ARE YOU READY FOR DATA PROTECTION?

The Data Protection (Privacy of Personal Information) Act 2003 (DPA) came into force on 2nd April, 2007 and the Office of the Data Protection Commissioner (ODPC) is fully operational. The Data Protection Commissioner is on a campaign to educate the public on some of the important steps you need to take to comply with the Data Protection obligations.

Section 8 of the DPA deals with the right of access to personal information. It is the most important right that an individual has, and organizations need to make preparations for handling access requests. However, dealing with access requests is not your only obligation. Your staff should be made aware of the obligations imposed by the DPA.

Specifically, 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 awareness, so that data protection is a "living" process aligned to the way the organization 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, including the Police and other enforcement agencies.

Staff should be aware that from 2nd April 2008, Data Controllers are obliged to respond to legitimate access requests in accordance with the DPA.

Note that there are certain exceptions to the right of access including:-

- Information kept for law enforcement and personal security purposes; statistical and/or research purposes;
- Information kept in the interest of national security and protecting international relations.

See Section 9 of the DPA for full details in this regard.

Obligations on retention and security need to be addressed

You need to:-

- 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;

- Ensure that you have retention policies for the various categories of data.

The organization should provide for:-

- Periodic audit checks and reviews;
- A procedure for complaints handling;
- Plans for remedial steps if things go wrong;
- Privacy/Data Protection Statements on Forms and Websites and an internal e-mail and internet use policy.

Dealing with Subject Access Requests

As stated above 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 8 of the DPA. The time limit for complying with an access request is 40 days. In order to ensure your compliance with the time limit and your other access obligations the following organizational and procedural steps are recommended:

1. Appoint a Co-ordinator 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 organization and staff should be advised of the necessity for co-operation with the Co-ordinator.
2. All subject access matters should be submitted to the Co-ordinator.
3. Check the validity of the access request. Ensure that it is in writing.
4. Check that sufficient information has been supplied to definitively identify the individual. This is most important. You should set down criteria on what is sufficient to prove identity for your organization. This may be the signature, an ID number in combination with name and address or date of birth. It should not be possible for a third party to provide the material to lodge a false access request.
5. 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 organization.
6. Log the date of receipt of the valid request.

7. Keep note of all steps taken to locate and collate data – if different departments of the organization are involved, have the steps "signed off"by the appropriate person.
8. If data relating to a third party is involved, do not disclose without the consent of the third party or anonymise such data if this would conceal the identityof the third party. 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.
9. Monitor process of responding to the request – observing time limit of 40 days.

10. 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.
11. Regularly review your procedures and processes.
12. If in doubt, feel free to contact us using e-mail dataprotection@bahamas.gov.bs