



Data Processing Agreement

Deep Space platform and DS Site

Supplier	Deep Space Trading Pty Ltd
ABN	65 669 436 373
Parent entity	Deep Space Holdings Pty Ltd
Registered office	Level 4, Suite 30, 50-56 Sanders Street, Upper Mount Gravatt QLD 4122, Australia
Jurisdiction of incorporation	Australia
Contact	sales@deepspacegroup.ai deepspacegroup.ai
Version	1.0
Privacy contact	privacy@deepspacegroup.ai
Published at	deepspacegroup.ai/dpa
Effective date	As set out in the Agreement

1. Parties and application

1.1 This Data Processing Agreement (DPA) is published by Deep Space Trading Pty Ltd ABN 65 669 436 373, a company incorporated in Australia of Level 4, Suite 30, 50-56 Sanders Street, Upper Mount Gravatt QLD 4122 (Deep Space). It applies between Deep Space and the entity identified as the customer in the Agreement (the Customer), and is incorporated into the Agreement by reference. No separate signature is required.

1.2 This DPA forms part of, and is subject to, the agreement between the parties for the supply of the Deep Space platform and DS Site (the Agreement), comprising the Purchase Terms and the Supply Terms.

1.3 This DPA applies to the extent Deep Space Processes Personal Information on behalf of the Customer in connection with the Services.

1.4 Where there is any inconsistency in relation to the Processing of Personal Information, this DPA prevails over both the Purchase Terms and the Supply Terms, except where a Special Condition in the Purchase Terms expressly refers to this DPA and gives the Customer greater protection. For all other purposes the order of precedence in the Agreement applies.

1.5 This DPA takes effect on the commencement date of the Agreement and continues while Deep Space Processes Personal Information for the Customer.

2. Definitions

Terms not defined here have the meaning given in the Agreement.

- Privacy Laws means the Privacy Act 1988 (Cth) and the Australian Privacy Principles, and, where the Customer or the individuals concerned are in New Zealand, the Privacy Act 2020 (NZ) and the Information Privacy Principles, together with any other data protection law applicable to a party in respect of the Processing.
- Customer Data means all data and documents the Customer or its Users upload to, generate in, or transmit through the Services.
- Personal Information has the meaning given in the Privacy Act 1988 (Cth), and includes personal information as defined in the Privacy Act 2020 (NZ), and forms part of the Customer Data.
- Processing means any operation performed on Personal Information, including collection, storage, use, disclosure, access, alteration, transmission and deletion.
- Eligible Data Breach has the meaning given in Part IIIC of the Privacy Act 1988 (Cth), and includes a notifiable privacy breach under Part 6 of the Privacy Act 2020 (NZ).
- Data Breach means unauthorised or accidental access to, disclosure of, alteration of, loss of, or destruction of Personal Information, whether or not it amounts to an Eligible Data Breach.
- Sub-processor means a third party engaged by Deep Space to Process Personal Information in connection with the Services.
- Services means the Deep Space platform, DS Site, and related implementation and support services supplied under the Agreement.
- Users means the individuals the Customer authorises to access the Services.

3. Roles of the parties

3.1 As between the parties, the Customer determines the purposes and means of the Processing of Personal Information in the Services. Deep Space Processes that Personal Information only on the Customer's behalf and on its instructions.

3.2 The Customer is responsible for the accuracy and lawfulness of the Personal Information it uploads, and for giving any notices and obtaining any consents required under the Privacy Laws to permit Deep Space to Process it as contemplated by the Agreement. This includes Personal Information about the Customer's subcontractors, suppliers, consultants and site personnel.

3.3 Deep Space acts on its own behalf, not the Customer's, in relation to account administration, billing, and Personal Information collected directly from the Customer's personnel in the course of Deep Space's own business. That Processing is governed by the Deep Space Privacy Policy, not this DPA.

4. Instructions

4.1 Deep Space will Process Personal Information only:

- in accordance with the Customer's documented instructions, which include the Agreement, this DPA, and the Customer's configuration and use of the Services;
- as necessary to provide, maintain, secure and support the Services; and
- as required by applicable law, in which case Deep Space will notify the Customer before Processing unless legally prohibited from doing so.

4.2 Deep Space will not sell Personal Information and will not Process it for its own marketing or profiling purposes.

4.3 Deep Space will not use Customer Data to train public, shared or third party artificial intelligence models, and will not permit its Sub-processors to do so. Where Deep Space uses artificial intelligence infrastructure to generate an output for the Customer, that Processing occurs within the Customer's tenancy and solely to produce the requested output.

4.4 If Deep Space considers an instruction would breach the Privacy Laws, it will notify the Customer promptly and may suspend that element of the Processing until the instruction is amended or confirmed.

5. Details of Processing

The subject matter, nature, purpose, duration, categories of individual and types of Personal Information are set out in Annexure A.

6. Confidentiality and personnel

6.1 Deep Space will treat Personal Information as confidential information of the Customer.

6.2 Deep Space will limit access to personnel who need it to perform the Agreement, ensure those personnel are subject to written confidentiality obligations that survive their engagement, and provide privacy and security awareness training to personnel with access.

6.3 Deep Space operates role based access control, reviews access rights periodically, and revokes access promptly when personnel change role or leave.

7. Security

7.1 Deep Space will implement and maintain the technical and organisational measures in Annexure B, having regard to the state of the art, the cost of implementation, the nature and scope of the Processing, and the risk to individuals, consistent with its obligations under Australian Privacy Principle 11.

7.2 Deep Space maintains an information security management system certified to ISO/IEC 27001:2022 and will maintain that certification, or an equivalent recognised standard, for the term of the Agreement.

7.3 Deep Space will not materially reduce the overall level of protection provided by the measures in Annexure B during the term.

8. Sub-processors

8.1 Deep Space maintains a current list of its Sub-processors, including the purpose of each engagement and the location in which it Processes Personal Information, at deepspacegroup.ai/sub-processors. The Customer authorises Deep Space to engage the Sub-processors on that list as at the commencement date of the Agreement.

8.2 Where the Customer connects a third party system of its own to the Services, such as its accounting system, that connection operates on the Customer's instruction and the third party is not a Sub-processor of Deep Space.

8.3 Deep Space will impose on each Sub-processor data protection obligations no less protective than those in this DPA, and remains liable to the Customer for its Sub-processors' acts and omissions in relation to Personal Information as if they were its own.

8.4 Deep Space will give the Customer at least 30 days' written notice before appointing a new Sub-processor or materially changing the role of an existing one.

8.5 The Customer may object to a proposed Sub-processor on reasonable grounds relating to the protection of Personal Information within 15 days of notice. The parties will work in good faith to resolve the objection, including by considering alternative configurations. If it cannot be resolved and the Sub-processor is one Deep Space cannot practicably replace without ceasing to supply the Services, either party may terminate the Agreement on 30 days' written notice and the Customer will receive a pro rata refund of prepaid fees for the unexpired period. In any other case the Customer may terminate only the affected Services on the same basis.

9. Location of Processing and cross-border disclosure

9.1 Deep Space is an Australian company and the Services are operated from Australia. Live Customer Data and documents are hosted in Australia. The Deep Space platform is hosted on Google Cloud in the Sydney region and DS Site on Amazon Web Services in an Australian region. Backup copies are replicated to a separate multi-region location, identified on the Sub-processor list, so that no single region holds both the live data and the recovery copy.

9.2 Certain supporting services may Process limited Personal Information outside Australia. The location of each Sub-processor is stated on the Sub-processor list.

9.3 Where Personal Information is Processed outside Australia, Deep Space will take the steps reasonable in the circumstances to ensure the overseas recipient does not breach the Australian Privacy Principles, as required by Australian Privacy Principle 8, including through binding contractual commitments with the Sub-processor.

9.4 Where the Customer or the individuals concerned are in New Zealand, Deep Space acknowledges that the Privacy Act 2020 (NZ) applies to it in respect of that Personal Information irrespective of the governing law of the Agreement, and that its arrangements are intended to satisfy Information Privacy Principle 12.

10. Data Breach notification

10.1 Deep Space will notify the Customer without undue delay, and in any event within 48 hours, of becoming aware of a Data Breach affecting the Customer's Personal Information. Deep Space becomes aware when its security, engineering or support function has confirmed that a Data Breach has occurred, and Deep Space will not delay that confirmation unreasonably.

10.2 The notification will include, so far as known at the time and updated as more is learned:

- the nature of the Data Breach and the categories and approximate number of individuals and records affected;
- its likely consequences;
- the measures taken or proposed to address it and mitigate its effects; and
- a contact point for further information.

10.3 Deep Space will provide reasonable cooperation and assistance to enable the Customer to assess whether a Data Breach is an Eligible Data Breach and to meet its own obligations, including assessment and notification under the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act 1988 (Cth) and, where applicable, Part 6 of the Privacy Act 2020 (NZ).

10.4 Deep Space will not make any public statement identifying the Customer in connection with a Data Breach without the Customer's prior written consent, except where required by law.

10.5 Where both parties hold the affected Personal Information and section 26WE of the Privacy Act 1988 (Cth) permits a single notification, the Customer will make any notification to affected individuals and to the Office of the Australian Information Commissioner, and Deep Space will not do so separately unless the Customer fails to notify within the time required by law or Deep Space is independently compelled to. The parties will consult before either notifies.

11. Assistance to the Customer

11.1 Deep Space will provide reasonable assistance to the Customer, at the Customer's cost where the assistance is material and outside the ordinary operation of the Services, in relation to:

- requests from individuals to access or correct their Personal Information under Australian Privacy Principles 12 and 13, or the equivalent New Zealand principles;
- privacy impact assessments and consultations with a regulator; and

- inquiries, investigations or complaints by the Office of the Australian Information Commissioner, the New Zealand Office of the Privacy Commissioner, or any other regulator.

11.2 If Deep Space receives a request from an individual relating to Personal Information it Processes for the Customer, it will not respond substantively, will refer the individual to the Customer, and will notify the Customer promptly.

11.3 The Services allow the Customer to access, correct, export and delete Personal Information directly, and the Customer will use those functions in the first instance.

12. Audit and assurance

12.1 Deep Space will make available to the Customer, on reasonable written request, information reasonably necessary to demonstrate compliance with this DPA, including:

- its current ISO/IEC 27001 certificate and Statement of Applicability;
- the executive summary of its most recent independent penetration test, subject to confidentiality undertakings; and
- responses to a reasonable written security questionnaire.

12.2 Where that information is not sufficient to demonstrate compliance, and the Customer has reasonable grounds to believe a material breach of this DPA has occurred, the Customer may request an audit. Any audit will be at the Customer's cost, on at least 30 days' notice, during business hours, no more than once in any 12 month period, subject to confidentiality undertakings, and conducted so as not to disrupt the Services or affect the data of other customers.

12.3 Deep Space may object to a proposed auditor that is a competitor of Deep Space or is not suitably qualified or independent.

13. Return and deletion

13.1 During the term the Customer may export Customer Data, including Personal Information, from the Services.

13.2 On expiry or termination, Deep Space will provide a structured export of all Customer Data and documents in a machine-readable format at no additional cost.

13.3 Deep Space will not restrict, withhold, encrypt against or disable the Customer's access to its Customer Data during the term. This does not limit Deep Space's right to suspend the Services under clause 5.8(c) of the Supply Terms, and where the Services are suspended for non-payment under clause 5.8(c)(iii) Deep Space will still provide the Customer with a structured export of its Customer Data on request.

13.4 Following delivery of the export, and after 30 days during which the Customer may request a further copy, Deep Space will delete or de-identify the Personal Information it holds, except where required by Australian law to retain it or where it exists in routine backups.

13.5 Personal Information in backups will be deleted on the ordinary backup retention cycle and remains subject to this DPA until deleted.

13.6 The obligations in clauses 13.1 to 13.3 are intended to operate for the Customer's benefit on and after any insolvency event affecting Deep Space, to the extent permitted by law, and Deep Space will not assert any lien or set-off over Customer Data.

14. Liability

14.1 Each party's liability under or in connection with this DPA is subject to the limitations and exclusions of liability in the Agreement.

15. General

15.1 This DPA is governed by the laws of Queensland, Australia, consistent with the Agreement, and each party submits to the non-exclusive jurisdiction of the courts of Queensland. Nothing in this clause limits the application of the Privacy Act 2020 (NZ) to Deep Space where it applies.

15.2 If any provision is invalid or unenforceable, it is severed and the remainder continues in force.

15.3 Deep Space may update this DPA to reflect changes in the Privacy Laws or its Sub-processors, provided no update materially reduces the protections given to the Customer. Deep Space will give the Customer at least 30 days' written notice of any update, and the Customer may object under clause 8.5 where the update relates to a Sub-processor. Any other change to this DPA requires the written agreement of both parties. The version of this DPA in force at the commencement date of the Agreement continues to apply until an update takes effect under this clause, and superseded versions are retained and available on request.

15.4 All amounts referred to in this DPA are exclusive of GST.

15.5 Clauses 6 (Confidentiality and personnel), 10 (Data Breach notification), 13 (Return and deletion) and 14 (Liability) survive expiry or termination of the Agreement, and continue for so long as Deep Space holds any Personal Information of the Customer.

15.6 Notices to Deep Space under this DPA are given to the contacts in Annexure C. Notices to the Customer are given to the contact details recorded for the Customer under the Agreement. Each party will keep its contact details current.

Annexure A: Details of Processing

Item	Detail
Processor	Deep Space Trading Pty Ltd ABN 65 669 436 373
Subject matter	Supply of the Deep Space platform and DS Site under the Agreement.
Nature and purpose	Hosting, storage, transmission, display and processing of construction project records so the Customer can run its projects, covering estimating, procurement, commercial administration, site records, correspondence, document and drawing control, and health, safety, environment and quality.
Duration	The term of the Agreement, plus the retention and deletion periods in clause 13.
Categories of individual	The Customer's employees and contractors; personnel of the Customer's subcontractors, suppliers, consultants and clients; site visitors and inductees recorded through DS Site.
Types of Personal Information	Name, job title, employer, business email address, business telephone number, user account identifiers and authentication data, access and activity logs, site attendance and induction records, competency and licence details where recorded by the Customer, photographs where uploaded by the Customer, and any Personal Information in free text fields, correspondence or uploaded documents.
Sensitive information	Deep Space does not require sensitive information. Where the Customer records health, injury or incident information through health and safety functionality, that is sensitive information under the Privacy Act 1988 (Cth) and the Customer is responsible for having a lawful basis to collect it.

Annexure B: Technical and organisational measures

Governance

- Information security management system certified to ISO/IEC 27001:2022, with internal and external audit programmes and a documented Statement of Applicability.
- Documented information security, access control, incident response and vendor risk management policies, reviewed at least annually.
- Security awareness training for personnel, and background checks for personnel with production access where permitted by law.

Access control

- Role based access control, with production access limited to named personnel on a least privilege basis and reviewed periodically.
- Enterprise single sign-on available, so the Customer's own identity provider, conditional access policies and multi-factor authentication govern user access.
- Multi-factor authentication available for accounts not covered by single sign-on.
- Password controls including minimum length, blocking of commonly used passwords, and account lockout after repeated failed attempts.
- Logical separation of each customer tenancy.

Encryption

- Personal Information encrypted in transit using industry standard TLS.
- Personal Information encrypted at rest in the hosting providers' storage services.

Hosting and resilience

- Deep Space platform hosted on Google Cloud in the Sydney region; DS Site hosted on Amazon Web Services in an Australian region. Live Customer Data and documents are held in Australia.
- File storage replicated across multiple availability zones, being physically separate facilities with independent power, cooling and networking, and designed for 99.99999999% annual durability.
- Automated daily backups retained for 98 days, with backup copies replicated to a separate multi-region location so that no single region holds both the live data and the recovery copy.
- Point-in-time recovery enabled on both production databases, with seven days of transaction logs retained in cloud storage separately from the database instances, allowing restoration to any point within that window.
- Deleted documents recoverable for 7 days independently of the backup cycle.
- Recovery point objective for the production databases of 1 hour.
- Restoration procedures are tested on a scheduled cycle, with results recorded in the information security management system.

Monitoring and response

- Logging and monitoring of access to production systems.
- Documented incident response process with defined roles and escalation.
- Public status pages for the Deep Space platform and DS Site, to which the Customer may subscribe.

Assurance

- Independent penetration testing by a qualified third party, with material findings remediated and retested. An executive summary of the most recent test is available on request, subject to confidentiality undertakings.
- Vulnerability management and patching on a risk prioritised basis.

Annexure C: Contacts

Role	Contact
Deep Space privacy contact	privacy@deepspacegroup.ai
Deep Space security incident contact	security@deepspacegroup.ai
Deep Space registered office	Level 4, Suite 30, 50-56 Sanders Street, Upper Mount Gravatt QLD 4122, Australia