national electrical and communications association

The Notifiable Data Breaches Scheme

Presented by: Jacques Nel
Senior *Solicitor at NECA Legal*

This presentation is for information only and not legal advice

The NDB Scheme - Introduction

The NDB Scheme – Part IIIC of *Privacy Act 1988 (Cth)*

- **The *Privacy Amendment (Notifiable Data Breaches) Act 2017* came into effect on 22 February 2018 established the Notifiable Data Breaches (NDB) Scheme in Australia:**
- **Mandatory obligations for APP Entities to notify eligible data breaches:**
  - **Australian Information Commissioner;**
  - **Individuals whose personal information is involved.**

- **Assessment of data breach, if unclear whether eligible data breach occurred**

neca Legal

Key Concepts

- **Personal Information – What is it?**
- **APP Entities - Who must comply?**
- **Data breach – What is a data breach?**
- **Eligible Data Breach – Trigger for Notification**
- **Notification Obligations**
- **Data Response Plan**

Key Concepts – APP Entities

Who Must Comply – APP Entities

APP Entities

- **Australian agencies and organisations**
- **Annual Turnover of more than $3 Million**
- **Specific entities for example health service providers, trade in personal information, Tax File Number (TFN) recipients, credit providers and credit reporting bodies, contracting with Commonwealth (exceptions- employers)**

Resource: OIAC Checklist for Small Businesses https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10

neca Legal

Key Concepts – Personal Information

What is Personal Information ?

Privacy Act - Definition:

'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.'**

Examples of Personal Information:

- **Person's name, address or telephone number and date of birth;**
- **Medical records, bank account details or TFN,**
- **Commentary or opinion about a person**

neca Legal

Key Concepts – Personal Information

Sensitive Personal Information (S 6(1)):

- **Information or an opinion about a person's**:
  - **racial or ethnic origin; or**
  - **political opinions; or**
  - **membership of a political association; or**
  - **religious beliefs or affiliations; or**
  - **philosophical beliefs; or**
  - **membership of a professional or trade association; or**
  - **membership of a trade union; or**
  - **sexual orientation or practices; or**
  - **criminal record.**
- **Health Information;**
- **Biometric Information for use of biometric identification (DNA, fingerprints etc).**

Key Concepts – Data Breach

When is there a Data Breach?

- **Unauthorised access to or unauthorised disclosure of personal information or loss of personal information**
  - **Unauthorised access – access by person not permitted to have access, for example a hacker obtain access to personal information on server**
  - **Unauthorised disclosure – for example when personal information is inadvertently published by email or otherwise**
  - **Loss of personal information - for example an employee leaves laptop on public transport**

Key Concepts – Eligible Data Breach

Pre- 22 February 2018 – No notification obligations

Three Criteria for Eligible Data Breach (from 22 Feb 2018)

1. **Data Breach;**
2. **Data Breach must be likely to result in serious harm to one or more individuals;**
3. **Risk of serious harm could not be prevented by remedial action.**

Objective Assessment – Test is that of a reasonable person in the position of the entity

neca Legal

Eligible Data Breach – Serious Harm

- **What is serious harm?**
  - **No definition of serious harm in *Privacy Act***
  - **In context of a data breach may include physical, psychological, emotional, financial or reputational harm**

  Common Examples include:
    - **Financial fraud, including unauthorised transactions**
    - **Identity theft**

Serious harm is likely to occur, when the risk of serious harm to a person is more probable than not (rather than a possibility)

neca Legal

Likelihood of Serious Harm

- **NDB Scheme - non-exhaustive list of relevant matters to consider:**

• Type of Information	• Security technologies used - encryption
• Sensitivity of information	• Likelihood persons obtained info may have intention to cause harm
• Security measures in place	• Nature of harm
• Likelihood that security measures may be overcome	• Other matters

Type of Information – Serious Harm

- **Information with increased risk of serious harm**
  - **Sensitive information – health information**
  - **Documents used for identity fraud (Medicare Card, driver licence and passport details)**
  - **Financial information**
  - **Combination of personal information**

Assessment of Eligible Data Breach

Two Thresholds:

1. **Reasonable grounds to believe that eligible data breach has taken place → Notify immediately**
2. **Reasonable grounds to suspect that eligible data breach has taken place → Assessment within 30 days**

neca Legal

Notification of Eligible Data Breaches

- **Australian Information Commissioner**
- **Affected individuals**
- **Prescribed method of notification – Notifiable Breach Statement form**
- **Lodged online with Commissioner**
- **Individuals**
  - **Notify all individuals; or**
  - **Notify only individuals at risk of serious harm; or**
  - **Publish notification on website.**

neca Legal

Notifiable Breach Statement

- **Organisation Details**
- **Description of Eligible Data Breach**
- **Information involved in the data breach**
- **Recommended steps to reduce risk of serious harm**
- **Other entities involved (optional)**
- **Additional information, including date of breach, date breach discovered, primary cause of breach, number individuals involved, assistance provided to individuals at risk.**

neca Legal

Data Breach Response Plan

- **Entity's action plan for any data breach event**
- **Privacy Act requires APP entities to take reasonable steps to protect personal information – Data Breach Response Plan**
- **Limit consequences of data breach by fast response / limit reputational damage to entity**
- **Preserve and build public trust**

Data Breach Response Plan

- **Clear explanation of what constitutes a data breach**
- **Strategy for containing, assessing and managing data breaches**
- **Roles and responsibilities of personnel**
- **Documentation**
- **Review and evaluate plan regularly**

Penalties for non- compliance

- **Civil penalties for individual - $420,000**
- **Companies - $1.2Million**
- **Serious and repeated non-compliance with NDB Scheme**
- **Commissioner has acknowledged that it will take time for entities to become familiar with requirements of NDB Scheme – focus during first 12 months working with entities to ensure they understand requirements and are working in good faith to implement…**

Conclusion

- NDB Scheme applies to APP Entities – 22 February 2018
- Consider measures to protect personal information
- Data Breach Response Plan
- Online resources: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

Conclusion

Further NECA Legal Services

- Building Defects and Home Warranty Insurance Claims
- Commercial and Contractual Advice
- Debt Collection
- Representation
- Security of Payment Advice (SOPA)
- Training
- Workplace Health and Safety
- Workplace Relations

neca Legal

Contact Us

Contact NECA Legal

Stafford Poyser stafford.poyser@neca.asn.au
Solicitor/Director
Jacques Nel jacques.nel@neca.asn.au
Senior Solicitor
Marina Galatoulas law.clerk@neca.asn.au
Junior Solicitor
Margaret Ward: margaret.ward@neca.asn.au
Legal Secretary
Jane Button
Consultant Solicitor
Jakov Miljak
Industrial Relation *jakov.miljak@neca.asn.au*

Telephone:
(02) 9744 1099

Facsimile:
(02) 9744 1830

Websites:
www.neca.asn.au
www.constructionlawyersydney.com