BIZCOMMUNITY

Practical solutions to help you gear up for PoPI

By Simeon Tassev

29 Jul 2015

The Protection of Personal Information (PoPI) Act is currently a hot topic, given the imminent nature of its implementation. Since the penalties for contravention of the Act can be severe, many organisations are beginning to prepare themselves for compliance.

However, while companies are aware that non-compliance can have disastrous consequences, many are not fully cognisant of the benefits to their organisation that compliance can bring, including improved security, increased customer confidence and improved reliability of databases. Information management tools are an essential foundation for compliance. Implementing practical solutions for the storage of data, particularly email, can take organisations a long way on their journey toward applying PoPI legislation effectively within their business.

Severe penalties for not being PoPI compliant

Stuart Miles via freedigitalphotos.net

PoPI seeks to regulate the processing of personal information, which is defined as any information relating to an identifiable, living natural or juristic person. This includes, but is not limited to, contact details, demographic information, history, biometric information, and opinions of and about a person as private correspondence. Once PoPI comes into effect, organisations will have a year's grace period (which may be extended up to a maximum of three years) in order to become compliant. The potential penalties for non-compliance include fines of up to R10 million, and/or imprisonment of up to 12 months. In extreme cases, the penalty for non-compliance could include imprisonment of up 10 years.

Since the directors of a business are held accountable for compliance, they are also the ones who will face jail time should they contravene the Act. However, as onerous as these penalties are, the most significant impact on business is reputational damage and its on-going negative effects. Any consumer can report a business if they believe that a breach occurred, upon which the information regulator will investigate. If a breach occurred and satisfactory measures were not in place to mitigate this risk, penalties will be applied according to the severity of the breach, and the breach will be publicised. Consumers could lose confidence in the organisation, take their business elsewhere and potentially cause the downfall and failure of the enterprise.

Step one

PoPI relates to how all personal information is managed, from the security sign-in book at reception to application forms, correspondence and more. It covers the processing and storing of information, the duration of storage, and the need to inform data subjects that their information is being stored. The first step in the compliance journey is to understand how information is processed within an organisation, and identify which areas of business process personal customer information. Once this is done, information must be classified - which information is confidential to the company, which information contains sensitive consumer data, what information needs to be kept and which information requires customer consent to retain, and so on.

Retention and classification policies

Identifying and classifying data can prove challenging given the multiple different areas of business that customer information potentially touches. It is also essential to have the right systems in place to be able to apply different retention policies based on the classification of the information. Having multiple information processing systems for identification, classification and integration creates difficulties with regard to PoPI, as creating the necessary audit trail becomes a

challenge. It is, therefore, advisable to consolidate these processes into a single platform that is scalable without limitations, in order to meet future growth demand. Retention and classification policies must also be continually reviewed, to ensure they continue to meet evolving business requirements.

Implementing the right systems and controls

While many organisations view PoPI as just another piece of onerous legislature, the reality is that it is designed to protect both the business and its consumers. PoPI forces organisations to more effectively control and maintain their databases to prevent the risk of current and out-dated personal information being exposed. This in turn benefits organisations by ensuring their data is more accurate and up to date, enabling it to be more useful for generating business.

In addition, compliance ensures that organisations focus on how information is stored, processed and accessed, which provides additional security elements and helps to optimise storage by eliminating unnecessary data. Given the acceleration in data generation, and the increased quantity of data processing, implementing the right systems and controls is the only way to manage information effectively.

Compliance with PoPI, therefore, offers a number of business benefits. In addition, by complying with PoPI, organisations can boost customer confidence by guaranteeing that their information will be kept safe and secure and will not be leaked or sold for unauthorised purposes.

Three key areas

PoPI at its heart is all about more efficient, effective and secure management of information, which has many benefits for organisations outside of avoiding significant penalties. PoPI-compliant information management solutions should include the archiving, continuity and security of both structured and unstructured data. This needs to address three key areas, namely data classification, data retention and data privacy. Such solutions provide practical storage, archiving and retention of data to help organisations gear up for PoPI.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...