



TRAINING ON DATA PROTECTION

Presented by:

- 1) **Mr Vivekanand Bhantoo (DPO/SDPO)**
- 2) **Mr Reza Mukoon (DPO/SDPO)**

Date: Thursday 14th April 2016

Venue: Talents Centre, Pierrefonds

Today's Overview

1

- Familiarize yourself with the Data Protection Act

2

- Understand some key definitions

3

- Be aware of the Data Protection Principles

4

- Privacy Impact Assessment (PIA)

5

- Case Study

6

- Cloud Computing

7

- Disclosure of information

8

- Data Sharing

9

- Data Security

10

- Best Practices

DATA PROTECTION ACT (DPA)



THE ACT IN A NUTSHELL

PART I

- **PRELIMINARY - Definitions etc.**

PART II

- **DATA PROTECTION OFFICE**

PART III

- **POWERS OF COMMISSIONER**

PART IV

- **OBLIGATION ON DATA CONTROLLERS : S22 – S32**

PART V

- **THE DATA PROTECTION REGISTER : S33 – S40**

PART VI

- **RIGHTS OF DATA SUBJECT : S41 – S44**

PART VII

- **EXEMPTIONS: S45 – S54**

PART VIII

- **MISCELLANEOUS**

DATA PROTECTION ACT

AN ACT

To provide for the **protection** of the **privacy rights of individuals** in view of the developments in the techniques used to **capture, transmit, manipulate, record or store data** relating to individuals.

DEFINITIONS



DEFINITIONS

Data means information in a form which –

- a) (i) is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and
- (ii) is recorded with the intent of it being processed by such equipment; or
- b) is recorded as part of a relevant filing system or intended to be part of a relevant filing system;

DEFINITIONS (Cont.)

Personal Data means –

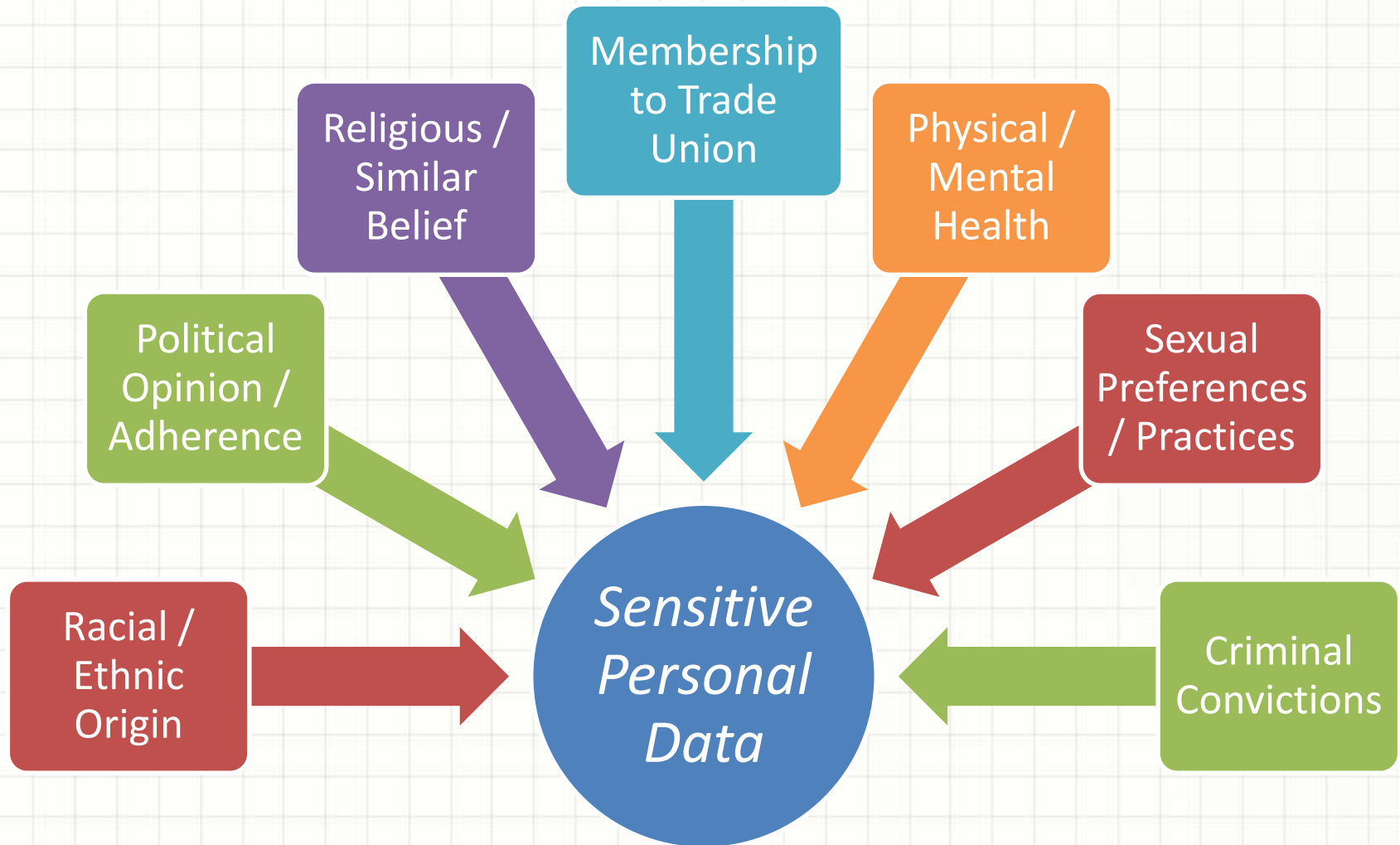
- a) data which relate to an individual who can be identified from those data;**
- a) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;**

EXAMPLES OF PERSONAL DATA

- ❖ Name of individual
- ❖ Address
- ❖ Car Registration No.
- ❖ Telephone No.
- ❖ Bank Account No.
- ❖ Email

DEFINITIONS (Cont.)

Sensitive Personal Data



DEFINITIONS (Cont.)

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;

8 PRINCIPLES OF DATA PROTECTION ACT



DATA PROTECTION PRINCIPLES

First Principle

Personal data shall be processed fairly and lawfully.

DATA PROTECTION PRINCIPLES

Practical Steps

For example, if an organisation is collecting personal data using application forms, the organisation is advised to explain the purposes/uses etc. on such forms such as:

- **This data will be used by the organisation for xxxx purposes.**
- **All personal data will be processed in accordance with the Data Protection Act 2004.**
- **I agree/disagree that the organisation processes my personal data in the way described above.**

DATA PROTECTION PRINCIPLES

Second Principle

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.

DATA PROTECTION PRINCIPLES

Practical Steps

Prepare a statement of the purpose/purposes for which the organisation holds information about others.

Remember:

Any individual has the right to ask the organisation to state the purpose/s for which such information is kept.

DATA PROTECTION PRINCIPLES

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.

DATA PROTECTION PRINCIPLES

Practical Steps

Decide on specific criteria by which to decide what is adequate, relevant, and not excessive.

Apply those criteria to each information item and the purposes for which it is held.

DATA PROTECTION PRINCIPLES

Fourth Principle

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

DATA PROTECTION PRINCIPLES

Practical Steps

Assign specific responsibility for data accuracy under the Data Protection Act and arrange periodic review and audit.

DATA PROTECTION PRINCIPLES

Fifth Principle

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

DATA PROTECTION PRINCIPLES

Practical Steps

Assign specific responsibility to someone for ensuring that files are regularly purged and that personal information is not retained any longer than necessary.

DATA PROTECTION PRINCIPLES

Sixth Principle

Personal data shall be processed in accordance with the rights of the data subjects under this Act.

DATA PROTECTION PRINCIPLES

Under section 41 of the Data Protection Act, on making **a written request** to a data controller, any individual about whom a data controller keeps personal information on computer or in a relevant filing system is entitled to:

- a copy of his/her data upon payment of the prescribed fee (Rs 75),
- whether the data kept by him include personal data relating to the data subject,
- a description of the purposes for which it is held;

DATA PROTECTION PRINCIPLES

Seventh Principle

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.

DATA PROTECTION PRINCIPLES

Practical Steps

Compile a checklist of security measures for your own systems.

In addition, where an agent is being retained to process personal data on behalf of the organisation, there should be a sound contractual basis for this, with appropriate security safeguards in place.

DATA PROTECTION PRINCIPLES

Eighth Principle

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 PRINCIPLES

- Authorisation is required from the Data Protection Commissioner to transfer data abroad.
- Organisation must fill and submit to this office the 'Transfer of Personal Data Form' available on <http://dataprotection.govmu.org>

PRIVACY IMPACT ASSESSMENT (PIA)



PRIVACY IMPACT ASSESSMENT (PIA)

PIA Tool or Questionnaire

- Privacy Assessment is seen as a valuable tool for businesses & governments.
- This application will enable public and private bodies to make informed choices.
- It will often be the case that a privacy enhancing solution will be no more difficult or more costly to implement than an intrusive one, if the option is identified sufficiently.
- However, this should not be the motivation since we are here dealing with the human right to privacy.

PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Assessment

- Protection of privacy is more than simply avoiding a breach of the law. It involves striving for something better.
- Privacy Impact Assessments & Privacy Compliance Assessments are new techniques which are increasingly being used internationally to better manage privacy risks.

PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Assessment (Cont.)

- Others include audits, privacy seals and associated self-regulatory initiatives and privacy enhancing technologies.
- Each builds on the bedrock of the enforceable privacy rights for citizens and consumers enshrined in law.

PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Assessment (Cont.)

- These assessments are being encouraged as a means by which business and government can proactively identify and avoid privacy problems.
- Internationally, these assessments play an important part of a policy approach to build trust and confidence in business and these processes are recommended as part of any new Project such as the HRMIS in the public sector.

PRIVACY IMPACT ASSESSMENT (PIA)



The screenshot shows the Data Protection Office website. The main banner reads "DATA PROTECTION OFFICE YOUR PRIVACY, OUR CONCERN". The navigation menu includes "About Us", "The Law", "Data Controllers", "Downloads and Links", "Decisions", "Related Laws", and "Essentials". The "Documents/Forms" section lists several items, with the "Self Assessment - Questionnaire on Data Protection for Data Controllers and Processors - pdf format" highlighted in red. The "MISSION" statement is "Safeguarding the processing of your personal data in the present age of Information and Communication."

Web Links

► For registration or renewal of registration as a data Controller

MISSION

Safeguarding the processing of your personal data in the present age of Information and Communication.

Documents/Forms

- List of Registered Data Controllers - Employee
- List of Registered Data Controllers - Non-Employee
- Data Protection Audit Questionnaire for Data Controllers and Data Processors - pdf format
- Data Protection Audit Questionnaire for Data Controllers and Data Processors
- Self Assessment - Questionnaire on Data Protection for Data Controllers and Processors - pdf format**
- Self Assessment - Questionnaire on Data Protection for Data Controllers and Processors

Privacy Assessment (Cont.)

- The questionnaire from website (*highlighted in red*).
- Demo of application

PRIVACY IMPACT ASSESSMENT (PIA)

Privacy By Design

- Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.
- Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.
- It helps organisations comply with their obligations under the legislation.

PRIVACY IMPACT ASSESSMENT (PIA)

Privacy By Design

- The Data Protection Office encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle.
- For example when:
 - building new IT systems for storing or accessing personal data;
 - developing legislation, policy or strategies that have privacy implications;
 - embarking on a data sharing initiative; or using data for new purposes.

PRIVACY IMPACT ASSESSMENT (PIA)

Benefits of taking a 'Privacy By Design' Approach

- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the DPA.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

PRIVACY IMPACT ASSESSMENT (PIA)

Benefits of taking a 'Privacy By Design' Approach (Cont.)

- Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust.
- Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:
 - ✓ Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
 - ✓ Increased awareness of privacy and data protection across an organisation.
 - ✓ Organisations are more likely to meet their legal obligations and less likely to breach the DPA.
 - ✓ Actions are less likely to be privacy intrusive and have a negative impact on individuals.

CASE STUDY



CASE STUDY

- **Fingerprint for attendance purpose**
 - Decision of the DPC
 - ✓ Decision 17 & 19
 - Determination of ICT Appeal Tribunal
 - ✓ 9 April 2015 & 5 August 2015

CLOUD COMPUTING



CLOUD COMPUTING

Cloud Computing in Organisations

- Organisations are increasingly moving to cloud across all application areas as well as platform and infrastructure investments.
- Cloud deployments are growing in size, and more mission-critical areas of their business are being run out of the cloud.
- Cloud is also becoming a new way to engage directly with customers and partners

CLOUD COMPUTING

Various Types of Cloud

- On premise
- Out of premise (Public Cloud)
- Hybrid

CLOUD COMPUTING

Two major issues

- **Cloud sourcing is an underdeveloped capability and requires newer skills and experiences.**
- **Contract requirements negotiation checklist which organisations have to work out with all their stakeholders to support their business strategy.**

CLOUD COMPUTING

Data Protection issues

- You will have to seek authorisation from the Data Protection Commissioner for the transfer of data abroad.
- Retention period depends on the purpose of the processing of the personal data as per section 28 of DPA.
- The duration which has to be determined by you must be reasonably justified.

CLOUD COMPUTING

Data Protection issues (Cont.)

- Section 27 of DPA explains the shared legal responsibilities between a data controller (Organisation) and a data processor (the cloud provider).
- Hence, the data controller must ensure that any selected cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organisation.

CLOUD COMPUTING

Data Protection issues (Cont.)

- Encryption is recommended during the transit of data from your company to the cloud provider.
- The country where the cloud provider is operating should have data protection principles in force.
- In other cases, there is a need to have data protection clauses in your contract.

CLOUD COMPUTING

Data Protection issues (Cont.)

- Encryption is recommended during the transit of data from your company to the cloud provider.
- The country where the cloud provider is operating should have data protection principles in force.
- In other cases, there is a need to have data protection clauses in your contract.

CLOUD COMPUTING

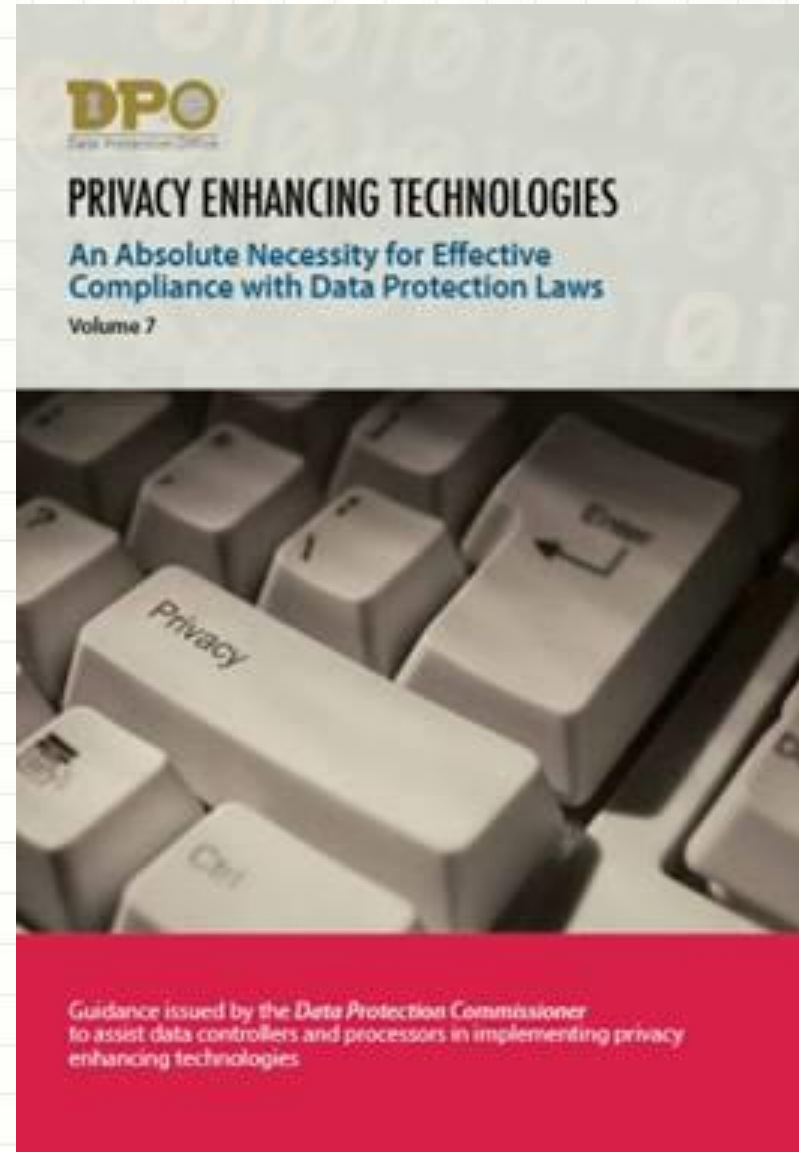
Data Protection issues - Contract

- You will need to have a written contract with the cloud provider that covers the following points amongst others:
 - Continuity of service, backups and integrity.
 - Certification such as ISO 27001 compliant.
 - Auditing of the cloud provider by third party.
 - Appropriate access rights are provided to officers of your company for creation, amendment and deletion of data with audit trails.
 - Termination of contract: Ensure that all personal data are returned to you and no copies are kept at the cloud provider.

CLOUD COMPUTING

Guideline

- Consult our guideline titled *Vol. 7- “Privacy Enhancing Technologies An Absolute Necessity for Effective Compliance with Data Protection Laws”* which covers cloud computing technology and which is available on our website address <http://dataprotection.govmu.org> under publications.



CLOUD COMPUTING

Other useful reference

- **“Brief: Cloud Contract Negotiations Checklist”**
- **Forrester report for an overview of the key areas you need to consider when negotiating a cloud contract and advice for negotiating with cloud vendors.**

DISCLOSURE



DISCLOSURE OF INFORMATION

An organisation must ensure that personal information in its possession is not disclosed in any manner incompatible with the purposes for which such data has been collected, which is an offence under section 29 of the Data Protection Act.

DISCLOSURE OF INFORMATION

The principle is that the prior consent from the concerned data subject should be obtained before any disclosure is made, unless the exceptions under section 24(2) of the DPA are applicable in the circumstances as follows:

- For the performance of a contract to which the data subject is a party and/or;
- For compliance with any legal obligation to which the organisation is subject.

DATA SHARING



DATA SHARING

The organisation who owns the personal data, i.e. the data controller, is responsible for the personal data in his custody.

As per section 24(1) of the Data Protection Act, the express consent of the data subject is required before sharing can be done and the data subject should be informed of that at the time of collection of the personal data according to section 22 of DPA.

DATA SHARING

However, as per section 24(2) of the Data Protection Act, personal data may be processed without obtaining the express consent of the data subject where the processing is necessary:

- for the performance of a contract to which the data subject is a party;
- in order to take steps required by the data subject prior to entering into a contract;
- in order to protect the vital interests of the data subject;
- for compliance with any legal obligation to which the data controller is subject;
- for the administration of justice; or
- in the public interest.

DATA SHARING

In the absence of the application of sections 24(1) and 24(2) of the Data Protection Act and any legislation/act which authorises the data to be shared, amendment to existing legislation/act is required to allow the sharing to be done.

DATA SHARING

Whenever data sharing is taking place, the data controller(i.e the organisation who owns the data) has to ensure that organisational and technical measures are in place to protect the data being shared.

DATA SHARING

Further information may be obtained in the guideline:
“Vol. 9 - Practical Notes on Data Sharing Good Practices for the Public and Private Sector”, which is available on our website at

[http://dataprotection.govmu.org/English/Documents
/Publications/Guidelines/Data_Sharing.pdf](http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/Data_Sharing.pdf)

DATA SECURITY



RISK



THREATS TO DATA PRIVACY

- **Identity Theft**
- **Data Breach**

IDENTITY THEFT

Identity theft occurs when someone uses your personally identifying information, like your name, social security number, or credit card number, without your permission, to commit fraud or other crimes.

DATA BREACH

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorised to do so.

BEST PRACTICES



EMPLOYEE OR END USER EDUCATION

- All relevant security policies must be clearly explained to staff.
- A clear explanation of the consequences for violating these policies must also be explained.
- The end user needs to sign a document acknowledging that they understand the policies and consequences for violating these policies.

STANDARDS

- **Data Security is subject to several types of audit standards and verification.**

Example - ISO 27001/27002 : ISMS

- **Security Administrators are responsible for creating and enforcing a policy that meets the standards that apply to their organisation's business.**

DATA CLASSIFICATION

- **Data needs to be classified in the security policy according to its sensitivity.**
- **Once this has taken place, the most sensitive data requires extra measures in place to safeguard and ensure its integrity and availability.**
- **All access to personal data must be logged using audit trail.**

PHYSICAL / TECHNICAL CONTROLS

- Physical access must be controlled to the data center or area where the data is stored.
- Fine Grained Access control must be implemented to define which user needs what type of access / no access on which data.
- Encryption of data is recommended for transmission of data across networks.

SYSTEM AND NETWORK SECURITY

- **The use of firewalls to protect against intrusions.**
- **Disconnect unused data points.**
- **If wireless is deployed, use authentication servers to verify and log the identity of those logging on.**
- **Anti-Virus and malicious software protection on all systems.**

SUMMARY

PRIVACY

SECURITY

PROTECTION

SAFETY



RESOURCES


The Data Protection website

-  Web Links
-  Documents / Forms
-  <http://dataprotection.govmu.org/English/Pages/default.asp>

The Law

-  <http://dataprotection.govmu.org/English/Legislation/Pages/default.aspx>

Guidelines

-  <http://dataprotection.govmu.org/English/Pages/Guidelines/Publications---Guidelines.aspx>

THANK YOU









APPENDIX

USEFUL REFERENCE & LINKS

The National Computer Board

-  Useful for any relevant documentation in ICT
 -  Legislations (Computer Misuse & Cybercrime Act 2003, etc.)
 -  Knowledge Bank (Guidelines, e-Security Bulletin, etc.)
-  <http://www.ncb.mu/>

ICTA

-  ICT Laws
-  <https://www.icta.mu>