Are you ready to air your dirty breaches?

Presented by Kay Lam-Macleod

1 June 2018

Privacy basics

- *Privacy Act 1988* (Cth)
  - Various state and territory statutes, eg: the *Privacy and Personal Information Protection Act 1998* (NSW)

- Personal information: information or an opinion about an identified individual, or an individual who is reasonably identifiable.

- *13 Australian Privacy Principles*
  - *APP 1: have a privacy policy;*
  - *APP 2: anonymity and pseudonymity;*
  - *APP 3: collecting solicited personal information*
  - *APP 4: collecting unsolicited personal information* … and so on.

- *APP Entities – what is an APP Entity?*

Notifiable Data Breaches

- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) amended the *Privacy Act 1988* (Cth) by introducing a new Pt IIIC - *Notification of Eligible Data Breaches*
- Failure to comply is an "interference with privacy" with sanctions under the Act
- Started 22 February 2018
- Applies to **APP Entities**
- Process is triggered by an **Eligible Data Breach**

Eligible Data Breach

- unauthorised access to, or unauthorised disclosure of,
- **personal information** under the entity's control
- if a reasonable person would conclude, in the circumstances, that the access or disclosure would be likely to result in **serious harm** to any individual to whom the information related
- unless an **exception** applies

Personal Information

- What is Personal Information?
- defined in section 6 as:

" …information or an opinion about an identified individual, or an individual who is reasonably identifiable:

  - whether the information or opinion is true or not; and
  - whether the information or opinion is recorded in a material form or not“

Serious Harm

- Not defined but could include:
  - *physical, psychological, emotional, economic and financial harm*
  - *serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach*
  - embrace identity theft, stalking, embarrassment or discrimination
- Is serious harm likely to have occurred? Consider:
  - kind of information
  - sensitivity of information
  - security measures in place
  - type of person who might have gained access
  - whether effective encryption in place

Exception

- Not an "eligible data breach" if effectively contained before damage done: s 26WF(1).

So you suspect an EDB. ***Now what?***

ASSESSMENT:

- If you have reasonable grounds to suspect that there may have been a serious breach
- If uncertain, carry out a "reasonable and expeditious assessment", if at all possible within 30 days
- Guideline: If can't meet the 30 day deadline, must demonstrate
  - reasonable steps were taken
  - reasons for delay
  - assessment was reasonable and expeditious
- Take remedial action if possible

Notification

If your assessment shows reasonable grounds to believe that an "eligible data breach" has occurred:

- Give an **EDB statement** to the Commissioner (online form)
- Give the EDB statement to the affected individuals
- If not practicable to notify specific individuals, publish a copy of the statement on its website and take reasonable steps to publicise the statement
- If breach was by a third party, either the entity or the third party can notify

EDB statement

EDB statement should set out:

- the identity and contact details of the entity
- a description of the EDB
  - the date, or date range, of the unauthorised access or disclosure
  - the date the entity detected the data breach
  - the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
  - who has obtained or is likely to have obtained access to the information
  - relevant information about the steps taken so far
- the kind or kinds of information involved in the EDB
- what steps the entity recommends that individuals take in response to the EDB

Responding to data breaches

Guidelines give four key steps:

- **Contain** the data breach to prevent further compromise
- **Assess** the data breach – gather information, evaluate risk, remediate risk
- **Notify** individuals and Commissioner if required (mandatory if it's an EDB)
- **Review** incident, identify preventative measures for the future

Data breach response plan

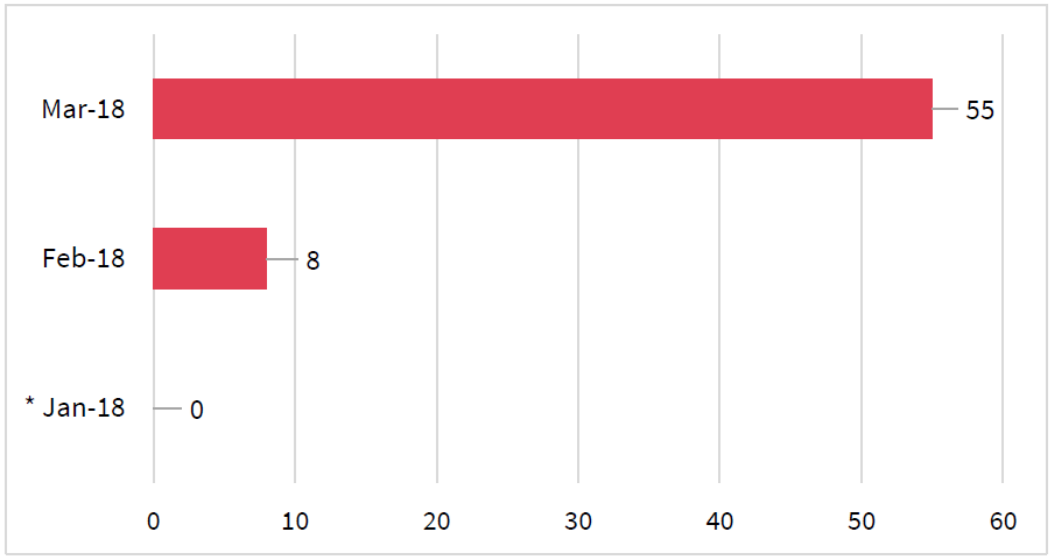
Guidelines: have a plan so staff know what to do:

- clear explanation of what constitutes a data breach
- Strategy for containing, assessing and managing data breaches
- Roles and responsibilities of staff
- How to document the data breach
- Strategy for reviewing weaknesses in data handling practices, and a system for post-breach assessment

So how's it going so far?

- Notifiable Data Breaches scheme started 22 February
- Office of the Australian Information Commissioner publishes quarterly reports
- First report covered Jan-Mar 2018

Number of breaches reported under the Notifiable Data Breaches scheme



* The NDB Scheme commenced on 22 Feb 2018

Total received for the quarter: 63

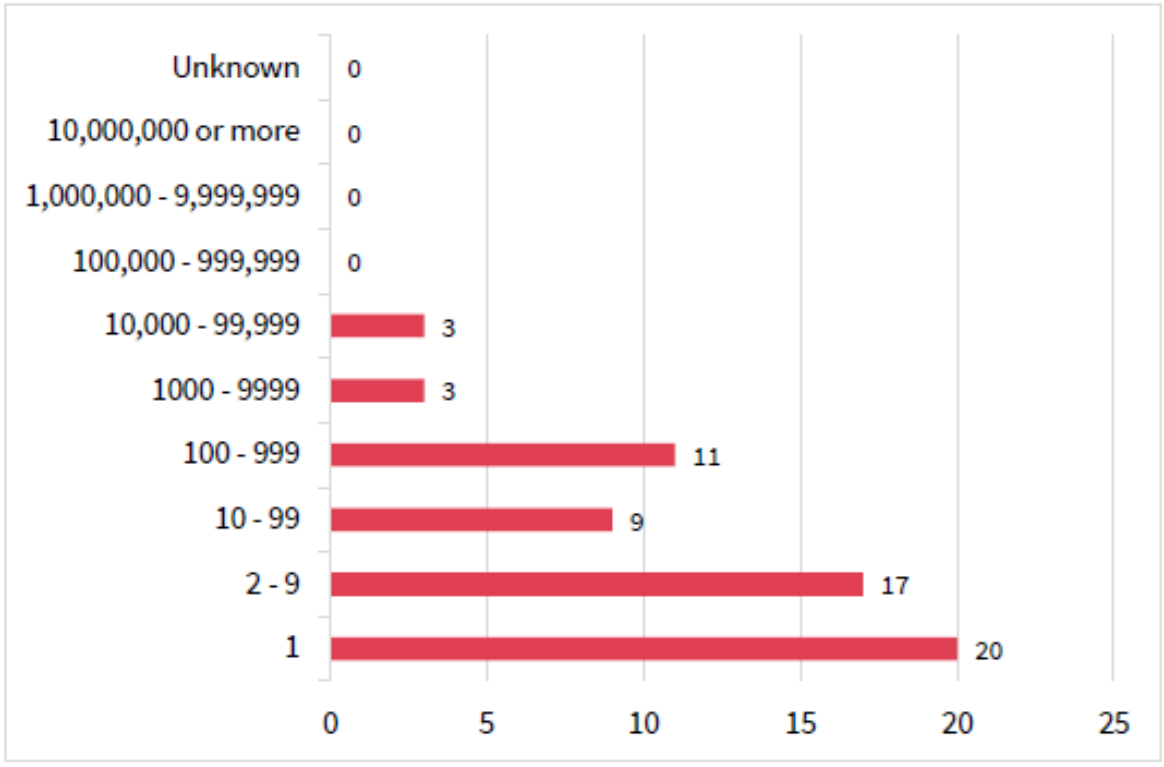
Total received YTD: 63

As the NDB scheme commenced on 22 February 2018, data is only available for part of the quarter.

Top 5 industry sectors that reported breaches in the quarter

Top 5 industry sectors	NDBs received
Health service providers	15
Legal, Accounting & Management services	10
Finance (incl. superannuation)	8
Education	6
Charities	4

Number of people affected in breaches reported in the quarter



Australian Privacy Law
vs
GDPR

GDPR key points

- What?
  - The European Union's General Data Protection Regulation (GDPR)
- When?
  - Approved by the EU Parliament on 14 April 2016
  - Enforcement starts 25 May 2018
- Why?
  - Extraterritorial
  - Multinationals meet highest applicable national standard
  - Massive penalties

International transfers

- Section 16C of the Privacy Act:
  - An APP Entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.
- APP 8:
  - Before an APP Entity discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information.
- Australian link

The GDPR Framework

- "Personal Data" – "any information relating to an identified or identifiable natural person".
  - An identifiable person means "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

- Obvious similarities to the Australian "Personal Information".

- The GDPR also has special protections for "special categories", in a similar way to how the Australian law protects "sensitive information".

The GDPR Framework

- The GDPR applies to organisations that:
  - have an establishment in the EU;
  - offer goods or services to EU data subjects (regardless of whether there is payment involved); or
  - monitor the behaviour of EU data subjects.

- (No threshold, such as the $3m APP Entity threshold.)

The GDPR Framework

- Data Controller
  - Determines how and why the personal data is processed; that is, the purposes and means of the processing.
- Data Processor
  - Processes the personal data on behalf of the Controller.
- Art 28 Agreements

Article 28 Agreements

- Under Article 28, a written agreement must be in place whenever a controller uses a processor to process personal data.
- GDPR prescribes what must be in the contract.
- Controllers must only appoint processors who can provide "sufficient guarantees" that the requirements of the GDPR can be met and the rights of the data subjects protected.
- Processors must only act on the documented instructions of the controller.

KEY SIMILARITIES AND DIFFERENCES

Key similarities and differences

- What is protected?

Privacy Act: Personal information

- Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

GDPR: Personal data

- Any information relating to an identified or identifiable natural person.

Key similarities and differences

- Who is bound?

Privacy Act: APP Entities

- Most government entities
- All private sector and NFP organisations with annual turnover > $3m
- Some types of small businesses, such as health service providers

GDPR: the data processing activities of businesses.

- No size threshold
- Different application for controllers and processors

Key similarities and differences

- Accountability and Governance requirements

Privacy Act:

- APP entities must take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and to enable complaints.
- Businesses are expected to appoint key roles and responsibilities for privacy management and to conduct privacy impact assessments for many new and updated projects.

GDPR:

- Article 30 Register.
- DPIA are compulsory
- DPOs and Representatives

Key similarities and differences

- Consent requirements

Privacy Act:

- Informed
- Voluntary
- Current and specific
- Individual has capacity

GDPR:

- Freely given, specific and informed
- An unambiguous indication of the individual's wishes which signifies agreement to processing
- Proactive
- Valid lawful bases

Key similarities and differences

- Mandatory data breach notification

Privacy Act:

- New provisions (commenced 22/02/18)
- Modeled on the GDPR provisions, so very similar.
- An APP Entity has to provide a statement to the Privacy Commissioner notifying of an eligible data breach as soon as practicable after becoming aware, and notify individuals after preparing the statement (30 calendar days to assess suspected breach).
- Eligibility

GDPR:

- Controllers must advise the regulator of a data breach within 72 hours of becoming aware. (Processors must advise the relevant Controller)
- Unless the breach is unlikely to result in serious harm to any of the data subjects.

Key similarities and differences

- Privacy notices

Privacy Act:

- APP Entities must notify individuals of various facts on collecting their information.

GDPR:

- Very similar provision
  - DPOs
  - Legal basis of processing

Key similarities and differences

- Overseas transfers

Privacy Act:

- APP 8 and 16C – as discussed.

GDPR:

- Only to countries with adequate level of data protection.
- Those countries are formally listed.
- If the recipient is in a country that is not listed, then only with the recipient volunteering to equivalent obligations by contract
- If no contract, then only by explicit and informed consent of the data subject.

Key similarities and differences

- Penalties

Privacy Act:

- Privacy Commissioner has enforcement powers, including maximum civil penalties of $2.1M.
- In 2016-17, the Privacy Commissioner resolved 124 complaints involving compensation:
  - 17 for less than $1,000
  - 38 for in between $1,000 and $5,000
  - 18 between $5,000 and $10,000
  - 14 over $10,000

GDPR:

- Serious contraventions: up to €20 million or 4% of annual worldwide turnover (whichever is higher)
- Less serious contraventions: up to €10 million or 2% of annual worldwide turnover (whichever is higher)

Key similarities and differences

- Individual rights

Privacy Act:

- No real individual rights in the Privacy Act
  - Access records
  - Correct records
  - Deal anonymously or pseudonymously
- Enforcement through Privacy Commissioner

GDPR:

- A suite of new individual rights
- Game changing

Individual rights

The Right to Erasure

- Also known as the "right to be forgotten".

- Applies in quite a few sets of circumstances, including:
  - the personal data is no longer necessary for the purpose for which it was originally collected or processed;
  - consent is the relied upon lawful basis, and consent is now withdrawn;
  - legitimate interests was the relied upon lawful basis, and now the individual objects and points to a countervailing interest;
  - processing for direct marketing, and individual now objects to that processing;

- Individuals can make a request for erasure verbally or in writing
- One month to respond to request.
- But obligation to delete may arise elsewhere in the GDPR.

The Right to Restrict Processing

- Individuals can ask a controller to restrict processing in certain circumstances.

- The GDPR suggests a number of different methods that could be used to restrict data, such as:

  - temporarily moving the data to another processing system;

  - making the data unavailable to users; or

  - temporarily removing published data from a website.

The Right to Data Portability

- Individuals have the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format.

- Individuals also have the right to request that a controller transmits this data directly to another controller, in a safe and secure way, without affecting its usability

The Right to Object to Processing

- Individuals have the **absolute right** to object to the processing of their personal data if it is for direct marketing purposes.

- Individuals can also object if the processing is for:
  - a task carried out in the public interest;
  - the exercise of official authority vested in you; or
  - your legitimate interests (or those of a third party).
- In these circumstances the right to object is **not absolute**

Rights related to automated decision making, including profiling

- Essentially a prohibition against profiling.
  - Profiling: "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

- Article 22 gives individuals a right not to be subject to a decision based solely on automated processing, including profiling, which **produces legal effects** concerning him or her or **significantly affects** him or her.

Brexit

- If your client's European operations are limited to the UK, then will it need to worry about GDPR-compliance post-Brexit?

Summary

- The GDPR implements the following changes:
  - The GDPR sets a clear standard, rather than piecemeal approach
  - More comprehensive than other privacy law;
  - Requires organisations to know what personal data they hold;
  - The GDPR has more onerous governance and accountability requirements, in particular DPOs.
  - Individual rights
  - Consent
  - Obligations follow the data
  - Penalties

Contact

Kay Lam-Macleod
Special Counsel
P +61 7 3169 4721
E klmacleod@hwle.com.au

Adelaide | Brisbane | Canberra | Darwin | Hobart | Melbourne | Norwest | Perth | Sydney