



When it comes to data privacy, organizations in New Zealand are guided by the Privacy Act 2020. The 2020 Act replaces and repeals the 1993 legislation which has lasted almost three decades.

Below, we've mapped requirements from the Privacy Act 2020 to Blanco 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 organization.

New Zealand Privacy Act (NZPA) 2020 <http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html>

REQUIREMENTS	HOW BLANCCO HELPS
<p>Information privacy principle 9</p> <p>Agency not to keep personal information for longer than necessary</p> <p>An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.</p>	<p>Blanco Data Erasure Solutions offer data erasure across the entire data lifecycle, with the ability to erase all active and inactive data across the widest variety of IT asset, including live environments (selective files, virtual environment, cloud storage, etc.)</p> <p>With Blanco, you can dispose of, reuse or resell IT assets (including mobile phones, tablets, laptops, desktops and flash storage devices) with no risk of data recovery by ensuring data has been certifiably erased.</p>
<p>Schedule 6. Information matching rules:</p> <p>5. Destruction of information:</p> <ol style="list-style-type: none"> 2. Information matching information held by an agency that does not reveal a discrepancy must be destroyed as soon as practicable by the agency. 3. An agency that holds information matching information that reveals a discrepancy must destroy that information within 60 working days after becoming aware of the discrepancy unless the agency decides to take adverse action against any individual on the basis of that discrepancy. 4. An agency that decides to take adverse action against any individual on the basis of a discrepancy must destroy the information as soon as practicable after the information is no longer required. 	<p>Blanco active erasure solutions, including Blanco File, Blanco LUN and Blanco Virtual Machine, securely erase data in active environments when it is no longer needed. This increases data erasure compliance, lessening downtime and lessening the impact on your business when a cyber breach does occur by limiting the attack surface. This can be done either manually or, to better ensure that data management policies are followed at end-of-life, set up to be conducted automatically according to specific parameters (e.g., by file type, date, or other configurations).</p> <ul style="list-style-type: none"> • For PCs, laptops, and servers, Blanco File Eraser can securely erase sensitive files and folders • Blanco LUN Eraser allows organizations to erase data in active storage environments while allowing the operating system to remain intact. LUNs are immediately available for reuse after erasure. • Blanco Virtual Machine Eraser allows organizations to automatically destroy all data when virtual machines are no longer needed.

REQUIREMENTS	HOW BLANCCO HELPS
<p>Schedule 8. Basic principles of national application set out in Part Two of OECD Guidelines: Individual participation principle</p> <p>An individual should have the right:</p> <ul style="list-style-type: none"> d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. 	<p>Blancco File Erasure ensures full compliance with 'right to erasure' requirements by automating data erasure routines that selectively erase data on active PCs, laptops and servers.</p> <p>Blancco File Eraser supports the erasure of any and all files that contain personal data. Blancco File seamlessly integrates with Active Directory and allows remote, automated data erasure routines.</p>

Information privacy principles descriptions and examples of breaches of the Information Privacy Principles, New Zealand Government

https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/GCPO/Information-privacy-principles.pdf

PRINCIPLES	HOW BLANCCO HELPS
<p>Principle 9. If the information is to be destroyed, do your processes ensure:</p> <ul style="list-style-type: none"> • Personal information is de-identified where appropriate? • Shredders and/or secure destruction services are used? • Hard drives of computers, photocopiers, phones, etc. are securely erased before sale or decommission? • Back-up files, as well as originals, are deleted? 	<p>Blancco Data Eraser Solutions offer data erasure across the entire data lifecycle, with the ability to erase all active and inactive data across every type of IT asset, including live environments.</p> <p>With Blancco, you can dispose of, reuse or resell IT assets (including mobile phones, tablets, laptops, desktops, and flash storage devices) with no risk of data recovery by ensuring assets and/or specific data has been certifiably erased and contain no personal information.</p>
<p>What could be done to reduce the risk?</p> <p>Ensure you have a Disposal Authority in place and implement procedures to ensure that all public records (including personal information) are disposed of in accordance with a General Disposal Authority or an agency-specific Disposal Authority.</p>	<p>The ability to automate and integrate Blancco Data Erasure Solutions gives the Disposal Authority an efficient, secure and auditable data disposal process.</p>
<p>Design systems and processes to record a date of expiry or review (of whether it should be disposed) for personal information that aligns with the business need for it. Many systems have the functionality to apply these dates from the point of collection.</p>	<p>Blancco File Eraser ensures full compliance with 'right to erasure' requirements by automating data erasure routines that selectively erase data on active PCs, laptops and servers.</p> <p>Blancco File Eraser supports the erasure of any and all files that contain personal data. Blancco File seamlessly integrates with Active Directory and allows remote, automated data erasure routines.</p>

PRINCIPLES	HOW BLANCCO HELPS
<p>Put in place an internal policy that:</p> <ul style="list-style-type: none"> • details the requirements for ensuring all personal information is disposed of in a secure and appropriate manner, and • ensures systems/processes are in place to monitor and report compliance with the policy. 	<p>Blanco Data Erasure Solutions allows organizations to easily manage, automate and document data erasure routines according to internal timelines and policies. This helps users reduce errors while enhancing security and meeting compliance. Blanco Management Console allows organizations to manage data erasure across all IT assets within a single program for consolidated reporting, producing a 100-percent certified audit trail.</p> <p>Additionally, Blanco could provide help with gap analysis and Professional Services to establish a well-defined data sanitization policy for organizations.</p>

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.

