New Privacy Laws – Notifiable Data Breaches

Amendments to the Privacy Act 1988, introducing a notifiable data breach scheme, commence on 22 February 2018.

As from that date, persons and organisations to whom the privacy laws apply, who experience a notifiable data breach, need to notify the person to whom the data relates and the Privacy Commissioner. The notification must set out:

- The organisation's identity and contact details;
- a description of the data breach;
- the kinds of information concerned; and
- recommendations about the steps the person should take in response to the data breach.

There are potentially large civil penalty orders, but apparently only where failure to notify involves a serious or repeated interference with privacy.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure, e.g. when:

- a device containing customers' personal information is lost or stolen;
- a database containing personal information is hacked; or
- personal information is mistakenly provided to the wrong person.

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. Serious harm is not defined in the Privacy Act. There is some commentary on the Privacy Commissioner's website, suggesting a reasonably high bar, including:

In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

In assessing the risk of serious harm, entities should consider the broad range of potential kinds of harms that may follow a data breach. It may be helpful for entities assessing the likelihood of harm to consider a number of scenarios that would result in serious harm and the likelihood of each. Examples may include:

- *identity theft*
- *significant financial loss by the individual*
- *threats to an individual's physical safety*
- *loss of business or employment opportunities*
- *humiliation, damage to reputation or relationships*
- *workplace or social bullying or marginalisation.*

BANNERMANS LAWYERS

T: (02) 9929 0226 M: 0403 738 996 ABN: 61 649 876 437
E: dbannerman@bannermans.com.au W: www.bannermans.com.au
P: PO Box 514 NORTH SYDNEY NSW 2059 AUSTRALIA

Basically, if the privacy laws apply to you and you get hacked or lose a phone or laptop containing personal information, you need to consider whether "serious harm" could result and if so make a notification. Your privacy officer should keep a register of privacy transactions, e.g. requests for access and any issues in this area. On a technical level, you might want to consider a higher level of security for information which could be used for fraudulent transactions or identity theft, e.g. account details and copies of passports.

We have considerable experience with these issues and can assist if you are having difficulties with them.

Prepared by Bannermans Lawyers
28 November 2017

BANNERMANS LAWYERS

T: (02) 9929 0226 M: 0403 738 996 ABN: 61 649 876 437
E: dbannerman@bannermans.com.au W: www.bannermans.com.au
P: PO Box 514 NORTH SYDNEY NSW 2059 AUSTRALIA