PRIME MINISTER'S OFFICE
DATA PROTECTION OFFICE

An overview of the Mauritian Data Protection Act with regard to its legal implications on the rights of data subjects and the corresponding legal obligations of data controllers and data processors for guaranteeing these rights namely the protection of personal data for processing purposes.

PRESENTED BY:

MRS D. CAULLYCHURN-MADHUB
SENIOR STATE COUNSEL &
DATA PROTECTION COMMISSIONER

30.11.07

OBJECTIVES

- The objectives which the DATA PROTECTION OFFICE is striving to attain in its ambitious endeavour to protect in an efficient manner the privacy rights of all individuals are founded on the following principles derived from :-

  - Article 12 of the Universal Declaration of Human Rights of 10 December 1948 provides:-

    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.

OBJECTIVES

- Article 17 of the International Covenant on Civil and Political Rights of 16 December 1966 to which Mauritius is a party provides:-
  - No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
  - Everyone has the right to the protection of the law against such interference or attacks.
- And in compliance with the EU Directive 95/46 to secure investment in the country.

OBJECTIVES

- The data protection office derives its existence from the the Data Protection Act 2000 (DPA) and up to now only sections 1, 2, 4, 5 (b), (c), (e), (g), (h), (i), (j) and 6 of the Act have been proclaimed, that is, have force of law since 27.12.04 whereas the other provisions of the Act do not yet enjoy legal existence as they have not yet been proclaimed.

OBJECTIVES

- It is the urgent priority of this office to have the DPA as a whole proclaimed for the proper launching of the office.
- The relevant documents have already been sent to the Senior Chief Executive of the PMO for the proclamation together with the required regulations, a draft of the website, the relevant guidelines for data controllers and data subjects and a leaflet addressed to the general public.
- The Data Protection Act 2004 (DPA) gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

OBJECTIVES

- Should an individual or organisation feel they're being denied access to personal information they're entitled to, or feel their information has not been handled according to the DPA, they can contact the Data Protection Office for help.

- However, though not all the sections of the DPA have yet been proclaimed, the Commissioner, do enjoy the following powers, as they are provided in section 5 of the Act:-

  - to issue or approve codes of practice or guidelines;
  - create and maintain a register of all data controllers;
  - promote self-regulation among data controllers;

OBJECTIVES

- 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 computer technology, including data-matching and data linkage, ensure that any adverse effects of such developments on the privacy of individuals are minimized;

- 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;

- 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 data protection principles?

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for any 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.
- 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.

What are the data protection principles?

- 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 a third country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

- **Is the Data Protection Office a public one?**

Yes.

- **What is the composition of the Data Protection Office for the time being?**

The Office consists of the Commissioner for the time being, who is also the head of the office.

What is the mission of the Data Protection Office?

The mission of the Data Protection Office is to safeguard the privacy rights of all individuals with regard to the processing of their personal data, in Mauritius.

What are the functions of the Commissioner?

She registers all data controllers in Mauritius, exercises control over all data processing activities in Mauritius, investigates complaints, undertakes research in data processing and computer technology, amongst others.

Who can make a complaint to the Data Protection Office?

Any individual or organization who feel that their privacy rights with regard to their 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.

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*.

- 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.

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.

- 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.

What are the other powers of the Commissioner?

- 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.
- If it is a dwelling house, the officer must show a warrant to enter and search the dwelling house issued by a magistrate.
- An officer of the Data Protection Office may at any time enter and search the premises where data processing activities are being carried on.
- If it is a dwelling house, the officer must show a warrant to enter and search the dwelling house issued by a magistrate.

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.

What is data?

- Data means information which can be processed by automated means or manually through a filing system.

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.

✓ Can sensitive data be processed by a data controller ?

- No sensitive data can be processed without the consent of the data subject or the latter has made the data public, subject to certain further exceptions as provided in the Act.

✓ Who is a data controller ?

- A data controller is a person or a group of persons who decide as to the purposes for which personal data is to be processed.

Are you a "data controller"?

- Data controllers are the people or body, who determine the purposes and the means of the processing, 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 controllers are required to observe several principles. These principles not only aim to protect the data subjects but also are a statement of good business practices that contribute to reliable and efficient data processing.

Each data controller must adhere to the Data Protection Act when 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.

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.

A data controller is therefore the natural person (the individual) or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

Being a data controller carries with it serious legal responsibilities, so you should be quite clear if these responsibilities apply to you or your organisation. If you are in any doubt, or are unsure about the identity of the data controller in any particular case, you should consult your legal adviser or seek the advice of the Data Protection Commissioner.

In essence, you are a data controller if you can answer **YES** to the following question:-

- Do you keep or process any information about living people?
- In practice, to find out who controls the contents and use of personal information kept, you should ask yourself the following questions:-
- Who decides what personal information is going to be kept?
- Who decides the use to which the information will be put?

If your organisation controls and is responsible for the personal data which it holds, then your organisation is a data controller. If, on the other hand, you hold the personal data, but some other organisation decides and is responsible for what happens to the data, then that other organisation is the data contoller, and your organisation is a "data processor".

Data Processors

- As mentioned above, if you hold or process personal data, but do not exercise responsibility for or control over the personal data, then you are a "data processor".
- Examples of data processors include payroll companies, accountants and market research companies, all of which could hold or process personal information on behalf of someone else.
- A data processor is distinct from the data controller for whom they are processing the personal data. An employee of a data controller, or a section or unit within a company which is processing personal data for the company as a whole, is not a "data processor".
- However, someone who is not employed by the data controller, but is contracted to provide a particular data processing service (such as a tax adviser, or a telemarketing company used to manage customer accounts) would be a data processor.

Data Processors

- A subsidiary company owned by a data controller to process personal data on its behalf (for example to manage the payroll) is a distinct legal person and is a data processor.

- It is possible for one company or person to be both a data controller and a data processor, in respect of distinct sets of personal data.

- For example, a payroll company would be the data controller in respect of the data about its own staff, but would be the data processor in respect of the staff payroll data it is processing for its client companies.

Responsibilities of Data Processors

- Unlike data controllers, data processors have a very limited set of responsibilities under the Data Protection Act.

- These responsibilities concern the necessity to keep personal data secure from unauthorised access, alteration, unlawful disclosure, destruction or accidental loss and the duty to destroy data whenever he receives such a notification from the data controller

How is the Act enforced ?

- The Commissioner's role is to ensure that those who keep personal information comply with the provisions of the Act.
- These powers include the serving of legal notices compelling data controllers to provide information needed to assist his enquires, or compelling a data controller to implement one or more provisions of the Acts. She may investigate complaints made by the general public or carry out investigations proactively.
- She may, for example, authorise officers to enter premises and to inspect the type of personal information kept, how it is processed and the security measures in place. You and your staff must cooperate fully with such officers.
- A data controller found guilty of an offence under the Acts can be fined to a maximum of Rs 200,000 and imprisoned to a maximum of five years.

Basic Data Protection Checklist

- Are the individuals whose data you collect aware of your identity?
- Have you told the data subject what use you make of his/her data?
- Are the disclosures you make of that data legitimate ones?
- Do you have appropriate security measures in place?
- Do you have appropriate procedures in place to ensure that each data item is kept up-to-date?

Basic Data Protection Checklist

- Do you have a defined policy on retention periods for all items of personal data?
- Do you have a data protection policy in place?
- Do you have procedures for handling access requests from individuals?
- Are you clear on whether or not you should be registered?
- Are your staff appropriately trained in data protection?
- Do you regularly review and audit the data which you hold and the manner in which they are processed?

What is the scope of the exemptions provided in the Data Protection Act ?

- Personal data which is required for the purposes of:-
  - safeguarding national security;
  - the prevention or detection of crime;
  - The prosecution of offenders;
  - The collection of any tax, duty or any such similar charges;
  - health and social work;

What is the scope of the exemptions provided in the Data Protection Act ?

- journalism, literature, art, research, history and statistics;
- where information is required to be made available to the public by the law or in connection with legal proceedings;
- domestic purposes; and
- confidential information between client and legal practitioner, is exempt from the application of certain or all provisions of the Data Protection Act

MAIN RESPONSIBILITIES

- **Registration**
- Are we clear about whether or not we need to be registered with the Data Protection Commissioner?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? *[Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]*
- Is a named individual responsible for meeting our registration requirements?

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

- It must be made in writing to the Commissioner and it must contain the following information:-
  - His/her name and address or that of his/her representative.
  - A description of the personal data being processed, the purpose for which it is being processed and the category of data subjects targetted, where possible their names.
  - A statement as to whether he/she holds sensitive personal data
  - A description of the intended recipients of the information detained by the data controller.
  - A description of the country to which the data controller intends to transfer data.

Where an offence is committed, which court has jurisdiction to try the criminal case?

- The Intermediate Court will have jurisdiction.

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.

MAIN RESPONSIBILITIES

How to organize yourself to ensure the protection of data within your organization?

- The right of access is the most important right that an individual has and you need to organize yourself for handling access requests. Dealing with access requests is not your only obligation. Staff should also be made aware of the obligations imposed by the Data Protection Act.

MAIN RESPONSIBILITIES

To comply you should:

- Ensure that the basic principles of data protection are explained to staff;
- Ensure that there are regular updates to guidance material and staff training and awareness, so that data protection is a "living" process aligned to the way the organisation conducts its business;
- Document procedures, for example with regard to accuracy and have regular security reviews;
- Allocate responsibility for compliance and set-out what in-house sanctions may be imposed if correct procedures are not followed;
- Set out the circumstances in which personal data may be disclosed to third parties.

MAIN RESPONSIBILITIES

- Obligations on retention and security need to be addressed
- Adhere to the 'need to know principle' – only personal data necessary for the purpose should be collected and staff should only be able to access the personal data that they need to carry out their functions;
- Have adequate access controls, firewalls and virus protection and do not forget manual files;
- There should be retention policies for the various categories of data.

MAIN RESPONSIBILITIES

- Dealing with Subject Access Requests
- The key right for the individual is the right of access. Essentially this means that you have to supply to the individual the personal data that you hold if a valid request is made under Section 41.
- 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:

MAIN RESPONSIBILITIES

- 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 is included.

MAIN RESPONSIBILITIES

- 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.

MAIN RESPONSIBILITIES

- 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.

MAIN RESPONSIBILITIES

- 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). Number the documents supplied. Have the response "signed-off" by an appropriate person.
- Regularly review your procedures and processes.

MAIN RESPONSIBILITIES

- **Self Regulation and Codes of Practice**
  The requirements of data protection law are quite clear, and applying the rules and principles of data protection to your business activities is often a matter of common sense.

- However, for some businesses and professions, interpreting and applying data protection law is not so straightforward, and sometimes requires a fine appreciation of the ethical norms and standards, and the traditional expectations of good practice, associated with that sector.

MAIN RESPONSIBILITIES

- For that reason, Section 56 of the Data Protection Act 2004 provides that the Commissioner may approve codes of practice elaborated by data controllers which should have a direct input into the establishment of data protection standards within their sector.

MAIN RESPONSIBILITIES

- It is a matter for the data controller to devise a code of practice that is appropriate to his sector. If the Commissioner agrees that the code provides adequate data protection for individuals, then the code of practice may be approved by her and incorporated through regulations to be enacted under the Act. The code will then have the force of law, and will be binding upon all data controllers in that sector.

MAIN RESPONSIBILITIES

- The Commissioner will keep a register of approved codes and guidelines which will be available for public inspection. Upon the payment of the prescribed fee, provide copies or extracts from the register.

MAIN RESPONSIBILITIES

How can the Data Controller initiate a statutory Code of Practice?

- If you would like to initiate a code of practice, to clarify how data protection rules are to be applied for your sector, then we suggest that you contact the Data Protection Commissioner, with a view to arranging discussions to progress the matter. The Commissioner will be glad to provide you with practical advice on what should be covered in your code of practice, and on how circumstances specific to your sector might be handled.

Your Rights

Under section 41 of the Data Protection Act, any individual may make a written request to the data controller, who keeps personal information regarding that particular individual on computer or in a relevant filing system and is entitled to:

>> A copy of the data upon payment of the prescribed fee,

>> Whether the data kept by the data controller include personal data relating to the data subject, (c) a description of the purposes for which it is held and (d) a description of those to whom the data may be disclosed unless compliance with such a request would be in breach of the confidentiality obligation of the data controller.

Your Rights

Every individual about whom a data controller keeps personal information on computer or in a relevant filing system, has a number of other rights under the Act, in addition to the Right of Access.

These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

Your Rights

The data controller is also obliged to explain to the data subject the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process.

This "right of access" is subject to a limited number of exceptions, which are listed below.

Your Rights

An individual making an access request must:-

Apply to the data controller in writing by filling in the request for access to data form available on the website or at the Data Protection Office ,

Give any details which might be needed to help the data controller identify him or her and locate all the information the data controller may keep about him/her.

The individual must also pay the data controller the access fee

Your Rights

Are there exceptions or limitations on the right of access to personal data?

Yes, there are. Section 43 of the Data Protection Act provides that the right of access does not apply in a number of cases.

The restrictions upon the right of access fall into five groups:

The obligation to comply with an access request does not apply where the data controller is not supplied with the information he reasonably requires in order to satisfy himself as to the identity of the person making the request and to locate the information which the person seeks;

Your Rights

Where compliance with the request would be in contravention of the confidentiality obligation of the data controller under the Mauritian law;

The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion except where that expression of opinion was given in confidence;

The right of access does not include the revelation of evidence of the commission of a criminal offence other than an offence under the Act.

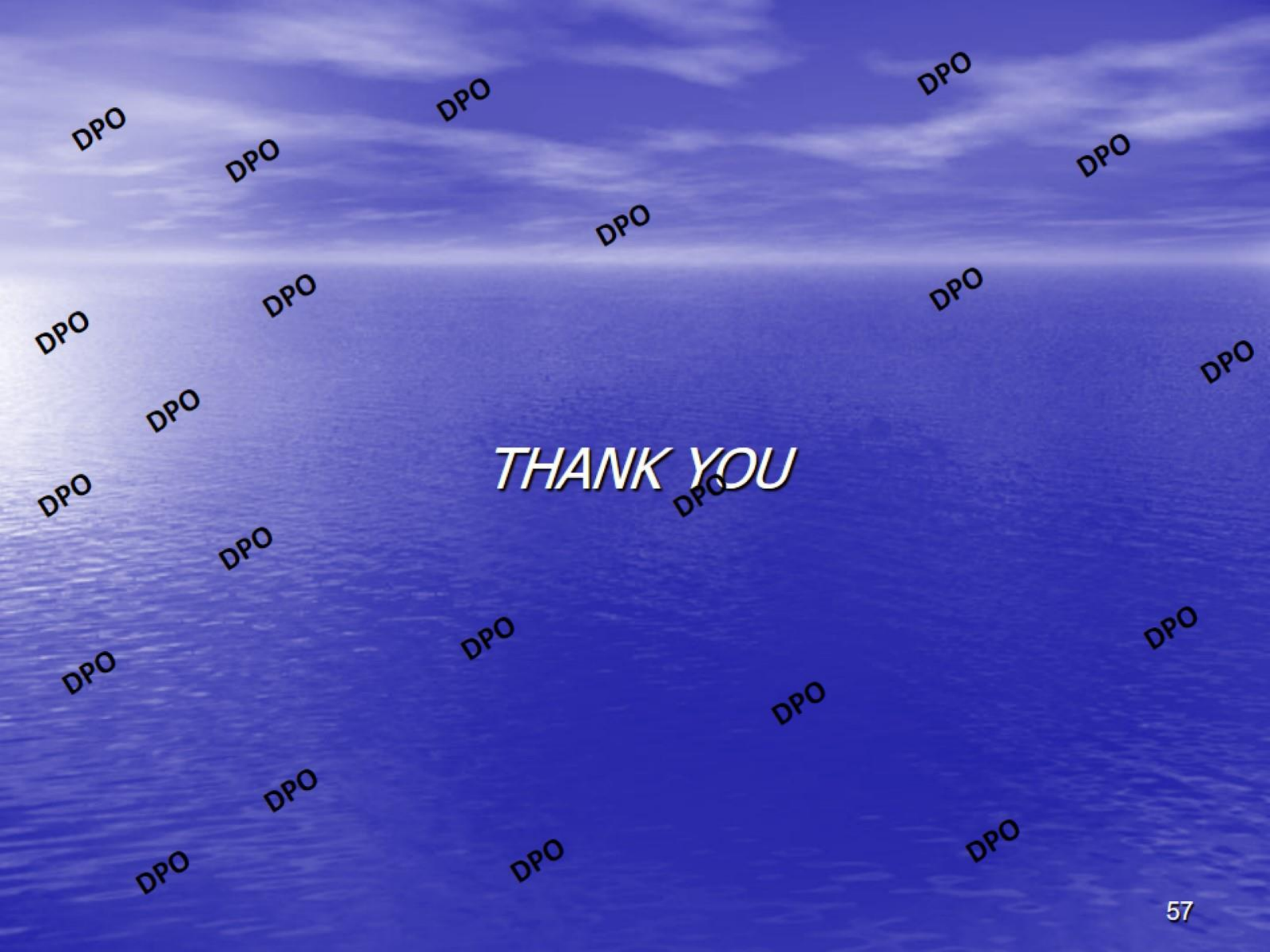
Your Rights

Where the data controller cannot comply with the request without disclosing personal data relating to another person, he may refuse the request unless the other individual has consented to the disclosure of his personal data to the person making the request or he obtains the written approval of the Commissioner;

The right of access does not include information given in confidence to the data controller for the purposes of the education, training or employment, or prospective education, of the data subject, the appointment or prospective appointment of the data subject to any office, the provision or prospective provision by the data subject of any service, the personal data requested consist of information recorded by candidates during an academic, professional or other examination;

Contact details

- **Address:** Data Protection Office
  6th Floor,
  New Government Centre,
  Port Louis
- **Phone:** + (230) 201 3604
- **Email:** dmo-dpo@mail.gov.mu
- **Website:** www.dataprotection.gov.mu


DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
DPO
THANK YOU