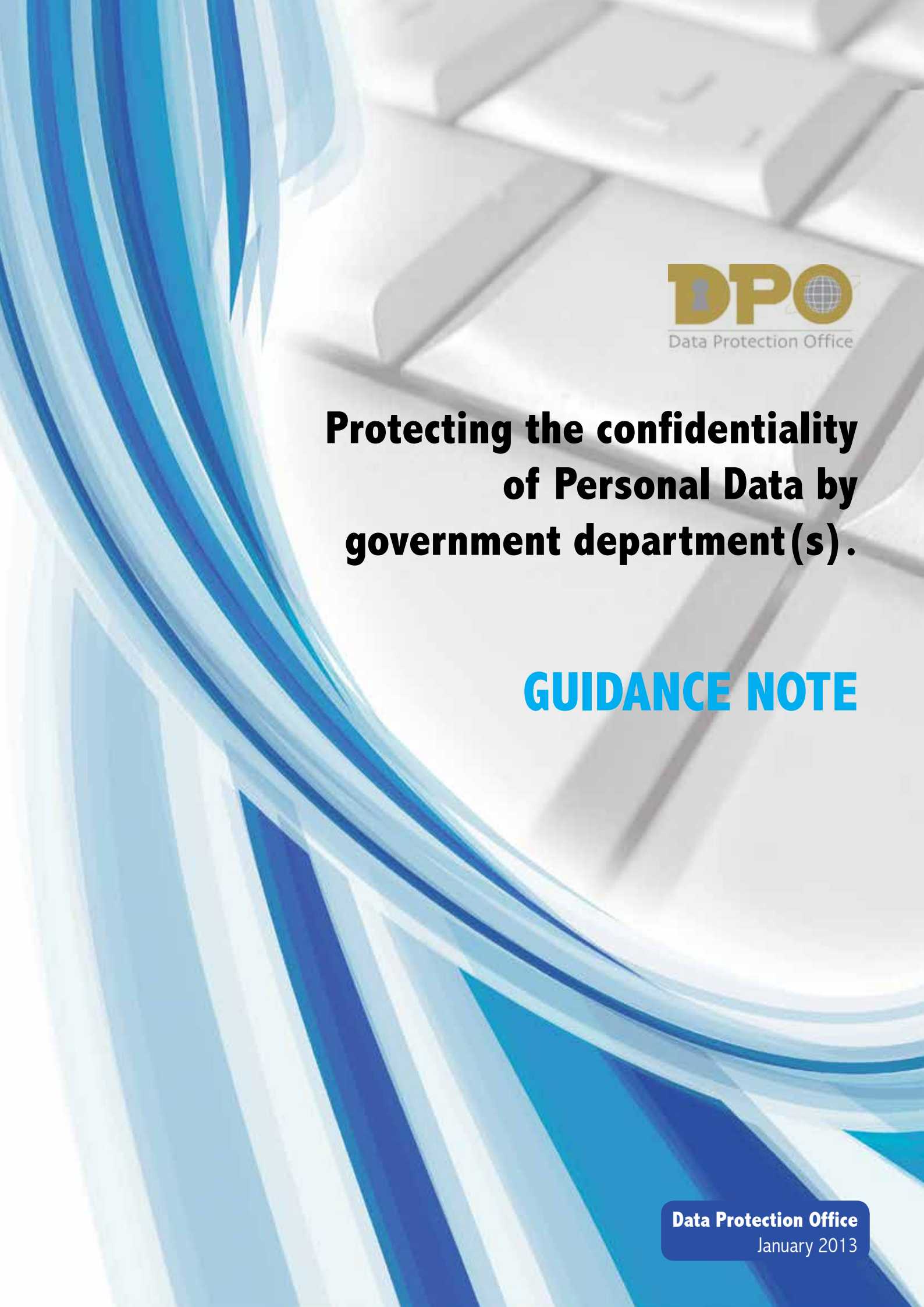

Protecting the confidentiality of Personal Data by government department(s).

GUIDANCE NOTE

Data Protection Office
January 2013

Contents

Introduction

Under the Data Protection Act, Government Departments, Offices and Agencies, as data controllers, have a legal responsibility to:-

- obtain and process personal data fairly;
- keep it only for one or more specified and explicit lawful purposes;
- process it only in ways compatible with the purposes for which it was given initially;
- keep personal data safe and secure;
- keep data accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes and,
- provide a copy of personal data to a data subject, on his/her request.

The purpose of this guide is to assist Departments, Offices and Agencies in implementing systems and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help them meet their legal responsibilities as set out above.This document can be expanded upon by Departments to create detailed policies and procedures which reflect their specific business requirements.

Any queries in relation to the content of this document should be forwarded via email to pmo-dpo@mail.gov.mu.

* A **data controller** is a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed.

* A **Data processor** is a person other than an employee of the data controller, who processes the personal data on behalf of the data controller under a written contract. The data processor must act only on instructions received from the data controller.

Scope

This document provides guidelines on how personal data is to be stored, handled and protected under the following headings:-

a. General Procedures;
b. Paper Records;
c. Email and Personal Productivity Software;
d. Electronic Remote Access;
e. Laptops/Notebooks;
f. Mobile Storage Devices;
g. Data Transfers;
h. Inappropriate Access/Audit Trail Monitoring;
i. Breach Management.

Audience

The information contained in this document is intended for general distribution.

However, it is especially important that senior management in Departments are aware of the contents of the document as the responsibility rests with them to ensure that the guidelines contained in it are followed. The guidelines should also be brought to the attention of all staff whose work involves the handling of personal data.

General Procedures

This document also sets out the guidelines in a number of specific areas where particular attention should be paid in order to help protect the confidentiality of personal data held in a Department. There are, however, a number of general procedures which Departments should follow:-

1. The first stage in establishing policies and procedures to ensure the protection of personal data is to know what data is held, where it is held and what the consequences would be should that data be lost or stolen. With that in mind, as a first step, Departments should conduct an audit identifying the types of personal data held within the organisation, identifying and listing all information repositories holding personal data and their location. Risks associated with the storage, handling and protection of this data should be included in the Department's risk register. Departments can then establish whether the security measures in place are appropriate and proportionate to the data being held while also taking on board the guidelines available in this document;

2. Access to all data centres and server rooms used to host hardware and software on which personal data is stored should be restricted only to those staff members that have clearance to work there. This should, where possible, entail swipe card and/or PIN technology to the room(s) in question – such a system should record when, where and by whom the room was accessed. These access records and procedures should be reviewed by management regularly;

3. Access to systems which are no longer in active use and which contain personal data should be removed where such access is no longer necessary or cannot be justified;

4. Passwords used to access PCs, applications, databases, etc. should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters.If possible, password length should be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Departments must also ensure that passwords are changed on a regular basis;

5. Departments should have procedures in place to properly evaluate requests from other organisations for access to personal data in its possession.Such procedures should assist Departments in assessing whether the release of personal data is fully justifiable under the Data Protection Act. Departments should also ensure that access by staff of personal data for analysis or research purposes is fully justifiable and proportionate;

6. Personnel who retire, transfer from the Department, resign etc. should be removed immediately from mailing lists and access control lists. Relevant changes should also occur when staff are transferred to other assignments internally. It is the responsibility of Departments to ensure that procedures are in place to support this, i.e. so that notification is provided to the relevant individual(s)/Unit in a timely fashion;

7. Contractors, consultants and external service providers employed by Departments should be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Act. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance;

8. Departments should have in place an up-to-date *Acceptable Usage Policy* in relation to the use of Information and Communications Technology (e.g. telephone, mobile phone, fax, email, internet, intranet and remote access, etc.) by its staff. This policy should be understood and signed by each user of such technology in the Department;

9. Internal Control Units(ICUs), should ensure that their programme contains adequate coverage of areas within their organisations which are responsible for the storage, handling and protection of personal data.The particular focus of any review by ICUs would be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any breach of data protection laws. Risks associated with the storage, handling and protection of personal data should be included in the Department's risk register and risk assessments should take place as part of a Department's risk strategy exercise. Regular monitoring should be done;

10. Procedures should be put in place in relation to disposal of files (both paper and electronic) containing personal data. In doing so, Departments should be aware of their legal obligations as set out in various legislations. Procedures should also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life.This could include the use of degaussers, erasers and physical destruction devices, etc;

11. Quality Customer Service documentation/customer charters should detail how customers' data are held and how they will be used/not used. Website privacy statements should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data;

12. New staff should be carefully coached and trained before being allowed to access confidential or personal files;

13. Staff should ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information whether held on paper documents or information displayed on PC monitors, etc.;

14. All staff should ensure that PCs are logged off or 'locked' when left unattended for any period of time (e.g. in Windows, using Ctrl+Alt+Del keys). Where possible, staff should be restricted from saving files to the local disk. Users should be instructed to only save files to their allocated network drive;

15. Personal and sensitive information should be locked away when not in use or at end of day;

16. Appropriate filing procedures (both paper and electronic) should be drawn up and followed;

17. All Data controllers must be registered with the Office of the Data Protection Commissioner.

Paper Records

The Data Protection Act apply equally to personal data held on ICT systems and on paper files. The following guidelines should be followed with regard to personal and sensitive data held on paper files:-

1. Paper records and files containing personal data should be handled in such a way as to restrict access only to those persons with business reasons to access them;

2. This should entail the operation of a policy whereby paper files containing such data are locked away when not required;

3. Consideration should also be given to logging access to paper files containing such data and information items;

4. Personal and sensitive information held on paper must be kept hidden from callers to offices;

5. Secure disposal of confidential waste should be in place and properly used. If third parties are employed to carry out such disposal, they must contractually agree to the Department's data protection procedures and ensure that the confidentiality of all personal data is protected. Such contracts should contain clauses similar to those outlined in the section on 'Data Transfers' below;

6. When paper files are transferred within a Department, this usually entails hand delivery. However, it should be noted that, in many cases, internal post in Departments ultimately feeds into the general postal system (this is particularly true for Departments with disparate locations). In these instances, senders must consider registered mail or guaranteed parcel post service where appropriate. Procedures must be in place for ensuring that the data is delivered only to the person to whom it is addressed, or another officer clearly acting on their behalf, and not any other staff member. Consideration should also be given to the security of manual files when in transit internally;

7. Facsimile technology (fax machines) should not be used for transmitting documents containing sensitive personal data, unless adequate care has been taken to ensure the confidentiality of the documents.

Email and Personal Productivity Software

Email and other personal productivity software such as word processing applications, spreadsheets, etc. are valuable business tools which are in use across every Department. However, Departments must take extreme care in using this software where personal and sensitive data is concerned. In particular:-

1. Standard unencrypted email should never be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent.The strongest encryption methods available should be used. Departments should also ensure that such email is sent only to the intended recipient.In order to ensure interoperability and to avoid significant key management costs, particular attention should be paid to any central solutions put in place for this purpose;

2. Departments should consider implementing solutions that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission;

3. Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls should be considered that would prevent such data from being copied to a personal productivity software (such as word processing applications, spreadsheets, etc.) where no security or access controls are in place and/or can be bypassed.

Remote Access

There is an increasing business requirement for mobile working and e-working across the public service. Consequently, the demand from staff to access remotely the same systems that they can access from the office is increasing.This brings its own challenges in relation to data security which Departments must address. With regard to personal and sensitive data, the following guidelines should be adhered to:-

1. In the first instance, all personal and sensitive data held electronically should be stored centrally (e.g. in a data centre or in a Department's secure server room with documented security in place). Data that is readily available via remote access should not be copied to client PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost;

2. When accessing this data remotely, it must be done via a secure encrypted link (e.g. IPSEC or SSL VPN tunnel) with relevant access controls in place;

3. Additional stringent security and access controls should be in place, e.g. the mandatory use of strong passwords and security token authentication (i.e. two-factor authentication);

4. Data being accessed in this way should be prevented from being copied from the central location to the remote machine;

5. Departments must utilise technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system;

6. Departments should ensure that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately to the Department's standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.), are allowed to remotely access centrally held personal or sensitive data. The strongest encryption methods available should be used to encrypt data on these machines. In addition, 'strong' passwords/passphrases (see 'General Procedures') must be used to protect access to these machines and to encrypt/decrypt the data held on them;

7. Staff should be aware that it is imperative that any wireless technologies/networks used when accessing the Department's systems should be encrypted to the strongest standard available.

Laptops and Other Mobile Storage Devices (incl. Mobile Phones, PDAs, USB memory sticks, External Hard Drives, etc.)

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications and storage devices such as mobile phones, PDAs, etc. has also increased. These devices are useful tools to meet the business needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations should be followed:

1. All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device;

2. Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full disk encryption must be employed regardless of the type of data stored;

3. With regard to mobile technologies, staff should be aware that when 'roaming' abroad, communications may not be as secure as they would be within Mauritius;

4. Data held on portable devices should be backed up regularly to the Department's servers;

5. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons;

6. Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through a Department's IT Unit;

7. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software;

8. Departments should ensure that when providing portable devices for use by staff members, each device is authorised for use by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual;

9. Laptops must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times;

10. Portable devices should never be left in an unattended vehicle;

11. Portable storage media should only be used for data transfer where there is a business requirement to do so, should only be used on approved workstations and must be encrypted;

12. In order to minimise incidents of unauthorised access and/or incidents of lost/stolen data, Departments should restrict the use of personal storage media and devices (e.g. floppy disks, CDs, DVDs, USB memory sticks, etc.) to staff that require to use these media/ devices for business purposes;

13. Only storage media provided by a Department's IT Unit should be permitted for use with that Department's computer equipment. Departments must put in place solutions which only allow officially sanctioned media to be used on a Department's computer equipment (i.e. on networks, USB ports, etc.);

14. Staff owned devices such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc. must be technologically restricted from connecting to Department computers;

15. Departments should consider implementing additional log-in controls on portable devices such as laptops;

16. Departments should implement technologies that will allow the remote deletion of personal data from portable devices (such as mobile phones and PDAs) should such devices be lost or stolen. A procedure for early notification of such loss should be put in place. This would allow for the disconnection of the missing device from a Department's email, calendar and file systems;

17. Departments should implement procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required (e.g. through fully formatting the devices' hard drive);

Data Transfers

Data Transfers are a daily business requirement for most, if not all, Government Departments. With regard to personal and sensitive data, such transfers should take place only where absolutely necessary, using the most secure channel available. To support this, Departments should adhere to the following:-

1. Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. Where this is not possible or appropriate, the safety of the data should be ensured before, during and after transit;

2. Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should end where possible;

3. In the meantime, where data is copied to removable media for transportation, such data must be encrypted using the strongest possible encryption method available.

4. Any such encrypted media should wherever possible be accompanied by a member of the Department's staff, be delivered directly to, and be signed for by, the intended recipient. If this is not possible, the use of registered post or another certifiable delivery method may be used if an agreement similar to that outlined in 7. below has been put in place;

5. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person;

6. Standard email should never be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent. Staff should ensure that such mail is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention should be paid to any central solutions put in place for this purpose;

7. When a data transfer with a third party is required (including to/from other Government Departments), a written agreement should be put in place between both parties in advance of any data transfer. Such an agreement should define:-

- The information that is required by the third party (the purposes for which the information can be used should also be defined if the recipient party is carrying out processing on behalf of the organisation);
- Named contacts in each organisation responsible for the data;
- The frequency of the proposed transfers;
- An explanation of the requirement for the information/data transfer;
- The transfer method that will be used (e.g. Secure FTP, Secure email, etc.);
- The encryption method that will be used;
- The acknowledgement procedures on receipt of the data;
- The length of time the information will be retained by the third party;
- Confirmation from the third party that the information will be handled to the same level of controls that the Department apply to that category of information;
- Confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);
- The method of secure disposal of the transfer media and the timeline for disposal;
- The method for highlighting breaches in the transfer process;
- For data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;
- Business procedures need to be in place to ensure that all such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;
- Particular attention should be focussed on data made available to third party data processors under contract for testing purposes. Live data should not be used for this purpose.

Appropriate Access and Audit Trail Monitoring

All organisations have an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction" in compliance with section 27 of Data Protection Act. It is imperative, therefore, that Departments have security in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data. In addition to this general requirement, the following guidelines should be followed:-

1. Departments should ensure that their ICT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats;

2. In order to capture instances of inappropriate access (whether internal or external), addition, deletion, reading and editing of data, audit trails should be used where technically possible. In situations where systems containing personal data do not currently record 'view' or 'read' access, it should be investigated, as a matter of urgency whether such

functionality can be enabled. In carrying out such an investigation, Departments should take into account whether there would be any effect on system performance that may hinder the ability of the Department to conduct its business. If the functionality cannot be enabled and the risk of inappropriate access is sufficiently high, such systems should be scheduled for removal from use and replaced by systems with appropriate auditing functionality;

3. Access to files containing personal data should be monitored by supervisors on an ongoing basis. Staff should be made aware that this is being done. IT systems may need to be put in place to support this supervision.

Breach Management

A data security breach can happen for a number of reasons, including:-

- Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a flood or fire;
- A hacking attack;
- Access where information is obtained by deceiving the organisation that holds it.

It is important that departments put into place a breach management plan to follow, should such an incident occur. There are five elements to any breach management plan:-

1. **Identification and Classification**
2. **Containment and Recovery**
3. **Risk Assessment**
4. **Notification of Breach**
5. **Evaluation and Response**

1. Identification and Classification

Departments must put in place procedures that will allow any staff member to report an information security incident. It is important that all staff are aware to whom they should report such an incident. Having such a procedure in place will allow for early recognition of the incident so that it can be dealt with in the most appropriate manner. Details of the incident should be recorded accurately, including the date and time the incident occurred, the date and time it was detected, who/what reported the incident, description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff need to be made fully aware as to what constitutes a breach.

2. Containment and Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures. If a breach occurs, Departments should:-

- decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation;
- establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.;
- establish whether there is anything that can be done to recover losses and limit the damage the breach can cause;
- where appropriate, inform the Police.

3. Risk Assessment

In assessing the risk arising from a data security breach, Departments should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Departments should consider the following points:-

- what type of data is involved?;
- how sensitive is it?;
- are there any protections in place (e.g. encryption)?;
- what could the data tell a third party about the individual?;
- how many individuals' personal data are affected by the breach?;

4. Notification of Breach

Although there is no current explicit legal obligation to notify individuals or other bodies under the Data Protection Act of a breach, the Data Protection Commissioner's Office encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/ loss of personal data occurs, it should be reported immediately, both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is. In this regard, Departments should be aware of the dangers of 'over notifying'. Not every incident will warrant notification. For example, notifying a whole 200,000 strong customer base of an issue affecting only 2,000 customers may cause disproportionate enquiries and work.

When notifying individuals, Departments should consider using the most appropriate medium to do so. They should also bear in mind the security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of the situation. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the Department is willing to do to assist them. Departments should also provide a way in which individuals can make contact for further information, e.g. a helpline number, webpage, etc.

Departments should consider notifying third parties such as the police, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

5. Evaluation and Response

Subsequent to any information security breach, a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter.

Each Department should identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

Designed and Printed by the Government Printing Department - May 2013