

Dataspace Privacy Policy



20260923 Dataspace Privacy Policy_V1.docx

VERSION 1

VERSION DATE: 23 SEPTEMBER 2026
DOCUMENT STATUS: APPROVED



DATASPACE



1. ABOUT THIS POLICY

TREA OpCo Pty Ltd, trading as Dataspace (**Dataspace, we, us or our**), operates a principally colocation data centre business in Australia. We respect your privacy and are committed to complying with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (**APPs**).

This policy explains how we collect, hold, use and disclose personal information, and how you can request access or correction or make a privacy complaint. It applies to our business operations, facilities, websites and services, including our dealings with customer representatives, visitors, suppliers, contractors, job applicants and other individuals.

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not it is true or recorded in a material form. Sensitive information is a category given additional protection by law, including health information, criminal records, biometric information used for automated verification or identification, and biometric templates.

2. CUSTOMER EQUIPMENT AND DATA

Colocation customers control the data on their own equipment. Providing space, power, cooling and physical security does not ordinarily involve us accessing that content. We handle customer contact, billing, support and facility-access information under this policy. Where an agreed service (e.g. remote-hands support or media disposal) requires access, we limit that access to the authorised task.

For requests about information held by a customer, please contact that customer first. If a request concerns information we hold or a service we perform, we will assess our responsibilities and, where appropriate and lawful, assist or coordinate with the customer.

3. COLLECTION OF PERSONAL INFORMATION

We collect only what is reasonably necessary for our functions and activities. This may include:

- Contact and business details: name, employer, role, email, phone and authorised-person status.
- Service and financial records: contracts, orders, billing, support tickets and account history.
- Facility and security records: identity verification, photos, access credentials, biometric information and templates, visitor and vehicle details, entry/exit logs, CCTV footage and incident reports.
- People and safety information: applications, qualifications, work rights, background checks, emergency contacts and health information needed for safety or reasonable adjustments.
- Digital information: IP addresses, device details, website activity and security logs where linked to an identifiable person.

We use personal information to operate our business and perform the functions for which it was collected, including to:

- Respond to enquiries, prepare proposals, establish and administer customer or supplier relationships, provide services, process payments and resolve disputes.
- Verify identities and authorisations, manage visitors, deliveries and contractors, administer inductions and protect people, facilities, equipment and systems.
- Provide support, coordinate authorised work and communicate about maintenance, service changes, outages, safety and security incidents.
- Recruit and engage personnel, check suitability for relevant roles or access, and manage workplace health, safety and accessibility.
- Maintain and improve our websites, services and business systems, investigate misuse, manage risk, conduct audits and meet legal obligations.



- Send relevant business updates or marketing where permitted, subject to the choices described in this policy.

We may collect sensitive information regarding individuals, including but not limited to health information, criminal records, biometric information used for automated verification or identification, and biometric templates. Dataspace will only collect sensitive information in circumstances where it is reasonably necessary to do so for one or more of the services we provide or functions we carry out and the relevant individual consents to the collection of the information or we are required or authorised by law to collect the sensitive information.

Dataspace will, if it is reasonable or practicable to do so, collect directly from you through enquiries, contracts, forms, email, phone, online services, recruitment and facility visits. CCTV and access-control systems also collect information when used.

Where direct collection is impracticable, we may collect from your employer, a sponsoring customer, recruitment agencies, referees, public sources or screening providers. We obtain consent for sensitive information unless a legal exception applies.

At or before collection, or as soon as practicable afterwards, we take reasonable steps to explain the relevant circumstances, purposes, usual disclosures and consequences of not providing information. Specific collection notices, including visitor and biometric-enrolment notices, supplement this policy. Publishing this policy does not itself constitute consent. We do not adopt government-related identifiers as our own identifiers, or use or disclose them, except as permitted by law.

If we receive information we did not request, we assess whether we could lawfully have collected it. If not, we destroy or de-identify it as soon as practicable where lawful and reasonable, subject to the rules for Commonwealth records.

Individuals may choose to deal with Dataspace anonymously or under a pseudonym where lawful and practical. Where anonymity or use of a pseudonym will render us unable to provide the relevant service or do business, we may request that an individual identify him or herself.

4. CCTV AND BIOMETRIC ACCESS CONTROLS

We use CCTV and biometric access controls to protect people, equipment and facilities and to manage authorised entry. Surveillance is limited to appropriate areas with notices as required by law.

Before biometric enrolment we explain the technology, information collected, purposes, storage, retention and available alternatives. We obtain express, informed and voluntary consent. Site entry or acceptance of this policy alone is not consent. If you do not consent or later withdraw, contact site security or our Privacy Officer to arrange a reasonable alternative. Access may be restricted if identity requirements cannot otherwise be met lawfully.

Biometric systems compare a presented biometric sample with an enrolled reference to support access decisions. Access also depends on applicable authorisations and security rules. If verification fails or you dispute an access outcome, ask site security for human review. We restrict access to biometric records, protect them according to their sensitivity and do not use them for marketing.

5. WHO WE SHARE INFORMATION WITH

We limit disclosures to information appropriate for the relevant purpose. Depending on the circumstances, recipients may include:



- Your employer, the customer sponsoring your access, or your authorised representative, for access administration, service delivery or relevant incident investigation. We limit disclosure of CCTV and access records to what is justified and protect other people's information.
- Providers supporting our operations, including security and access-control providers, IT and cloud services, communications and website providers, payment services, recruitment and screening providers, maintenance contractors and secure-disposal providers.
- Our related bodies corporate, owners including Next Capital, and their advisers, where reasonably necessary and lawfully permitted for governance, risk management, financing or a business transaction. Ownership does not give unrestricted access to personal information or customer content.
- Professional advisers, auditors, insurers and financiers, and prospective purchasers or investors and their advisers in a proposed transaction, subject to appropriate confidentiality and disclosure limits.
- Regulators, courts, law enforcement or emergency services where required or authorised by law, and others where you authorise disclosure or a lawful exception applies.

We apply appropriate contractual, confidentiality and security requirements to service providers handling personal information for us. We use de-identified or aggregated information for reporting where it meets the purpose. We do not sell personal information or provide it to other organisations for their own marketing without your express consent.

6. OVERSEAS HANDLING

Some of our service providers may store or process personal information outside Australia, and we may disclose personal information to overseas recipients in connection with cloud services, technology support and other business services. The locations of these recipients may vary depending on the services used and, where it is not practicable to identify particular countries, may include locations in North America, Europe and the Asia-Pacific region.

Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure the recipient handles the information in accordance with applicable Australian privacy requirements, unless an exception under the Privacy Act applies.

7. WEBSITES COOKIES AND ONLINE SERVICES

Our websites and online services may use cookies and similar technologies for functionality, security, preferences, usage measurement and service improvement. These technologies may collect online identifiers and browsing activity that are personal information, including when linked with other records.

Where we use optional analytics or advertising technologies, we explain their purposes and relevant third-party disclosures through the applicable website notice and obtain consent where required. We do not treat browsing alone as consent to uses that require consent. You can manage cookies through your browser and any controls provided on the website; disabling some cookies may affect functionality.

Other organisations' websites, platforms and services have their own privacy practices. Please check their privacy notices when following a link or providing information directly to them.

8. MARKETING COMMUNICATIONS

We may contact you about our services and events where permitted by the APPs, the *Spam Act 2003* (Cth) and applicable telemarketing rules. We do not use sensitive information for direct marketing without consent.



You may opt out at any time by using the unsubscribe facility or emailing privacy@dataspace.com.au. We process electronic unsubscribe requests within five working days. Opting out does not affect service, safety or security communications.

9. SECURITY AND RETENTION

We hold information electronically in our systems and those of service providers, and where necessary in physical records. We take reasonable technical and organisational measures to protect it against misuse, interference, loss and unauthorised access, modification or disclosure.

Measures are proportionate to the information and risks, and include restricted physical access, role-based system access, authentication, secure transfer and storage, monitoring, staff training, supplier controls and incident-response processes. Access is limited to people who need it for an authorised purpose. No security measure can guarantee complete protection.

We retain information only while needed for a permitted purpose or to meet a legal retention obligation. We take reasonable steps to destroy or de-identify information when it is no longer needed and no retention exception applies.

CCTV, visitor records, access logs and biometric records have retention rules appropriate to their purpose and sensitivity. We review the need to retain biometric information when access ends or consent is withdrawn, and remove it when no lawful basis for retention remains. Copies retained for an incident or legal hold are restricted and reviewed. Backup copies remain protected and are removed through controlled retention and disposal processes.

10. ACCESS AND CORRECTION

You may request access to, or correction of, personal information we hold about you by contacting our Privacy Officer. We may reasonably verify your identity and any representative's authority. We take reasonable steps to keep information accurate, up to date and complete, and relevant to its use or disclosure.

We respond within a reasonable period and aim to do so within 30 days. If more time is needed, we explain why and provide an expected response date. There is no fee to make a request or for correction. If we propose a reasonable, non-excessive charge for providing access, we explain it in advance.

Access or correction may be refused only where permitted by law. We provide written reasons, except where it would be unreasonable to do so, and explain how to complain.

You may also ask us to associate a correction statement with declined corrections, or to delete information, we assess deletion requests against our retention obligations.

11. PRIVACY COMPLAINTS

If you believe there has been a breach of the APPs, you are entitled to complain to us. Please direct any complaints to our privacy contact below. We will investigate your complaint and endeavour to resolve it.

If you consider that we have not dealt with your complaint adequately, you may complain to the Office of the Australian Information Commissioner on the below details:

Post: Office of the Australian Information Commissioner (OAIC)
GPO Box 5218
SYDNEY NSW 2001



Email: enquiries@oaic.gov.au

Telephone: 1300 363 992

12. CONTACT US

To contact us about any privacy or data matter or to notify us that you wish to be removed from our distribution lists, please either post or email:

Privacy Officer

Dataspace | TREA OpCo Pty Ltd

Email: privacy@dataspace.com.au

Post: Level 12, 143 Macquarie Street, Sydney NSW 2000, Australia

13. EMPLOYEES AND POLICY REVIEW

Some acts or practices directly related to a current or former employment relationship and an employee record may be exempt from the *Privacy Act*. This exemption does not generally cover contractors or unsuccessful applicants.

We review this policy at least annually and following material changes to our operations or the law. The current version is available on our website and from our Privacy Officer.