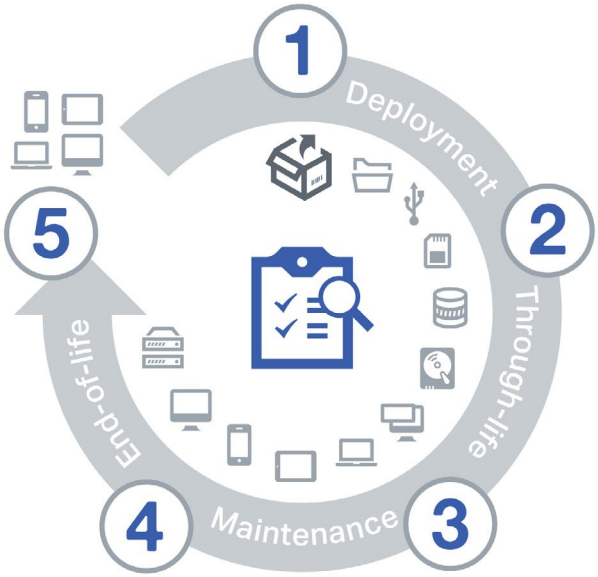
How Does Blancco Help Organizations Comply with Australia's Notifiable Data Breaches Scheme?

The Notifiable Data Breaches (NDB) scheme, which went into effect February 22, 2018, mandates that Australian Government agencies and other organizations 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. Much in the same way the EU's GDPR will penalize those organizations that do not comply with this notification. Fines for noncompliance can reach up to $2.1 million.

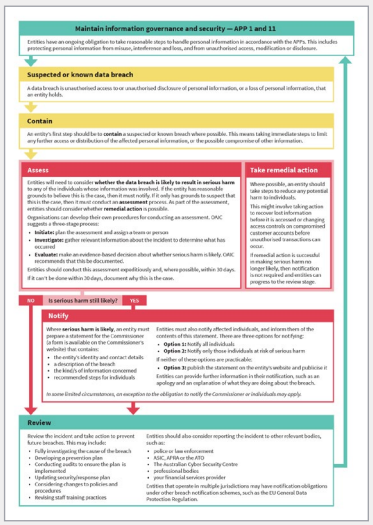
The new Scheme falls under Part IIIC of the ***Privacy Act 1988*** (Privacy Act). The requirements of this Act are outlined in the Australian government's 'Guide to securing personal information' which provides guidance on the reasonable steps organizations are required to take to protect "the personal information they hold from misuse, interference, loss, and from unauthori[z]ed access, modification or disclosure." This guide is not legally binding; however, it is used by the government as a reference when undertaking Privacy Act functions, including its privacy assessments and investigations.

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."

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



Data Breach Response Summary



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

Click here to download the PDF.

Under the *Australian Privacy Principles guidelines* (APP) 11.2, 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 that it may be used or disclosed under these guidelines. The exception is personal information is included in a "Commonwealth record" or where the entity is required to do so by law (court order) to retain the personal information.

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

blancco

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?

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 Console when it's time to prove compliance.

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

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.