Tip of the Month - November, 2011

Six Things that make Privacy work

Data Protection (Privacy of Personal Information) requires six basic elements to make it work effectively in our community. Briefly, these are noted below:-

1. **Involvement of the Community**

   Reaching out to the community through Public Service Announcements (PSAs), Town Meetings and other forms of awareness campaigns is vital. We have already participated in forms of the above and intend to increase activity in this area, within our limited resources.

   The public must also develop a sense of trust when considering how their personal information is handled.

2. **Privacy by Design**

   It is important that privacy protections are built into everything we do rather than treated as an afterthought. Privacy should be BUILT IN not BOLTED ON! This suggests that Privacy Impact Assessments (PIAs) should be undertaken when projects are likely to impact on privacy.

   A PIA is an assessment tool that describes in detail the personal information flows in a project and analyses its possible privacy impacts. A PIA can help agencies to identify when the collection of particular information is unnecessary for a given project or where additional accountability or oversight process may reduce privacy tasks.

   PIAs are becoming the norm now for new projects that involve the handling of personal information and they are an accepted assessment tool in many countries across the world. They also help to gain community trust and confidence in new proposals.

3. Choice and Control

Always allow your clients to exercise choice and control over the way their information is handled. They should be able to decide whether or not their information will be shared between service providers for their convenience, (Such things like Medical Records and/or other vital government records).

4. Maintaining Database Integrity and Compliance

There is no point offering customers the ability to control the way you handle their personal information if you cannot provide adequate security and information management. Databases containing personal information collected for different programs need to maintain some form of separation. This is sometimes referred to as "siloing." Each service provider maintains its own self contained, independent database, or "Silo" of information, over which it has control. In this silo will be all the information that it collects in the course of delivering its service to the public.

Under the DPA agencies/organizations must comply with all the principles of data protection.

5. Take extra care with Sensitive Information

The DPA incorporates a subset of personal information known as "sensitive Information." Sensitive information includes information about an individual's health, social or ethnic origin, religious beliefs, sexual preference or practices, trade union involvement or activities and criminal record. Consequently, agencies need to be particularly careful when handling sensitive information. In addition agencies should consider giving individuals a greater capacity to exercise control over the way their sensitive information is handled.

6. **Leverage Expertise**

The key is to maximize the many benefits of "doing privacy well" when delivering a service where personal information is involved. Best practices both at home and abroad should put us in good standing.

Remember "Privacy is the Best Policy."

Feel free to contact us at dataprotection@bahamas.gov.bs our visit our website www.bahamas.gov.bs/dataprotection to learn more about our mandate to protect the privacy rights of individuals.