighth Principle i.e, in which circumstances may a transfer to a country not offering adequate data protection take place:-
- Where the data subject has given his consent for the transfer;

DATA PROTECTION OFFICE

- or the transfer is necessary for the execution or intended execution of a contract between the data subject or any other person acting at the request of data subject or in the interest of the data subject and the data controller;
- or the transfer is necessary for the execution or intended execution of a contract between the data subject or any other person acting at the request of data subject or in the interest of the data subject and the data controller;
- or is in the public interest, to safeguard public security or national security;

DATA PROTECTION OFFICE

- or the transfer is made on such terms as may be approved by the Commissioner as ensuring adequate safeguards for the protection of the rights of the data subject;
- A transfer to a country not satisfying adequate safeguards may be effected.
- The adequacy of the level of protection in a particular country as regards personal data is assessed by the Commissioner by taking into consideration the following principles:-

DATA PROTECTION OFFICE

- The nature of the personal data;
- The purpose and duration of the proposed processing;
- The country of origin and country of final destination; the rules of law applicable in that particular country;
- any relevant codes of conduct and security measures applicable in that country;

DATA PROTECTION OFFICE

Where the particular country does not have any of the above-mentioned legal principles, Model Clauses as approved by the EU for transfers outside Europe which are recognised standard contractual clauses, safe harbor principles for transfers to the US or binding corporate rules, i.e, internal codes of conduct operating within a multinational organisation for transfers outside Europe may be considered as offering adequate safeguards by the Commissioner.

DATA PROTECTION OFFICE

- It is therefore imperative before any transfer of personal data is effected that these criteria are borne in mind and applied.

- What are the powers of the Commissioner?
  - to issue or approve codes of practice or guidelines;
  - create and maintain a register of all data controllers;
  - promote self-regulation among data controllers;

DATA PROTECTION OFFICE

- take such measures as may be necessary so as to bring to the knowledge of the general public the provisions of this Act;
- undertake research into, and monitor developments in, data processing and information technology, including data-matching and data linkage;
- examine any proposal for data matching or data linkage that may involve an interference with, or may otherwise have adverse effects on the privacy of individuals and, ensure that any adverse effects of such proposal on the privacy of individuals are minimised;

DATA PROTECTION OFFICE

- do anything incidental or conducive to the attainment of the objects of, and to the better performance of his duties and functions under this Act.

✓ **What are the other powers of the Commissioner?**

- Where the Commissioner is of the view that the investigation reveals the commission of a criminal offence under the Data Protection Act, she can refer the matter to the Police.

- The Commissioner can also request information from a person whenever it is required for the Commissioner to discharge her functions properly by sending a notice.

DATA PROTECTION OFFICE

- The Commissioner can also carry out security checks when she believes that the processing or transfer of data by a data controller will entail specific risks to the privacy rights of the data subjects to assess the security measures taken by the data controller prior to the beginning of the processing or transfer.
- The Commissioner can also carry out periodical audits of the systems of data controllers to ensure compliance with the data protection principles.
- An officer of the Data Protection Office may at any time enter and search the premises where data processing activities are being carried on.

DATA PROTECTION OFFICE

- **Who can make a complaint to the Data Protection Office?**

  Any individual or organization who feels that his privacy rights with regard to the processing of his personal data may have been affected.

- **What does the Data Protection Office do when it receives a complaint?**

  It investigates the complaint, unless the complaint is frivolous, and as soon as possible, notify the complainant in writing of its decision.

DATA PROTECTION OFFICE

✓**What can the complainant do if he/she is not satisfied with the outcome of the investigation?**

The complainant may appeal to the Information and Communication Technologies (ICT) Tribunal if he/she is not satisfied with the decision reached by the Commissioner.

DATA PROTECTION OFFICE

- **Dealing with Subject Access Requests**
- The key right for the individual is the right of access. Essentially this means that you as data controller have to supply to the individual the personal data that you hold if a valid request is made to you under Section 41 of the DPA.
- The data subject must fill in the request for access to personal data form available at the DPO and send it to you.
- The time limit for complying with an access request is 28 days. In order to ensure your compliance with the time limit and your other access obligations the following organisational and procedural steps may be effected:

DATA PROTECTION OFFICE

- Appoint a Co-ordinator or a Data Protection Officer who will be responsible for the response to the access request. A description of the functions and responsibilities of the Co-ordinator should be circulated within the organisation and staff should be advised of the necessity for co-operation with the Co-ordinator.
- All subject access matters should be submitted to the Co-ordinator.
- Check the validity of the access request. Ensure that it is in writing, that the appropriate fee of Rs 75 is included.

.

DATA PROTECTION OFFICE

- Check that sufficient material has been supplied to definitively identify the individual. This is most important as a third party may provide false material to lodge a false access request.
- Check that sufficient information to locate the data has been supplied. If it is not clear what kind of data is being requested you should ask the data subject for more information. This could involve identifying the databases, locations or files to be searched or giving a description of the interactions the individual has had with the organisation.
- Log the date of receipt of the valid request..

DATA PROTECTION OFFICE

- Keep note of all steps taken to locate and collate data – if different divisions of the organisation are involved, have the steps "signed off" by the appropriate person.
- Check each item of data to establish whether any of the restrictions on or denial of access provided by section 43 will apply.
- If data relating to a third party is involved, do not disclose without the consent of the third party such data. An opinion given by a third party may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.

DATA PROTECTION OFFICE

- Monitor process of responding to the request – observing time limit of **28 days.**
- Supply the data in an intelligible form (include an explanation of terms if necessary). Also provide description of purposes, disclosees and source of data (unless revealing the source would be contrary to the public interest and confidentiality obligations). Number the documents supplied. Have the response "signed-off" by an appropriate person.
- Regularly review your procedures and processes.
- If either the data controller or the data processor receives a request for information from another jurisdiction, the data controller will need to comply with the request.

DATA PROTECTION OFFICE

Thank You

Any questions?

Comments?