DATA PROTECTION CHECKLIST

Data Controllers have several legal responsibilities under the Data Protection (Privacy of Personal Information) Act 2003 (DPA). To meet these responsibilities the issues involved have to be specifically examined in a structural manner and the result of that examination converted into a clear policy position on how they handle data protection.

The below checklist may be used to assist Data Controllers in carrying out an appropriate examination of their responsibilities. It should also help you to formulate a policy statement on data protection for your organization.

A “YES” answer to all of the following questions would suggest that your organization is in good shape from a data protection viewpoint. If you don’t have a clean sheet, the checklist can help you identify areas where you need to improve.

<u>Main Responsibilities</u>

Rule 1: Collect data by means which are lawful and fair.

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people’s consent for any secondary uses of their personal data, which might not be obvious to them?
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: The data must be accurate and up-to-date (except in the case of back-up-data).

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure databases are kept up-to-date?

Rule 3: The data shall be kept only for one or more specified and lawful purpose.

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?

Rule 4: The data shall not be used or disclosed in any manner incompatible with that purpose or purposes.

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.

Rule 5. The data shall be kept accurate, relevant and not excessive in relation to that purpose or those purposes.

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 6: The data shall not be kept for longer than is necessary (except in the case of personal data kept for historical, statistical, or research purposes).

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 7: Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorized people?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the DPA requirements?

Training & Education

- Do we know about the level of awareness of data protection in our organization?
- Is our staff aware of their data protection responsibilities – including the need for confidentiality?
- Is data protection included as part of the training Programme for our staff?

Co-ordination and Compliance

- Has a data protection co-coordinator and compliance person been appointed?
- Is all staff aware of his or her role?
- Are there mechanisms in place for formal review by the co-coordinator of data protection activities within our organization?

For more information, please refer to our “Resource Center” note ***“Are you ready for Data Protection.”***

If you require any assistance, the Data Protection Commissioner will be happy to help. E-mail: dataprotection@bahamas.gov.bs