How Blancco Helps Organisations Comply with Australian Privacy Regulations

What's Inside...

An Overview of Australian Data Privacy Act and ISM Requirements

When it comes to data privacy, federal public sector enterprises in Australia are primarily guided by the Australian Privacy Act (which also governs certain private sector organisations) and the Australian Government Information Security Manual. Together, they cover data destruction requirements and methods for different kinds of data stored across various media types and locations.

The Australian Privacy Act of 1988 (Privacy Act)

The Australian Privacy Act of 1988 (Privacy Act) applies primarily to large organisations ($3+ million annual turnover) and most government agencies. Both must follow the Privacy Act's direction on managing personal information along the data lifecycle, including at data disposal. To do otherwise means being subject to financial penalties for noncompliance, as well as becoming more vulnerable to unauthorised data access.

The Privacy Act's 13 Australian Privacy Principles (APPs) include guidance on how personal information should be processed, protected and corrected, with APP 11, 'Security of personal information', dealing most directly with data destruction. It states that all APP entities, with a few exceptions, must take reasonable steps to:

- Protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- Destroy personal information or ensure that it is de-identified when the APP entity no longer needs that information.

The Privacy Act also contains the Notifiable Data Breaches (NDB) scheme, which lays out who to contact when a data breach involving personal information is likely to result in serious harm.

The Australian Government Information Security Manual (ISM)

The Australian Government Information Security Manual (ISM) provides a cybersecurity framework that organisations can use to protect their information systems and data from cyber threats. Key guidance here addresses secure management of information and communications (ICT) equipment, including the importance of onsite data sanitisation when sending equipment out for maintenance and repairs or when outsourcing hardware sanitisation and disposal. The ISM also includes requirements for removing data from various digital media. In both cases, the ISM defines media sanitisation as '[t]he process of erasing or overwriting information stored on media so that it cannot be retrieved or reconstructed,' a definition echoed by the Australian government's 'Guide to Securing Personal Information.'

Additional Data Destruction Considerations

The OAIC's Guide To Securing Personal Information

While not legally binding, this 'Guide to Securing Personal Information', published by the Office of the Australian Information Commissioner (OAIC), works in conjunction with APP guidelines and organisations are encouraged to read both. The OAIC also refers to other standards and publications on data security, including the ISM.

In addressing data security, the Guide calls destroying or de-identifying personal information 'an important risk mitigation strategy'. The Guide also states that the obligation to destroy or de-identify personal information that's no longer needed 'applies even where the entity does not physically possess the personal information, but has the right or power to deal with it'. In essence, eligible public and private sector organisations are responsible for destroying or permanently de-identifying the personal information they steward when it reaches data end-of-life, regardless of whether the data resides on their own network, on backups (addressed earlier in the Guide under 'ICT security') or on the networks of third-party vendors, including cloud providers. It also advocates verifying that the correct data destruction measures have occurred.

Common Data Lifecycle Principles

All three resources, the Privacy Act, and ISM, and the Guide, advocate destroying data at various stages along the asset and data lifecycles so that it is irretrievable. The Guide also notes that some information may not be considered personal information on its own, but combined with other data points, individuals may still be identifiable. To protect sensitive or personal data against breaches, entities must take reasonable steps to ensure this data never leaves its location or control in any way that renders it vulnerable to unauthorised access. For these reasons, and when at all possible, the ISM recommends that hardware containing personal information should be properly sanitised onsite so that data is irretrievable. Likewise, data management policies should include data sanitisation as a mandatory piece to comply with data privacy regulations and to protect against data breaches.

Penalties

The OAIC has the authority to initiate the process for levying tough penalties against any entity that is alleged to have violated the Privacy Act. Following the 2019 changes to the Privacy Act, penalties can be even more substantial. The current maximum penalty amounts for APP entities for the misuse of personal information has been raised to the greatest of:

- $10 million, or
- three times the court-determined 'value of any benefit...reasonably attributable to the violation', or
- 10 percent of an organisation's annual turnover during the applicable 12-month period.[1]

1 For further information: www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties

How Blancco Can Help

For proper sanitisation, data removal should result in data being completely and permanently unrecoverable and each erasure should be verified. This means formatting, deleting and many other commonly used methods are insufficient, often leaving data behind.

Blancco's software-based data erasure solutions can target specific files or folders in active environments, sanitise entire devices—from flash drives to whole server arrays—or remove data from public or private cloud networks and erase to more than 25 recognised data erasure standards. Blancco customers receive an audit-ready, tamper-proof certificate for each erasure. Blancco also provides an option to allow auditors to log in to the customer's Blancco Management Console through an auditor-specific role. This makes it easy to prove compliance .

With this in perspective, the following Blancco solutions will be useful.

- **Blancco File Eraser**. If sensitive information is identified on the file level (e.g., a copy of a customer database or a file structure with individual files and folders), Blancco File Eraser can target and erase files on computers and servers on both UNIX and Windows operating systems.
- **Blancco Drive Eraser**. Blancco Drive Eraser securely erases all data on enterprise laptops and desktops, as well as servers, storage systems and loose drives, including NVMes and self-encrypting drives.
- **Blancco Mobile Diagnostics & Erasure**. If sensitive information is identified on mobile devices or tablets, Blancco Mobile Diagnostics & Erasure can target and erase data on any device that's iOS or Android-based, using factory reset or more advanced erasure methods.
- **Blancco LUN** and **Virtual Machine Eraser**. For data stored temporarily on virtual volumes or machines, on premise or in the cloud, Blancco Virtual Machine Eraser and Blancco LUN Eraser can be used together or separately to target relevant data in active storage environments while allowing the operating system to remain intact.
- **Blancco Removable Media Eraser**. This solution erases removable flash media devices used within smartphones, tablets, network routers and cameras, including USBs and SD cards.

> **"The ISM defines media sanitisation as '[t]he process of erasing or overwriting information stored on media so that it cannot be retrieved or reconstructed,' a definition echoed by the Australian government's 'Guide to Securing Personal Information'.**

Privacy Act Compliance

Below, we've mapped data destruction requirements from the Australian Privacy Act (July 2020) to the Blancco data erasure solutions that help meet or exceed compliance. Please note the information provided in this presentation is not intended as legal and/or compliance advice. Please refer to the original legislation or to your own attorney or legal advisor for regulation exceptions, additional requirements and guidance on how these laws apply to your organisation.

PART IIIA—CREDIT REPORTING

REQUIREMENTS	HOW BLANCCO HELPS
Subdivision D—Dealing with credit reporting information, etc. **20J Destruction of pre screening assessment** 1. If an entity has possession or control of a pre screening assessment, the entity must destroy the assessment if: a. the entity no longer needs the assessment for any purpose for which it may be used or disclosed under section 20H ['Use or disclosure of pre-screening assessments']; and b. the entity is not required…to retain the assessment. **Subdivision E—Integrity of Credit Information and Credit Eligibility Information** **21S Security of credit eligibility information** 1. (1) If: a. a credit provider holds credit eligibility information about an individual; and b. the provider no longer needs the information…; and c. the provider is not required…to retain the information; the provider must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.	**Secure Folder & File-Level Data Erasure** If information is identified on the file level (e.g., a copy of a customer database or a file structure with individual files and folders), Blancco File Eraser can target and erase files on computers and servers manually or automatically on both UNIX and Windows operating systems. Blancco File Eraser easily integrates into enterprise IT systems and may be centrally managed and deployed onto any machine, including desktop computers, laptops, and servers. This allows enterprises to implement rules and automatic routines to erase files and folders, enforcing data retention and disposal policies while creating and maintaining a comprehensive audit trail. While typical file shredding or wiping software may delete some data, Blancco File Eraser erases files and folders to comply with the most stringent requirements, including ISO 27001, ISO 27040, and PCI DSS, to ensure that any sensitive data has been permanently removed. Blancco File Eraser also supports all global data erasure standards, including NIST 800-88 Clear and others. It also supports the file sanitisation guidance in the Australian ISM. Blancco File Eraser is certified by more regulatory bodies than any other solution—including Common Criteria (ISO 15408)[2] — and erasures are verified with a 100% tamper-proof report.

2 Blancco File Eraser 8.2

PART IIIA—CREDIT REPORTING *Continued*

REQUIREMENTS	HOW BLANCCO HELPS
Subdivision G—Dealing with credit reporting information after the retention period ends **20V Destruction etc. of credit reporting information after the retention period ends** This section applies if: a. a credit reporting body holds credit information about an individual; and b. the retention period for the information ends. *Destruction etc. of credit information* The credit reporting body must destroy the credit information, or ensure that the information is de-identified, within 1 month after the retention period... [***Blancco Note:*** Retention periods are specified in **'20W Retention period for credit information—general'**. Periods range from two to seven years, depending on the type of general credit information. Additional retention periods for information related to personal insolvency are in subsection **20X**.]	**Verified Data Sanitisation for Out-of-Retention Data Across All Data Storage Assets** Blancco data erasure solutions enable automatic data erasure according to an organisation's retention policy requirements. Blancco File Eraser supports scripting and scheduling to erase qualified data on a regular, ongoing basis. Used with Blancco Management Console, a central operations and reporting dashboard for all Blancco erasure products, this process minimises unnecessary data while documenting what erasures have occurred. Blancco File Eraser is also supported by Blancco Virtual Machine Eraser and Blancco LUN Eraser, erasing data centre virtual machines and logical unit numbers all the way down to individual files and folders on the desktop. For entire drives storing out-of-retention data, Common Criteria-Certified Blancco Drive Eraser, certified under the Australasian Information Security Evaluation Program, supports full erasure of hard disk drives and solid-state drives, including advanced SSDs.[3] The erasure process includes detection, notification and erasure of hidden areas (DCO, HPA) and remapped sectors, and provides support for internal drive erasure commands, ensuring that all data is completely removed. Blancco Drive Eraser also supports erasure of self-encrypting drives. ISM Guidelines for Media: Media sanitisation includes more details on media sanitisation guidance that the Blancco Drive Eraser fulfils.

[3] Blancco Drive Eraser 6.9.1 was evaluated and certified in the category of Data Protection and complies with the requirements of Common Criteria EAL2. Please see 'Blancco Drive Eraser Certified for Government Use in Australia and New Zealand' on our website for more information.

PART IIIA—CREDIT REPORTING *Continued*

REQUIREMENTS	HOW BLANCCO HELPS
20Y Destruction of credit reporting information in cases of fraud *Destruction of credit reporting information* 2. The credit reporting body must: a. destroy the credit reporting information; and b. within a reasonable period after the information is destroyed: i. give the individual a written notice that states that the information has been destroyed and sets out the effect of subsection (4.); *and* ii. give the credit provider a written notice that states that the information has been destroyed. 3. Subsection (2.) does not apply if the credit reporting body is required...to retain the credit reporting information.	**Centralised Erasure, Reporting & Communication** *Please also see 'Secure Folder & File-Level Data Erasure'.* Used with Blancco Management Console, Blancco data erasure solutions facilitate easy report importing, exporting (PDF, XML, CSV), editing, emailing and validating, enabling you not only to destroy credit information but also to notify the appropriate stakeholders when this information has been destroyed. With Blancco Management Console, organisations have the flexibility to integrate with existing systems, manage remote erasures, distribute licenses across global locations and manage users from one central point of control. Reports may be stored, managed and accessed at any time in the Blancco Management Console, available in on-premise or as a cloud service hosted by AWS.
20Z Dealing with information if there is a pending correction request etc. *Direction to destroy information etc.* 6. The Commissioner may, by legislative instrument, direct the credit reporting body to destroy the information, or ensure that the information is de identified, by a specified day. 7. If the Commissioner gives a direction under subsection (6.) to the credit reporting body, the body must comply with the direction.	**Secure, Complete, and Permanent Data Destruction** Whether data is located on local devices, in the cloud, or in virtual or logical storage, Blancco data solutions provide software-based data destruction that is complete and verified. Other data destruction attempts—including deleting, formatting and file shredding—fail to verify data destruction, and in fact, often leave data behind. Each Blancco erasure is documented with a detailed, tamper-proof report to attest that the erasure was completed and verified. This can help enterprises document compliance with regulations and respond to audit requests from the regulatory authorities.

> **Blancco customers receive an audit-ready, tamper-proof certificate for each erasure. Blancco also provides an option to allow auditors to log in to the customer's Blancco Management Console through an auditor-specific role. This makes it easy to prove compliance'.**

AUSTRALIAN PRIVACY PRINCIPLE 11—SECURITY OF PERSONAL INFORMATION

REQUIREMENTS	HOW BLANCCO HELPS
Schedule 1—Australian Privacy Principles **Part 4—Integrity of personal information** **11.2 If:** a. an APP entity holds personal information about an individual; and b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and c. the information is not contained in a Commonwealth record; and d. the entity is not required…to retain the information the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.	**Efficient and Integrated Data Destruction** Data sanitisation is the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. By implementing Blancco data erasure solutions across the full data lifecycle, organisations can confidently meet and exceed data destruction requirements. With flexible deployment options, automated workflows, and centralised reporting and management, Blancco solutions facilitate efficient and compliant data destruction practices in even the largest organisations.
Australian Privacy Principles Guidelines **Destroying Personal Information—Irretrievable Destruction** 11.36. Personal information is destroyed when it can no longer be retrieved. The steps that are reasonable for an organisation to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form. 11.37. For example, for personal information held: • in electronic form, reasonable steps will vary depending on the kind of hardware used to store the personal information. In some cases, it may be possible to 'sanitise' the hardware to completely remove stored personal information. For hardware that cannot be sanitised, reasonable steps must be taken to destroy the personal information in another way, such as by irretrievably destroying it… • on a third party's hardware, such as cloud storage, where the organisation has instructed the third party to irretrievably destroy the personal information, reasonable steps would include taking steps to verify that this has occurred **De-Identifying Personal Information** 11.44. …Where it is not possible for the risk of re-identification to be appropriately minimised, the organisation could instead consider taking reasonable steps to destroy the personal information….	**Irretrievable Destruction** When attempting to remove individual files, many data destruction methods simply remove the pointers to the file, rather than the file itself. The data is still on the machine, though not easily available to the operating system or the apps that created it. In other cases, 'file shredding' may overwrite the file, but it's unclear whether the overwriting process has been successful. Even a full reformat of a device can leave data behind. Often, this information can be recovered through keyboard methods or the assistance of forensic tools. Blancco data erasure solutions have been tested, certified and approved by more than 15+ government agencies and industry bodies around the world, and is the only company able to erase all types of devices (including files, folders, LUNs and virtual volumes) via a single, centrally-managed cloud-based or on-premise solution. Blancco LUN also enables secure data erasure on public cloud storage platforms such as AWS and Azure. Enterprises may choose from more than 25 data erasure standards, including the globally recognised NIST Clear and Purge levels, before reusing, reselling, recycling or physically destroying data storage assets. In case destruction of personal information is outsourced, secure data erasure can be executed on-premise before transferring media to a third-party vendor. This minimises human errors and chain of custody risks because data is removed before assets leave the premises.

Following the ISM Framework

Blancco provides the only solution that can erase data in both active and inactive environments, and across a variety of IT assets, from mobile phones to large, virtualised data centres, and provide proof that it's been done correctly. Blancco software meets the highest standards for secure data erasure in accordance with privacy and security regulations across the globe. Blancco data erasure solutions support 25+ erasure standards, such as AGISM, NIST Clear and NIST Purge, DoD and more.

ISM GUIDELINES FOR ICT EQUIPMENT MANAGEMENT

REQUIREMENTS	HOW BLANCCO HELPS
Off-Site Maintenance and Repairs Organisations choosing to have ICT equipment maintained or repaired off-site can sanitise the ICT equipment prior to transport, and subsequent maintenance or repair activities, to lower (depending on the types of media involved) its physical transfer and storage requirements. **ICT Equipment Sanitisation and Disposal** When disposing of ICT equipment, any media in the ICT equipment should be sanitised in situ or removed and sanitised separately. [Once sanitised,] the ICT equipment can then be declassified and formally authorised for release into the public domain. However, if media cannot be sanitised or removed, the ICT equipment will need to be destroyed in its entirety. Media typically found in ICT equipment includes: • electrostatic memory devices, such as laser printer cartridges used in multifunction devices (MFDs) • non-volatile magnetic memory, such as hard disks • non-volatile semiconductor memory, such as flash cards and solid-state drives • volatile memory, such as random-access memory sticks.	**Secure, On-Site IT Asset Erasure Before Repairs or Disposal** Onsite maintenance and repairs are highly recommended to ensure that data remains secure. However, in case of off-site maintenance, embedded or attached storage media (HDD, SSD, flash media, etc.) and devices may be securely erased before sending equipment off premise for maintenance. This prevents sensitive data from leaving the security of your network infrastructure. In case of RMA hard disks, Blancco's high-speed, industrial-grade hardware solutions, Blancco 8-Bay Eraser and 24-bay appliances can facilitate secure data erasure for multiple drives across a wide range of drive types before returning assets to the vendor. Onsite erasure mitigates the risk of lost or stolen devices and ensures that data is never retrievable from drive fragments. Unfortunately, our research shows that over a third of all organisations use inappropriate methods such as formatting, overwriting with free tools or other ineffective data removal methods. Blancco's suite of data erasure software enables permanent and secure data sanitisation across end-of-life mobile phones, loose and embedded drives, servers, removable media and other hardware including hard disks, flash cards and solid-state drives.

ISM GUIDELINES FOR MEDIA

Australian Government ISM Guidelines for Media Sanitisation are fulfilled by several Blancco data erasure solutions, including Common Criteria Certified Blancco Drive Eraser. Blancco Drive Eraser 6.9.1 is certified by Common Criteria (EAL2) for secure data erasure on both HDDs and SSDs. For a detailed look at how Blancco Drive Eraser equips Australian organisations to follow ISM media sanitisation recommendations, see our solution brief, Blancco Drive Eraser Certified for Government Use in Australia and New Zealand.

Why Blancco?

For over 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as the Australian Privacy Act and guidelines such as those in the ISM. We support the need for governments and private businesses to stay compliant with these regulations, providing data erasure solutions that satisfy (and often exceed) those requirements across the widest range of media available.

> Contact us today for a **Free Data Erasure Trial for Enterprises**, and see how Blancco solutions equip you to fulfil your data privacy and protection obligations.