Australian Privacy Foundation

Data Breach Notification

APF Policy Statement on Data Breach Notification

A data breach occurs when personal data is exposed to an unauthorised person. It is a breach of trust by the organisation. It is commonly also a breach of the law. Unfortunately breaches of data protection laws are seldom subject to enforcement actions.

Data breaches occur remarkably frequently. Parliaments have failed to impose meaningful sanctions, and privacy oversight agencies have failed to exercise such powers and influence as they have to force organisations to ensure that appropriate security safeguards are in place.

In 2003, the Californian legislature responded to inadequacies in organisational practices by passing a Security Breach Notification Law. By 2006, 33 other US States had passed similar laws. Australian law reform has moved at glacial pace, and lags the US in this matter by a decade.

This document declares the APF's Policy on Data Breach Notification. It comprises the following sections:

Definitions

A **Data Breach** occurs where personal data held by an organisation has been subject to, or is reasonably likely to have been subject to, unauthorised access, disclosure, acquisition or loss.

A **Serious Data Breach** is a Data Breach that gives rise to a reasonable risk of harm to an individual.

A **Data Breach Notification** is a statement of the facts relating to a Data Breach.

The Purposes of Data Breach Notification

The purposes of Data Breach Notification are:

1. to inform the public, at a meaningful level of detail, about:
    - breaches
    - inadequacies in organisations' security safeguards
2. to inform individuals who have been affected by breaches, so that they can judge whether to:
    - take action to prevent or mitigate potential harm arising from the breach
    - seek compensation for harm caused
    - change their service-providers
3. to shame organisations that have seriously inadequate security safeguards into changing their ways
4. to encourage all organisations to implement adequate security safeguards

Data breach notification processes, guidelines and regulations need to be designed so as to achieve these purposes.

Organisations' Obligations in Relation to Data Security

1. All organisations must ensure that personal data is at all times subject to security safeguards commensurate with the sensitivity of the data. The APF has previously published a Policy Statement on Information Security
2. All organisations must take the steps appropriate in their particular circumstances to:
    - deter Data Breaches
    - prevent Data Breaches
    - detect Data Breaches
    - mitigate harm arising from Data Breaches; and
    - enable their investigation
3. All organisations must implement awareness, training and control measures to ensure appropriate practices by their staff
4. All organisations must conduct audits of security safeguards periodically, and when the circumstances warrant
5. All organisations must perform a Privacy Impact Assessment (PIA) when data systems are in the process of being created, and when such systems are being materially changed, in order to ensure that appropriate data protections are designed into their systems, and to demonstrate publicly that this is the case

---

Organisations' Obligations in Relation to Data Breach Notification

1. Conduct of an Investigation

Where grounds exist for suspecting that a Data Breach may have occurred, the organisation must conduct an investigation, in order to establish a sufficient understanding of the circumstances and the outcomes. The results of the investigation must be documented in a form that enables subsequent evaluation.

2. Submission of a Data Breach Notification

Where a Data Breach has occurred, or is reasonably likely to have occurred, the organisation must:

1. Submit a Data Breach Notification to the relevant oversight agency, in a manner consistent with the guidance issued by that oversight agency, as soon as practicable and without delay
2. Communicate sufficient information to affected categories of individual, the media, and/or representative and advocacy agencies, as appropriate to the circumstances

3. Form of a Data Breach Notification

A Data Breach Notification must include sufficient detail to enable the reader to achieve a proper understanding of the Data Breach, its causes, its scale, its consequences, mitigation measures, and the rights of individuals affected by it.

Details whose publication might result in harm or facilitate attacks on that or other organisations can be included within a separate Appendix whose distribution can be limited.

4. Additional Obligations in the Case of a Serious Data Breach

Where a Serious Data Breach has occurred, or is reasonably likely to have occurred, the organisation must, in addition:

1. Provide an explanation, apology and advice to each individual whose data is, or is reasonably likely to be, the subject of the Data Breach, as soon as feasible and without delay, but taking into account the possible need for a brief delay in the event that criminal investigation activities require a breathing-space
2. Publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information
3. Where material harm has occurred, provide appropriate restitution

4. Inform the oversight agency of the actions taken

The Reponsibilities of the Oversight Agency

1. Publish guidance in relation to data security safeguards.
This must make clear that organisations have obligations to perform Security Risk Assessment, and to establish an Information Security Risk Management Plan whereby information security safeguards are implemented and maintained, commensurate with the sensitivity of the data

2. Publish guidance in relation to Data Breach Notifications

3. In relation to Data Breaches:

- Liaise with organisations that have suffered Data Breaches
- Facilitate the Submission of Data Breach Notifications
- Inform the Public
- Publish the Data Breach Notifications in a Public Register

4. In relation to Serious Data Breaches:

- Review the outcomes of the organisation's internal investigation
- Where doubt exists about the quality of the internal investigation, conduct its own independent investigation
- Publish the results of the review and/or investigation
- Add details of the investigation into the Public Register

5. Facilitate improvements in organisational practices relating to data security

6. Facilitate remedies for individuals who have suffered as a result of Data Breaches

---

Enforcement

All obligations in relation to Data Breach Notification must be subject to sanctions and enforcement.

The sanctions applied must reflect:

- the organisation's degree of culpability, including:
  - the extent to which the organisation had implemented safeguards commensurate with the sensitivity of the data
  - the extent to which the threat(s) and vulnerability/ies that gave rise to the Data Breach were well-known or novel
- the promptness and effectiveness with which the organisation reacted once grounds existed for suspecting that a Data Breach may have occurred
- mitigation measures adopted by the organisation once it was apparent that a Data Breach had occurred, or was reasonably likely to have occurred
- any avoidance activities, misinformation or delays by the organisation in responding to the Data Breach and in its interactions with the oversight agency
- the scale of the Data Breach
- the sensitivity of the data that was the subject of the Data Breach
- the measures undertaken by the organisation in order to address the risk of recurrence of Data Breaches (as distinct from the organisation's statements about what it intends to do)
- to the extent that financial penalties are applied, the size of the organisation

---
