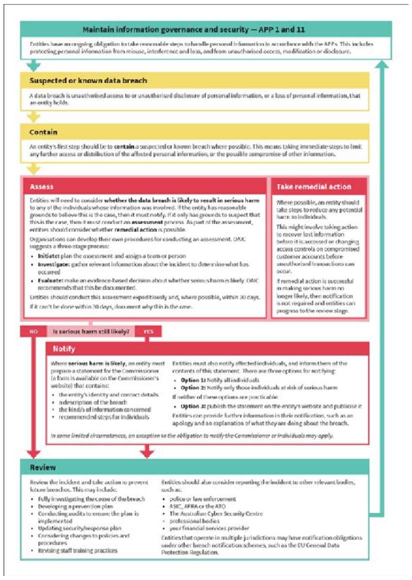
How Does Blancco Help

Organisations Comply with Australia's Notifiable Data Breaches Scheme?

Data Breach Response Summary

This diagram[1] provides an overview of a standard data breach response and follows the requirements of the NDB scheme.



Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO | Is serious harm still likely? | YES

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Visit the **OAIC website** to learn more about how to plan a data breach response.

Underpinning the Privacy Act are the **Australian Privacy Principles** guidelines (APP), with APP 11.2 setting out that government and other affected organizations must take reasonable steps to destroy or de-identify the information they have once it is no longer needed for any purpose permitted under these guidelines. Separate obligations exist for personal information included in "Commonwealth records" and where entities are required by law (court/tribunal order) to retain the information.

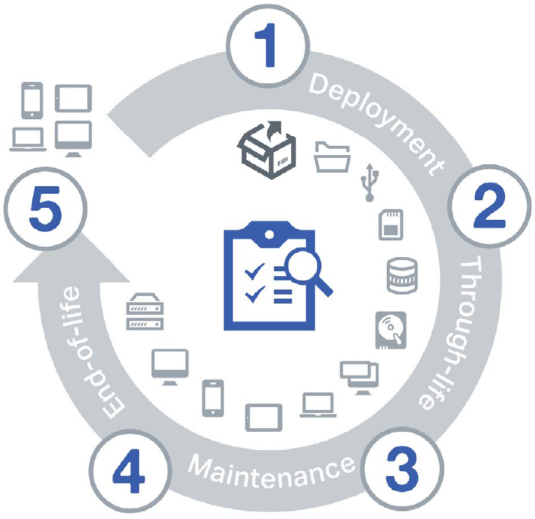
The Notifiable Data Breaches (NDB) scheme, which went into effect February 22, 2018, mandates that Australian Government agencies and other organisations with the obligation to protect secure personal information under the Privacy Act 1988 (Cth) (Privacy Act) must notify individuals affected by data breaches who are likely to be adversely affected.

The NDB falls under Part IIIC of the Privacy Act. The requirements of this Act are outlined in the **Guide to Securing Personal Information,** which gives guidance on the reasonable steps organisations are required to take to protect "the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure." The guide is not legally binding; however, it is used by the Office of the Australian Information Commissioner (OAIC) as a reference for privacy assessments and investigations under the Privacy Act.

The guide gives recommendations on securing data throughout its lifecycle, including the "destruction or de-identification of the personal information when it is no longer needed."

The image below shows how data erasure software can support data destruction throughout the IT asset lifecycle.

1. **Deployment**
   - IT Administration
   - MC Installation
   - Software Distribution (MSI, EXE)
   - Easy Deployment of Eraser
2. **Through-life**
   - Corporate / Data Center
   - Data End-of-life
   - No down time
   - Automated workflows
   - Time-based subscription
3. **Maintenance**
   - Loose HDD (RMA)
   - Maintenance, repairs & operations (MRO)
4. **End-of-life**
   - Employee departures
   - End of lease
   - Asset & data end-of-life
   - Volume-based
5. **Outgoing**
   - Pick up / ITAD
   - Asset is physically leaving
   - Second-hand market



[1] https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps/

How can Blancco help?

Blancco data erasure solutions can remove data from IT assets in both active and inactive environments to meet compliance with APP guidelines and assist companies with the NBD by providing them with proof of erasure of sensitive information in the event of a data breach. Each erasure is verified and certified with an audit-ready, tamper-proof data erasure certificate, which can be recorded, tracked and easily accessed within the **Blancco Management Portal** when it's time to prove compliance.

By securely erasing the data you no longer need, your organisation can reduce its attack surface to ensure sensitive data isn't within the reach of unauthorised individuals. And with a proper audit trail, you can ensure compliance and notify customers as soon as possible which data has been affected.

According to the APP Guidelines, your organization should ask the following questions regarding data disposal:

- ☑ Do you have policies, procedures and resources in place to determine whether personal information you hold needs to be: retained under law or a court/tribunal order, destroyed or de-identified?
- ☑ Are your staff informed of document destruction procedures?
- ☑ Is destruction of personal information done in-house or outsourced?
  - ☑ If outsourced, what steps have you taken to ensure appropriate handling of the personal information?
- ☑ Has personal information contained in hard copy records that are disposed of through garbage or recycling collection been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding?
- ☑ Is hardware containing personal information in electronic form properly 'sanitized' to completely remove the stored personal information?
- ☑ Have steps been taken to verify the irretrievable destruction of personal stored information by a third party on a third party's hardware, such as cloud storage, where the third party has been instructed by the organization to irretrievably destroy the personal information, have steps been taken to verify that this has occurred?
- ☑ Are back-ups of personal information also destroyed? Are backups arranged in such a way that destruction of backups is possible? If not:
  - ☑ have steps been taken to rectify this issue in the future?
  - ☑ has the backed-up personal information been put beyond use?
- ☑ How is compliance with data destruction procedures monitored and enforced?

Why Blancco?

For 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as Australia's Notifiable Data Breaches Scheme. We support the need for heavily-regulated industries to stay compliant with these regulations with data erasure solutions that satisfy (and often exceed) those requirements.

Contact us today for additional information about how we can help you pass your next data security and compliance audit.