ENSURING COMPLIANCE TO PRIVACY ACT 1988 AND MANDATORY DATA BREACH REPORTING (PRIVACY AMENDMENT BILL 2016) USING E-SAFE COMPLIANCE

Author: Dr Simon Scott

Published: July 2017

Entities covered by the Australian Privacy Act 1988 have obligations under the Act to take reasonable steps to protect the personal information held from misuse, interference and loss, and from unauthorised access, modification or disclosure. The Privacy Amendment (Notifiable Data Breaches) Bill 2016, establishes a mandatory data breach notification scheme in Australia.

e-Safe Compliance not only facilitates compliance with the Privacy Act, by providing reasonable protection of personal data under the Australian Privacy Principles, but also contains the necessary ISO27001 processes to enable the review and where necessary escalation of incidents on a case-by-case basis as under the recent Privacy Amendment Bill which makes reporting of breaches mandatory.

1 ENSURING COMPLIANCE WITH PRIVACY ACT 1988

The 'Guide to securing personal information' published by the Office of the Australian Information Commissioner provides guidance on the reasonable steps entities are required to take under the Privacy Act 1988 to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. e-Safe Compliance addresses all the following nine areas highlighted within the guide as being central to providing a strong protection against data breaches.

1. Governance, culture and training.
   - e-Safe Compliance implements a People Centric Security (PCS) approach in which end-users are educated through policy and personalized reports on the use of personal data.
2. Internal practices, procedures and systems.
   - e-Safe Compliance implements ISO27001 processes including the necessary separation of roles with respected to data ownership, protection, review and management oversight.
3. ICT security.
   - e-Safe Compliance mitigates the risks of internal / external attackers and human error whilst allowing users to continue work uninterrupted. Functionality includes:
     - Application, device and network blacklisting.
     - Monitoring of the movement of personal information across the network.
     - Monitoring of personal information within communications including emails and Internet Messaging.
     - Monitoring the usage of personal information within applications.
     - Automatic encryption of documents containing personal information, along with provision of applications to allow mobile workers and collaborating organizations to access the personal information where required.
4. Access security.
   - e-Safe Compliance provides access controls on personal data within encrypted documents to ensure only authorised users can access the data.
5. Third party providers including cloud computing.

- e-Safe Compliance tracks the outflow of personal data to cloud applications and websites including Office365, Dropbox, Google Docs, etc. and secures it using encryption

6. Data breaches.
   - e-Safe Compliance provides full visibility of potential data breaches and the necessary workflow to enable further investigation of the same.
7. Physical security.
   - e-Safe Compliance provides full auditing facilities including a Hardware asset audit so that missing devices can be quickly identified.
8. Destruction and de-identification.
   - e-Safe Compliance provides extensive data discovery functionality allowing the organisation to locate personal data stored within the organisation and so facilitate the destruction of the same.
9. Standards.
   - e-Safe Compliance implements the ISO27000 family of processes to ensure all personal data is identified, protected and any potential data breaches are managed in accordance with the standards specified by the Office of the Australian Information Commissioner.

2 ENSURING COMPLIANCE WITH MANDATORY DATA BREACH REPORTING (PRIVACY AMENDMENT BILL 2016)

The 'Guide to developing a data breach response plan', recently released by the Office of the Australian Information Commissioner, divides an ideal plan into the steps listed below. The functionalities and workflow provided by e-Safe Compliance facilitate these steps.

1. Contain the breach and do a preliminary assessment.
   - e-Safe Compliance identifies the users and channels involved in a breach so that further actions of the users can be contained via its data protection functionality, which includes application, device, network blacklisting and data encryption.
   - e-Safe Compliance enables a preliminary assessment to be conducted by specifying the personal information involved as well as the cause and extent of the breach.
   - Where necessary, the e-Safe Compliance enables the breach to be escalated to the relevant internal authorities via reporting workflow functionality. e-Safe Compliance implements ISO27001 processes including the necessary separate of roles with respected to data ownership, protection, review and management oversight.
2. Evaluate the risks associated with the breach.
   - e-Safe Compliance provides the necessary information including the type of personal information involved, the context the information appeared in and the extent of breach.
   - e-Safe Compliance report management workflow functionality enables communication between the internal authorities and those tasked with identifying data breaches and allows further information and related incidents to be gathered together within the same event to facilitate decision making.
3. Notification.
   - The incident reporting functionality provide all the necessary detail required to make a notification to the Office of the Australian Information Commissioner.
4. Prevent future breaches.
   - The outcome of the investigation can be fed back to those administrating e-Safe Compliance to allow the relevant settings to be modified to prevent further breaches.