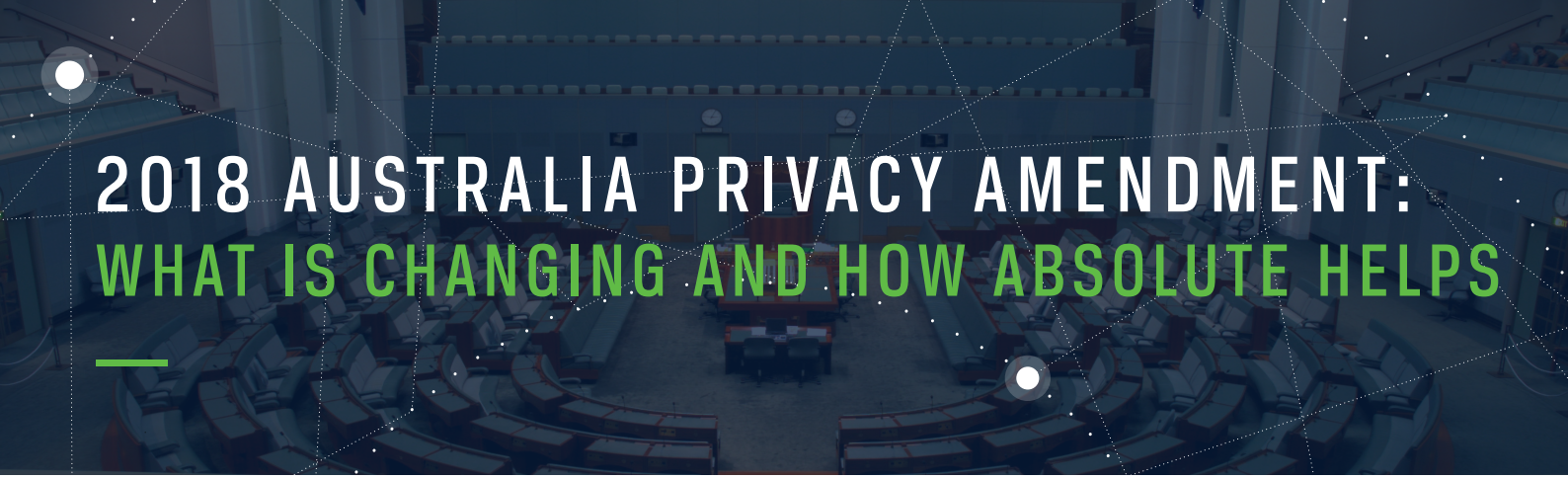

2018 AUSTRALIA PRIVACY AMENDMENT: WHAT IS CHANGING AND HOW ABSOLUTE HELPS

INFOSHEET

We live in a world where the collection and retention of personal information is easier than ever. The explosion of available storage coupled with unprecedented growth in network speeds has made it possible for organisations around the world to provide new services and technologies to citizens and customers that we couldn't have imagined even a decade ago.

But these opportunities are not without risk: cyber criminals the world over are continually hunting for new sources of personal information and data to abscond with and quickly monetise—leaving a huge mess behind for victims to clean up. The double-edged sword is that it can be incredibly difficult to even know what data you have inside your organisation that requires protection, let alone being able to determine if a breach of customer or citizen data has happened. Recent massive data breach events in the US and Europe have made organisations sit up and ask some very hard questions: are we exposed? Could we detect a breach or quickly respond to an incident?

In February 2017 Australia passed the *Privacy Amendment (Notifiable Data Breaches) Bill 2016*, giving a large number of federal government agencies and private/public companies 12 months to achieve compliance. Many Australian organisations are required to comply with the new laws; only small businesses with less than 3 million dollars of turnover, state government agencies, and local councils are exempt from these laws.

The new law includes the requirement for organisations to notify both the Office of the Australian Information Commissioner (OAIC) and those impacted by a data breach, and require organisations who have *reasonable grounds to believe* a breach may have occurred. In this case, an 'eligible' data breach is simply defined:

a.) unauthorised access or disclosure, or loss of information where unauthorised access or disclosure is likely; and

b.) a reasonable person would conclude that the access or disclosure would likely result in serious harm to the individuals to whom the information relates.

Serious harm is not clearly defined, but a list of factors that may demonstrate serious harm are included:

- The sensitivity of the information;
- How the information was protected by the organisation and how easily those protection mechanisms may be defeated;
- Who could have accessed the information;
- The nature of the harm; and
- Any other deemed relevant matters.

No two breaches are identical; obviously each breach or suspected breach will be judged on its own unique factors in determining if a notification is required. It's safe to assume that organisations should review all of their data security policies, procedures, and relevant controls to ensure they can do whatever is possible to minimise the possibility of triggering a breach notification.

However there are some exceptions built into the new laws that can exempt organisations from having to create a notification, most importantly:

- If the impacted organisation takes sufficient remediation steps in response to a breach or suspected breach before serious harm can occur;
- If the data breach or suspected breach involves data that more than one organisation has, only one of the impacted organisations must make the appropriate notifications.

The penalties for lack of compliance can be substantial: a serious incident or failure to comply risk financial penalties as high as $1.8 million for organisations and up to $360,000 for individuals.

HOW CAN ABSOLUTE HELP?

A large number of data breaches involve lost or stolen devices that were not adequately protected from both physical theft and the subsequent data theft from the device. Many organisations—both public and private—continue to struggle with one of the most fundamental cornerstones of information security: IT asset management. Absolute is the only solution to deliver always-connected IT asset management to ensure devices, applications, and data are visible, secure, and compliant—on and off the network. Absolute's technology is embedded in over 1 billion endpoints, protecting more than 15,000 customers worldwide including leading enterprises, educational organisations and government institutions. Absolute leverages its privileged position embedded in the firmware of the device to self-heal in the event of tampering or negligent user activity. This unique connection to the device allows organisations to monitor hundreds of different attributes, including:

- Device name, domain, IP address, username, current hardware specifications, etc.
- At-risk data currently on the device
- Current and historical location of the device
- The ability to monitor and report on the health of third-party applications and tools such as antivirus and encryption suites

If a device is lost or stolen, Absolute can report on the security posture of the device: was encryption enabled and functional? Was the device patched? Were other security applications enabled and functioning? If you can provide affirmative answers to all of these questions, you may be able to exempt yourself from creating a breach notification in the context of the Australian Amendment Bill, saving potentially millions in reputational and financial damages.

Absolute can also provide an additional layer of comfort by remotely deleting sensitive data or the entire device itself. The process not only deletes the data, but can prevent forensic recreation of the data by overwriting the data in a secure manner. Absolute can also provide proof data was not accessed after the incident occurred, important for compliance.

Absolute equips security teams with proactive alerting, designed specifically for the unique needs of the organisation, which can indicate a possible incident has happened, allowing the organization the time it needs to react and mitigate serious harm, potentially alleviating the need to create a breach notification.

It's no easy feat to ensure all of your endpoint devices are visible and in compliant at all times. Absolute can help deliver new levels of endpoint visibility and control in order to assist you in reaching your organisation's new obligations under these new laws.

ALWAYS-CONNECTED IT ASSET MANAGEMENT

EMBEDDED IN › 1 BILLION ENDPOINTS

SELF-HEALING ENDPOINT SECURITY

› 15,000 CUSTOMERS WORLDWIDE