Building Websites

It is increasingly essential for organisations to have a website as part of their sales, marketing and customer relationship management efforts. If your organisation's website is used to collect or store personal data such as customer and payment details, then it should be aware of the obligations under the Personal Data Protection Act (PDPA).

Key Considerations

When setting up a website for your organisation, do consider the following:

- Features and functions of the website, especially those functions that collect and handle personal data (e.g. online ordering portal, membership management, online forums);
- Amount and type of personal data that will be collected or used;
- Extent of security required;
- Location where the website will be hosted; and
- Resiliency of the website.

As websites are connected via the Internet, they face a multitude of cyber threats. Poorly protected websites can be compromised easily, putting any personal data that they collect or store at risk. Data breaches can be costly as this may lead to financial loss and loss of consumers' trust in your organisation.

Hence, the security of the website and the protection of the personal data should be a key design consideration at each stage of the website's life cycle:

Where data protection is not considered until the development of the website has been completed, making changes to the website at that later stage will incur additional cost, including cost to resolve any security breaches.

Security

Policies and Processes

Put in place policies and processes to protect the personal data handled by your organisation's website. Suggested policies and processes include:

- Use of risk assessments to select the most appropriate security arrangements
- Secure configuration of hardware and software components
- Security testing before the website is launched, and regular security testing thereafter
- Keeping track of the storage of all personal data
- Incident management

Design

Include security as an important requirement when designing the website. Some key security requirements include:

- Access Control
- Audit Log
- Server and Network Security
- Website Programming

Negotiating Responsibilities of IT Vendors

Your organisation may consider outsourcing the development and maintenance of the website if it does not have the technical resources to do so by engaging one or more IT vendors.

When engaging IT vendors, do emphasise the need for personal data protection by stating clearly the responsibilities of the IT vendor with respect to the PDPA. These responsibilities will depend on the IT vendors' scope of work. For instance:

- Developing the website in a way that ensures that it does not contain any web application vulnerabilities; and
- Ensuring that the servers and networks are securely configured.

Additionally, your organisation should require that the IT vendors prevent unauthorised disclosure of personal data by their personnel or sub-contractors. Consider the following:

- Put in place processes for the secure handling of personal data; and
- Require confidentiality agreements between your organisation and all IT vendor personnel and sub-contractors who have access to the personal data.

For more information, please refer to the Guide on Building Websites for SMEs and the Guide to Securing Personal Data in Electronic Medium, which can be found on the PDPC website at www.pdpc.gov.sg.

BROUGHT TO YOU BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

IN PARTNERSHIP WITH

CSA SINGAPORE