HERBERT SMITH FREEHILLS

BUSINESSES NOW NEED TO REPORT ON THEIR DATA BREACHES

20 February 2018 | Australia
Legal Briefings – By **Shadia Rahman and Natasha Blycha**

From 22 February 2018, as part of their privacy compliance measures, Australian businesses and government agencies will need to be ready to report on their data breaches.

Like the rest of the world, Australian governments and businesses are increasingly collecting data about the people they interact with. This data is often incredibly valuable, as it records the who, what and why of personal and business transactions.

But significant data breaches are also becoming more frequent – and larger in scale. The data breach at Equifax in 2017, described in one report as "the most significant data breach in recent history", exposed the financial information of around 145 million people, leaving them at risk of identity fraud. Australia's largest data breach occurred in October 2016, when private information of more than half a million Australian blood donors – including their medical histories – was accidentally leaked from the Australian Red Cross Blood Service.

Australia's new data breach notification law changes are designed to deal with data breaches like these. These changes will require regulated entities to report eligible data breaches to both the affected individuals and the Office of the Australian Information Commissioner (**OAIC**).

The purpose of these new laws is to improve transparency in the way organisations respond to data breaches – and to give individuals the opportunity to take steps to minimise the harm caused by a breach of their personal information.

WHO MUST COMPLY?

The amendments apply to all entities that are currently subject to the *Privacy Act 1988* (Cth) (**Privacy Act**). This includes private sector organisations with annual revenue of more than $3 million, and Federal government agencies. It also includes some organisations with less than $3 million revenue – for example, health service providers, credit reporting bodies or credit providers, or organisations that trade personal information.

WHAT NOTIFICATION IS REQUIRED?

If a regulated entity develops reasonable grounds to believe that there has been an "eligible data breach", they must prepare a statement to individuals at risk of being affected by that breach. The statement must include:

- the entity's contact details;
- a description of the breach;
- the kinds of information concerned; and
- the steps it recommends individuals take to mitigate the harm that may arise from the breach.

Copies of this statement must be provided to the OAIC. The entity must also take reasonable steps to notify affected or at risk individuals of the contents of the statement. If direct notification is not practicable, the entity must publish the statement on its website and take reasonable steps to publicise its content.

Notification must be provided as soon as practicable.

WHAT BREACHES ARE COVERED?

The new laws only apply to "eligible data breaches" – which means:

- there has been unauthorised access or disclosure of personal information, or a loss of personal information that makes unauthorised access or disclosure likely;
- this is likely to result in **serious harm** to one or more individuals; and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Serious harm could include physical, psychological, emotional, economic, financial and reputational harm. In assessing whether serious harm is likely, the entity needs to consider such matters as the types of personal information affected, the circumstances of the data breach, and the nature of the harm that may result.

If a regulated entity suspects there has been an eligible data breach, it must carry out a reasonable and speedy assessment – usually within 30 days or less. If the suspected eligible breach is confirmed, the notification obligations described above will apply.

REMEDIAL ACTION TO PREVENT HARM

An entity can avoid the requirement for notification if it takes proper remedial action – and that action is such that serious harm is no longer likely to result from the breach. The remedial action required will depend on the type of data breach. For example, if information has been inadvertently disclosed, remedial action could include a full recovery of that information before it has been accessed or used. If the remedial action prevents the likelihood of harm to individuals, then the entity is not required to notify affected individuals or the OAIC.

CONSEQUENCES FOR NON-COMPLIANCE

Depending on how serious or repeated the data breach is, failures to report can give rise to civil penalties of up to $2.1 million.

WHAT SHOULD YOU DO TO PREPARE?

If the Privacy Act applies to your organisation, then you should:

- audit your organisation’s security and privacy processes to ensure your organisation is protected against data breaches;
- review contracts with service providers and others who deal with personal information on your organisation’s behalf, to ensure there are appropriate provisions dealing with data breaches;
- have an action plan ready to deal with data breaches; and
- train your staff to identify when an eligible data breach has occurred, to be familiar with the action plan, and to know what to do if a breach occurs.

Organisations not subject to the Privacy Act may still seek to implement these measures – for example, to meet best practice, protect their brands, comply with contracts and meet other requirements to protect data security.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

TONY JOYNER
LEAD PARTNER – TMT; MANAGING PARTNER, PERTH OFFICE, PERTH
+61 8 9211 7582
Tony.Joyner@hsf.com

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

LEGAL NOTICE