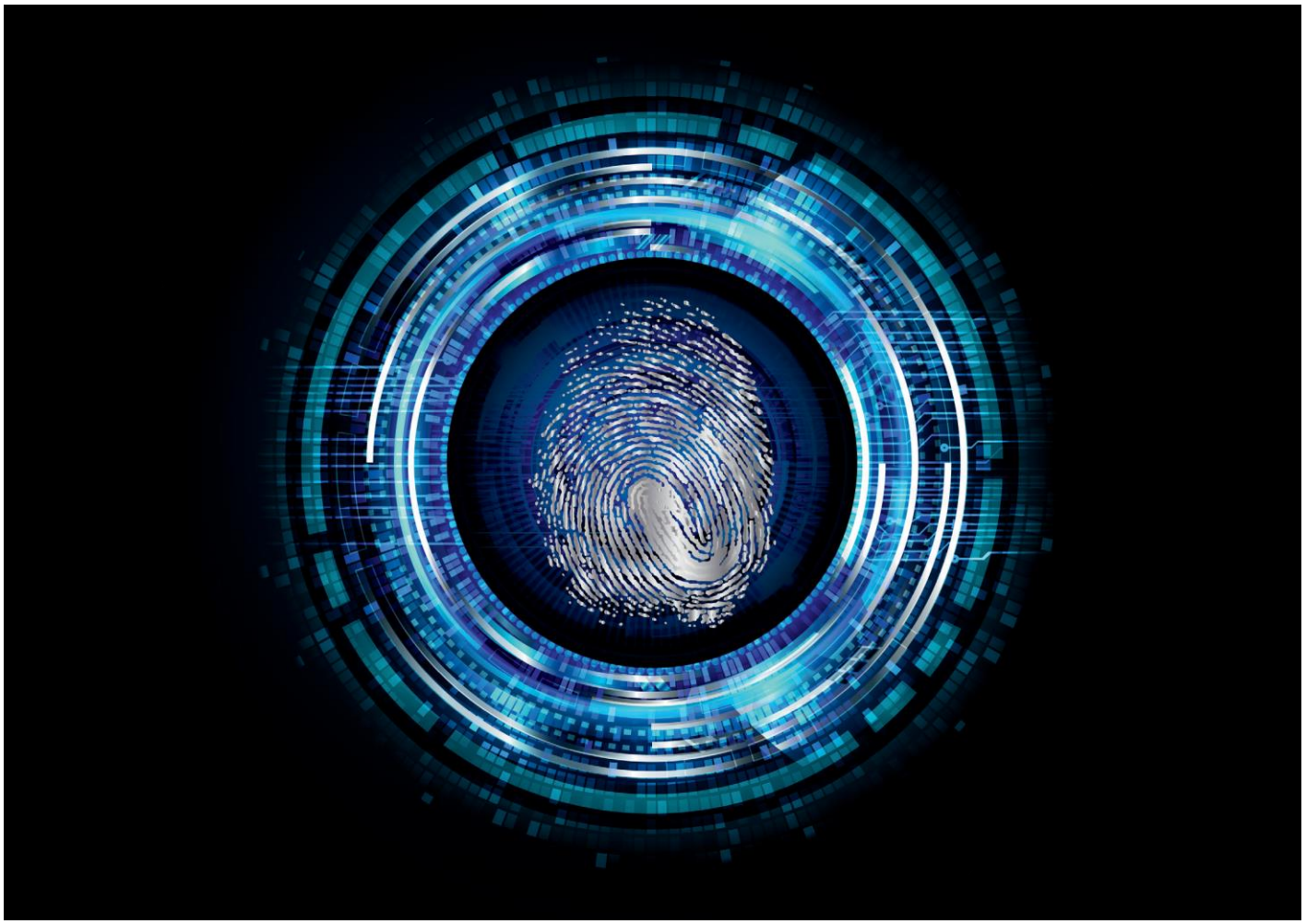

International Privacy Day!

The 28th of January marks the annual global Data Privacy Day event and with this year being of particular importance in the African context with the Protection of Personal Information Act (POPIA) coming into effect on 1 July 2021. We would like to highlight five important privacy areas to focus on in the next 5 months, as we approach the compliance deadline.

1. Third Party Risk Management

An undoubtedly high risk to all organisations, especially those who outsource the processing of personal information to third parties. Perhaps the most important starting block is to prescribe the privacy obligations the third parties are required to adhere to. It is important to expressly highlight the physical security, cyber security, data management and breach notification protocols in such agreement.

The second important component that should be considered, is the ongoing monitoring and assessment against these requirements and the remediation of areas of non-compliance in third party environments. There are several ways in which this can be achieved, including assessments or audits and certain reporting or disclosure requirements by the third party. It is important to ensure that where areas of non-compliance are discovered, remediation plans are created and deployed to track progress against the findings to ensure that the areas of non-compliance are remediated in a timely manner.

2. Incident and breach management

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, POPIA imposes an automatic obligation to notify the Information Regulator. In most instances, save where notification to the affected data subjects would impede a criminal investigation, notification to the affected data subjects is mandatory.

The notification to the Information Regulator and the data subject must contain certain mandatory information, including a description of the possible consequences of the security compromise, the measures taken by the responsible party to address the security compromise and the measures the data subject can take to mitigate the adverse effects of the security compromise.

At the point of notification by the responsible party to the Information Regulator and/or the data subjects, several important consequences are triggered including exposure to legal, reputational and business risks and consequences. As a result, it is important to ensure that an organisation is correctly configured to respond to a material event such as a security compromise.

Part of this configuration is to ensure that a task team is identified and mandated to respond to a security compromise which should consist of the Information Officer, legal representation, reputational management, the cyber security team and any other stakeholder that may be required.

3. Privacy metrics, monitoring and reporting

In order to ensure that an Information Officer can comply with their obligations to monitor compliance by the organisation with the requirements of POPIA, the Information Officer must ensure that it is able to aggregate compliance information from the organisation in respect of several key risks as it relates to privacy. As a result, determining and then defining key risk indicators as they relate to privacy, ensuring that the key risks remain within acceptable manageable levels of risk as determined by the organisation, and regularly providing this information to the relevant stakeholders within the organisation in terms of established reporting protocols and standards, is a key part of the Information Officer's role.

4. Data quality, Data minimization, Data life cycle management, Data governance

POPIA regulates the life-cycle of personal information within an organisation. This means that several key points in the flow of data in an organisation requires measures to be implemented to ensure that it is processed in accordance with POPIA.

However, prior to implementing these measures, one of the fundamental challenges many organisations face is understanding not only the flow of personal information through the organisation, but also essentially where that information resides within the organisation.

As a result, in many instances, a precursor to engaging in data related activities is the commissioning data flow diagrams which explicitly maps the flow of personal information in the context of business processes, people and technology; through a particular business area within an organisation. Once an understanding is gained of where personal information resides and how it is being processed, POPIA requires that specific measures be implemented in respect of collection, storage, retention and destruction to ensure that processing is based on the principles of fairness, transparency and good ethical governance.

5. Information security controls (NIST/ISO)

POPIA introduces a new minimum cyber security standard and posture that must be adopted to ensure that organisations can reasonably protect personal information, and that such protection is appropriate in the circumstances.

POPIA requires organisations to not only have regard to accepted information security practices and procedures which apply to it generally. It also requires the organisation to have due regard to any specific industry or professional rules and regulations that may impose additional requirements. Thus, the expectations of a responsible party may significantly vary depending on the industry or profession to which it belongs.

While traditional cyber security frameworks are a good starting point to determine an organisation frame of reference, it is important to note that the security measures that are required to be implemented in the context of privacy are peculiar and specific. An example of these are the recently published ISO 27 701 and updated NIST privacy control catalogue, both of which have a focus on privacy requirements.

The implementation of privacy projects is as much about compliance as it is about the management of the risk of non-compliance. It is important for organisations to recognise where it will not be able to comply with the provisions of POPIA by the effective date and ensure that the risk of non-compliance is managed appropriately. This should include formally registering the risk within the organisation, having the appropriate visibility and proper acknowledgement of the consequences that arise as a result of the risk of non-compliance. A risk owner should be allocated and a remediation plan implemented to mitigate the impact of non-compliance post the effective date, until the area of non-compliance is remediated and compliance is achieved. The management of the risks associated with non-compliance in this manner or any other should not detract from the fact that the risk area in question may not comply with

POPIA by the effective date, in which event the organisation is technically in breach of POPIA. Importantly though, the ability to demonstrate to an interested party that the risk of non-compliance is being managed reasonably and appropriately, may serve to mitigate any possible consequences that may arise.

Of course, POPIA is not only about compliance, but rather the value that it unlocks for organisations and all of the stakeholders. Seen from the perspective of a value driver, POPIA significantly enhances cyber security, data discipline and quality, efficiency and standardisation, and results in an increased data asset value. These in turn, reduce the impact of potential breaches on businesses and their adverse effects on data subjects, and fundamentally increases business insights through more meaningful data consumption and analytics. Indeed, in the case of POPIA, compliance will undoubtedly delivery value across the business; and perhaps it will deliver it in some of the areas where it is needed most.

Deloitte is ranked no.1 by revenue for 2019 in security consulting services by Gartner, the world's leading information technology and advisory company.

Contact us:

Leishen Pillay
Associate Director
Cyber Risk | Risk Advisory Africa
Tel: +27 (0)11 209 6418
Email: lpillay@deloitte.co.za

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Copyright © 2020 Deloitte Development LLC. All rights reserved. Member of Deloitte Touche Tohmatsu Limited