Information Security and the Data Protection Bill

1. The Cayman Islands' Data Protection Bill, which is currently the subject of a public consultation at www.dataprotection.ky/, seeks to protect an individual's rights with respect to the collection, use and sharing of his or her personal data (i.e. information about the individual). It sets out certain defined 'data protection principles' that you will have to follow.

2. This note offers an overview of what the Bill requires of businesses in terms of securing that personal information. It is intended to give you a general idea how the Bill might impact your business, whether you run a bank or you work for yourself.

3. You should be aware that the Bill may be subject to change before it becomes law and the observations made in this note are in relation to the Bill as currently drafted.

4. Before dealing with the specifics, let's address an important preliminary question, namely……..

Why should I worry about the Data Protection Bill at all?

5. **So you can meet your client's expectations**

   Customers and clients, whether here in Cayman or overseas, will expect you to manage their personal information properly. They will often want you to demonstrate that you are already complying with the provisions in the Bill before they will consider doing business with you or entrust you with their personal information.

6. **Because compliance with the law can enhance your reputation**

   Rather than seeing data protection as an onerous obligation that you 'have to comply with', it is an opportunity to show your customers and clients that you take the protection of their personal information seriously. In many areas of commerce, gaining a reputation for having robust and effective data protection procedures can give you a competitive advantage over your rivals.

7. **Because proper data management improves business efficiency**

   Many of the data protection principles in the Bill are simply about applying good information management practices, which you probably do anyway. All businesses need high quality and accurate information on which to make informed decisions and following the principles set out in the Bill can help your business achieve that. Even something as simple as having an up to date email address and phone number for your clients can make your operations run smoother and more efficiently.

8. **So you don't break the law!**

   The Information Commissioner has various powers under the Bill and can levy enforcement notices and fines for any breaches.

What the Bill says about Information Security

9. The Data Protection Bill places an obligation on you to have "**appropriate technical and organisational measures**" in place to prevent "**unauthorised or unlawful processing of, accidental loss of destruction of, or damage to**" personal information.

10. What does this mean for you? The Bill does not give specific instructions on how to comply with this provision (some suggestions are given later in this note) but it does give some guidance on how to determine what is **"appropriate"**.

11. Firstly, the measures you implement must be appropriate to the harm that might result from a breach and the nature of the personal information to be protected. In determining the measures to implement you can have regard to the **"state of technological development"** and the **"cost of implementing"** them.

12. The Bill also expects you to be accountable for the **"reliability"** of those employees that have access to personal information. That means you should undertake proper background checks on employees especially those who will be managing particularly sensitive personal information.

13. Finally, the provisions in the Bill place an ongoing obligation on you to ensure that your employees are properly trained to understand and apply the data protection principles.

Where do I begin?

14. Before you can establish what level of security is right for your business, you will need to review the personal information you hold and assess the risks to that information. You should consider all the processes involved as you collect, store, use and dispose of personal information.

15. You should consider how valuable, sensitive or confidential the personal information is and what damage or distress could be caused to individuals if there was a security breach (e.g. if the personal information you have was lost or stolen). With a clear view of the risks you can begin to choose the security measures that are appropriate for your needs.

> It is important to note that what is "appropriate" for a large multi-national company with large databases of personal data will be different to what is "appropriate" for a small business or a sole trader, like for example a plumber.

16. If you run one of the many small businesses that outsource some or all of your IT requirements then you should be satisfied that they are treating your data at least with the same level of security as you do. Practical steps you can take include:

    - Asking your IT contractor for a security audit of the systems containing your data,

      Review the contracts you have in place and make sure that they place obligations on your IT contractor to comply with the provisions set out in the Bill.

What sort of security measures should I deploy?

17. Unfortunately there is no one magic product that will provide you with 100% guaranteed security. The key is therefore to have a layered approach that fits in with your business set-up. A possible approach is where you combine several different tools and techniques to give you the best possible level of protection. If one of these layers fails to work the other layers will still be in place to counter the threat.

18. The Bill does not require you to have state-of-the-art security technology to protect the personal information you hold, but it does require you to consider the **"state of technological development"** and you should regularly review the security products you use and compare them with new technologies as they become available.

Technical Measures

Here are some suggestions of technical and organisational measures that you should consider, as recommended by the UK Information Commissioner's office:

Computer security

- Install a firewall and virus-checking on your computers.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow your staff access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. (Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer.)

Emails

- Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Faxes

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

Organisational

- Shred all your confidential paper waste.
- Check the physical security of your premises.
- Train your staff:
    - so they know what is expected of them;

- to be wary of people who may try to trick them into giving out personal details;
- so that they can be prosecuted if they deliberately give out personal details without permission;
- to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
- not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

Reporting a breach

19. If, despite the security measures you take to protect the personal information you hold, a breach of security occurs, you will have to report this to the Information Commissioner's Office and also to the individual concerned if the breach adversely affects their personal data or privacy, "**without undue delay**".

20. As drafted the Bill obliges you to report **any** personal data breach which is defined as…

    "***….a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by, or on behalf of, a data controller;***"

21. The breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. However the breach occurs, you must respond to and manage the incident appropriately. You will need a strategy for dealing with the breach, including:

    - a recovery plan, including damage limitation;
    - assessing the risks associated with the breach;
    - informing the appropriate people and organisations that the breach has occurred; and
    - reviewing your response and updating your information security.

Steve Smith
IT Risk Manager
Walkers
01.10.12