

How Blanco Helps Organisations Comply with Australian Privacy Regulations

What's Inside...

An Overview of Australian Data Privacy Act and ISM Requirements

Additional Data Destruction Considerations

Penalties

How Blanco Can Help

Privacy Act Compliance

ISM Compliance

Why Blanco?

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 Privacy Act 1988 (Privacy Act)

The Privacy Act applies primarily to large organisations (\$3+ million annual turnover) and Australian 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.

Australia has significantly enhanced its data privacy laws with the Privacy and Other Legislation Amendment Act 2024, which received Royal Assent on 10 December 2024. This marks the most substantial reform to Australia's privacy regime since the Privacy Act. The Act introduces new compliance obligations, expands regulatory enforcement powers, and imposes stricter penalties, reinforcing the importance of robust data protection practices for organisations handling personal data.



For organisations, compliance is no longer just about preventing breaches, it is about ensuring accountability, transparency, and responsible data handling. The amendments reflect Australia's commitment to aligning with global privacy frameworks, such as the EU's GDPR, and strengthening privacy protections against emerging risks from AI, cyber threats, and cross-border data transfers.

Organisations must now take a proactive stance to identify and mitigate privacy risks before they materialise.

Key Updates from the 2024 Amendments

1. Tort of Serious Invasion of Privacy

For the first time in Australia, individuals now have a legal right to sue for privacy invasions. If an entity intentionally or recklessly invades an individual's privacy by intruding upon their seclusion or misusing personal data, the affected individual can claim damages. Courts will also weigh public interest considerations (e.g., freedom of expression, public health) when determining liability. Legal exemptions apply to journalists, law enforcement, and intelligence agencies, provided they act in good faith. Damage caps for non-economic loss and exemplary damages are aligned with Australian defamation law. Effective date: 10 June 2025 (latest).

2. Children's Online Privacy Code

Australia is introducing a Children's Online Privacy Code to strengthen protections for minors in the digital space. The Office of the Australian Information Commissioner (OAIC) is responsible for developing the code, which will apply to social media platforms, online services, and digital applications accessed by children.

Organisations must comply with new obligations, including:

- ✓ **Prohibition on Targeted Advertising:** Businesses are restricted from using children's data for targeted marketing or behavioral profiling.
- ✓ **Parental Consent Requirements:** Organisations must obtain verifiable parental consent before collecting, processing, or sharing a child's personal data.

- ✓ **Transparency in Data Practices:** Digital platforms must clearly disclose how children's data is collected, used, and stored, ensuring compliance with the Australian Privacy Principles (APPs) and additional child-specific protections.

The new code aligns with global best practices in children's online privacy and will impose stricter compliance requirements on businesses operating in Australia. Once enforced, organisations will need to update their privacy frameworks to meet enhanced obligations under the Privacy Act.

3. Automated Decision-Making Transparency Requirements

Organisations using AI-driven decision-making must ensure transparency and explainability in automated processes. This includes notifying individuals when an AI system makes a decision that could impact them and providing detailed records of how their data was used in automated decisions. These measures align with global concerns over AI ethics and discriminatory decision-making. Grace period: Until 10 December 2026.

4. Expanded Powers for the OAIC

The OAIC now has expanded investigative and enforcement powers, including the ability to issue compliance notices, conduct unannounced audits, and impose tiered financial penalties for privacy violations. The OAIC has greater control over data breach enforcement and corporate privacy failures, increasing regulatory scrutiny and requiring businesses to be audit-ready at all times.

5. Overseas Data Transfers – New 'Whitelist' Rules

Australia has introduced a 'whitelist' system for international data transfers. Organisations may only transfer personal data to approved jurisdictions with equivalent privacy protections. The Australian Government will assess whether a country's laws provide substantially similar protection as Australia's Privacy Act. The approval list will reduce compliance burdens for transfers to trusted jurisdictions, mirroring the EU's GDPR adequacy decisions. This change streamlines global data transfers but imposes new due diligence obligations for companies relying on offshore data processing.

6. Criminalisation of Doxxing

Australia is among the first countries to criminalise doxxing—the malicious release of personal data with the intent to harass, intimidate, or endanger individuals. The law applies broadly, with no exemptions for small businesses or journalists, requiring companies to strengthen access controls and prevent misuse of sensitive personal data.

7. Strengthening Security Under the Privacy Act

The new APP 11.3 requires organisations to implement both technical and organisational safeguards to protect personal data. Compliance measures include comprehensive staff training on privacy and cybersecurity risks, formal governance frameworks for data security, regular audits and vulnerability assessments, and proactive risk management strategies to mitigate data breaches. This change moves beyond IT security and introduces mandatory governance and training requirements.

8. OAIC's Expanded Powers and Compliance Audits

The OAIC can now impose civil penalties for administrative failures such as failure to implement adequate security measures, non-compliant privacy policies, and failure to inform individuals of direct marketing opt-outs. With increased regulatory scrutiny, companies must maintain detailed compliance documentation and be prepared for heightened enforcement activity.

9. Data Breach Response and Government Oversight

In the event of a large-scale data breach, the Australian Government now has the authority to mandate data-sharing between businesses and government agencies to prevent widespread harm. Organisations should update incident response plans to align with new regulatory expectations, implement data-sharing mechanisms for crisis management, and prepare for real-time coordination with government agencies in major breaches.



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, the 'Guide to Securing Personal Information', published by the 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, the 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.

With the 2024 amendments, penalties for noncompliance with the Privacy Act have increased significantly. The OAIC has been granted broader enforcement powers, including the ability to impose heavier financial penalties on organisations that violate privacy laws.

The revised penalties now stand at the greater of:

- ✓ \$50 million, or
- ✓ Three times the benefit obtained from the misuse of information, or
- ✓ 30% of an organisation's annual adjusted turnover in the relevant period.¹

¹ For further information: <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments>

How Blanco 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.

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

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

- ✓ **Blanco 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), Blanco File Eraser can target and erase files on computers and servers on both UNIX and Windows operating systems.
- ✓ **Blanco Drive Eraser.** Blanco Drive Eraser securely erases all data on enterprise laptops and desktops, as well as servers, storage systems, and loose drives, including NVMe and self-encrypting drives.

- ✓ **Blanco Mobile Diagnostics & Erasure.** If sensitive information is identified on mobile devices or tablets, Blanco 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.
- ✓ **Blanco LUN Eraser and Blanco Virtual Machine Eraser.** For data stored temporarily on virtual volumes or machines, on-premise or in the cloud, Blanco Virtual Machine Eraser and Blanco LUN Eraser can be used together or separately to target relevant data in active storage environments while allowing the operating system to remain intact.
- ✓ **Blanco 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 the 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 to the Blanco 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 BLANCO HELPS
<p>Subdivision D—Dealing with credit reporting information, etc.</p> <p>20J Destruction of pre-screening assessment</p> <ol style="list-style-type: none"> 1. If an entity has possession or control of a pre-screening assessment, the entity must destroy the assessment if: <ol style="list-style-type: none"> 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. <p>Subdivision E—Integrity of Credit Information and Credit Eligibility Information</p> <p>21S Security of credit eligibility information</p> <ol style="list-style-type: none"> 1. (1) If: <ol style="list-style-type: none"> 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. 	<p>Secure Folder & File-Level Data Erasure</p> <p>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), Blanco File Eraser can target and erase files on computers and servers manually or automatically on both UNIX and Windows operating systems.</p> <p>Blanco 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.</p> <p>While typical file shredding or wiping software may delete some data, Blanco 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.</p> <p>Blanco 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.</p> <p>Blanco 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.</p>

² Blanco File Eraser 8.2

PART IIIA—CREDIT REPORTING continued

REQUIREMENTS	HOW BLANCCO HELPS
<p>Subdivision G—Dealing with credit reporting information after the retention period ends</p> <p>20V Destruction etc. of credit reporting information after the retention period ends</p> <p>This section applies if:</p> <ol style="list-style-type: none"> a credit reporting body holds credit information about an individual; and the retention period for the information ends. <p>Destruction etc. of credit information</p> <p>The credit reporting body must destroy the credit information, or ensure that the information is de-identified, within 1 month after the retention period...</p> <p>[Blanco 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.]</p>	<p>Verified Data Sanitisation for Out-of-Retention Data Across All Data Storage Assets</p> <p>Blanco data erasure solutions enable automatic data erasure according to an organisation's retention policy requirements. Blanco File Eraser supports scripting and scheduling to erase qualified data on a regular, ongoing basis. Used with Blanco Management Portal, a central operations and reporting dashboard for all Blanco erasure products, this process minimises unnecessary data while documenting what erasures have occurred. Blanco File Eraser is also supported by Blanco Virtual Machine Eraser and Blanco LUN Eraser, erasing data centre virtual machines and logical unit numbers all the way down to individual files and folders on the desktop.</p> <p>For entire drives storing out-of-retention data, Common Criteria-Certified Blanco 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. Blanco Drive Eraser also supports erasure of self-encrypting drives. ISM Guidelines for Media: Media sanitisation includes more details on media sanitisation guidance that the Blanco Drive Eraser fulfils.</p>
<p>20Y Destruction of credit reporting information in cases of fraud</p> <p>Destruction of credit reporting information</p> <ol style="list-style-type: none"> The credit reporting body must: <ol style="list-style-type: none"> destroy the credit reporting information; and within a reasonable period after the information is destroyed: <ol style="list-style-type: none"> give the individual a written notice that states that the information has been destroyed and sets out the effect of subsection (4.); and give the credit provider a written notice that states that the information has been destroyed. Subsection (2.) does not apply if the credit reporting body is required...to retain the credit reporting information. 	<p>Centralised Erasure, Reporting & Communication</p> <p>Please also see 'Secure Folder & File-Level Data Erasure'.</p> <p>Used with Blanco Management Portal, Blanco 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.</p> <p>With Blanco Management Portal, 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.</p> <p>Reports may be stored, managed, and accessed at any time in the Blanco Management Portal, available in on-premise or as a cloud service hosted by AWS.</p>

³ Blanco 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 'Blanco 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
<p>20Z Dealing with information if there is a pending correction request etc.</p> <p>Direction to destroy information etc.</p> <p>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.</p> <p>7. If the Commissioner gives a direction under subsection (6.) to the credit reporting body, the body must comply with the direction.</p>	<p>Secure, Complete & Permanent Data Destruction</p> <p>Whether data is located on local devices, in the cloud, or in virtual or logical storage, Blanco data erasure 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.</p> <p>Each Blanco 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.</p>

AUSTRALIAN PRIVACY PRINCIPLE 11—SECURITY OF PERSONAL INFORMATION

REQUIREMENTS	HOW BLANCCO HELPS
<p>Schedule 1—Australian Privacy Principles</p> <p>Part 4—Integrity of personal information</p> <p>11.2 If:</p> <ul style="list-style-type: none"> 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 <p>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.</p>	<p>Efficient & Integrated Data Destruction</p> <p>Data sanitisation is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable.</p> <p>By implementing Blanco 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, Blanco solutions facilitate efficient and compliant data destruction practices in even the largest organisations.</p>

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

AUSTRALIAN PRIVACY PRINCIPLE 11—SECURITY OF PERSONAL INFORMATION continued

REQUIREMENTS	HOW BLANCCO HELPS
<p>Australian Privacy Principles Guidelines</p> <p>Destroying Personal Information—Irretrievable Destruction</p> <p>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.</p> <p>11.37. For example, for personal information held:</p> <ul style="list-style-type: none"> ✓ 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 <p>De-Identifying Personal Information</p> <p>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...</p>	<p>Irretrievable Destruction</p> <p>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.</p> <p>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.</p> <p>Blanco data erasure solutions have been tested, certified, and approved by more than 13+ 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. Blanco LUN Eraser also enables secure data erasure on public cloud storage platforms such as AWS and Azure.</p> <p>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.</p> <p>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.</p>



Following the ISM Framework

Blanco software meets the highest standards for secure data erasure in accordance with privacy and security regulations across the globe. Blanco 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
<p>SOff-Site Maintenance and Repairs</p> <p>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.</p> <p>ICT Equipment Sanitisation and Disposal</p> <p>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.</p> <p>Media typically found in ICT equipment includes:</p> <ul style="list-style-type: none"> ✔ 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. 	<p>Secure, Onsite IT Asset Erasure Before Repairs or Disposal</p> <p>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.</p> <p>In case of RMA hard disks, Blanco's high-speed, industrial-grade hardware solutions, Blanco 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.</p> <p>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.</p> <p>Blanco'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.</p>

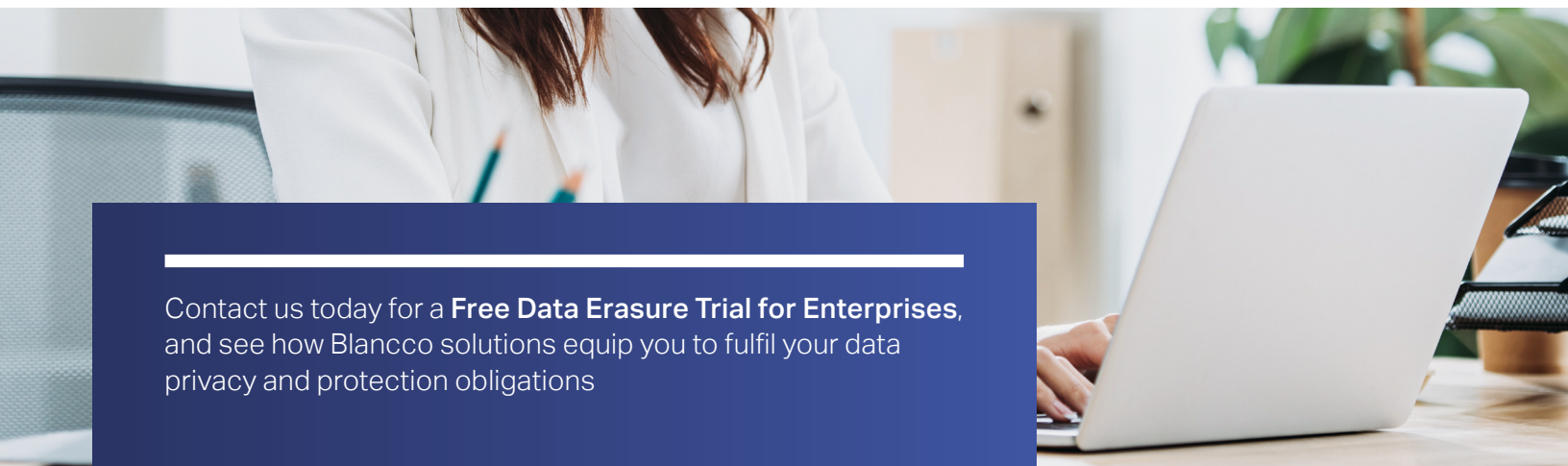
ISM guidelines for media

Australian Government ISM Guidelines for Media Sanitisation are fulfilled by several Blanco data erasure solutions, including Common Criteria-Certified Blanco Drive Eraser. Blanco Drive Eraser 6.9.1 and Blanco Drive Eraser 7.3.1 are certified by Common Criteria (EAL2) for secure data erasure on both HDDs and SSDs. For a detailed look at how Blanco Drive Eraser equips Australian organisations to follow ISM media sanitisation recommendations, see our solution brief, Blanco Drive Eraser Certified for Government Use in Australia and New Zealand.



Why Blanco?

For over 20 years, Blanco 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 Blanco solutions equip you to fulfil your data privacy and protection obligations