Sercha

DATA PROCESSING ADDENDUM

Sercha Data Processing Addendum

How Sercha handles personal information in Customer Data

Supplier	**Sercha Technologies · ABN 93 702 066 420**
Version	**1.0**
Effective	**24 September 2026**
Privacy contact	**[privacy@sercha.dev]**

This Data Processing Addendum (DPA) forms part of the agreement between Sercha Technologies (Sercha) and the Customer, which consists of the Sercha Master Services Agreement (MSA), this DPA and each Order Form (together, the Agreement). It applies whenever Sercha handles Customer Personal Information in providing the Service. Terms defined in the MSA have the same meaning in this DPA.

1. Roles

1.1 Customer in control. The Customer decides why and how Customer Personal Information is collected and used. Sercha handles Customer Personal Information only on the Customer's behalf, as its service provider, to provide the Service.

1.2 Customer responsibilities. The Customer is responsible for having a lawful basis to collect Customer Personal Information and to provide it to Sercha, including giving any notices and obtaining any consents required under the Privacy Act and under any confidentiality agreement or data room terms that apply, and for the accuracy of its instructions.

2. Handling on instructions

2.1 Purpose limitation. Sercha will collect, use, store and disclose Customer Personal Information only to provide, secure and support the Service in accordance with the Agreement and the Customer's documented instructions, or as required by law. The Agreement, the Customer's configuration of the Service and its written requests are the Customer's instructions.

2.2 Unlawful instructions. Sercha will tell the Customer promptly if it believes an instruction breaches the Privacy Act or another law, and is not required to follow that instruction.

2.3 No sale or secondary use. Sercha will not sell Customer Personal Information, use it for direct marketing, combine it with other customers' data, or use it to train or improve models made available to any other customer.

2.4 Details of handling. The subject matter, nature and purpose of the handling, and the types of personal information and individuals concerned, are set out in Schedule 1.

3. Privacy Act compliance

3.1 Standard of handling. Sercha will handle Customer Personal Information in accordance with the Privacy Act and in a manner consistent with the Australian Privacy Principles, whether or not Sercha is

itself an APP entity, including in particular APP 6 (use and disclosure), APP 8 (cross-border disclosure) and APP 11 (security).

3.2 Personnel. Sercha will ensure that personnel who can access Customer Personal Information are bound by confidentiality obligations, access it only as needed to perform their role, and receive appropriate privacy and security training.

3.3 Access and correction requests. If Sercha receives a request from an individual to access or correct their personal information, or a privacy complaint, relating to Customer Personal Information, it will refer the request to the Customer promptly and will not respond directly except as the Customer instructs or the law requires. Sercha will give reasonable assistance so the Customer can respond within the time required by APP 12 and APP 13.

3.4 Regulators. Sercha will give the Customer reasonable assistance with any enquiry from the Office of the Australian Information Commissioner or another regulator relating to Customer Personal Information, and will notify the Customer of any such enquiry directed to Sercha unless the law prohibits it.

4. Security

4.1 Measures. Sercha will implement and maintain the technical and organisational measures in Schedule 2, which are designed to protect Customer Personal Information from misuse, interference and loss, and from unauthorised access, modification and disclosure.

4.2 Changes. Sercha may update its security measures over time, provided the overall level of protection is not reduced.

5. Sub-processors

5.1 Authorisation. The Customer authorises Sercha to engage the sub-processors listed in Schedule 3.

5.2 New sub-processors. Sercha will notify the Customer at least 30 days before engaging a new sub-processor or replacing an existing one. The Customer may object on reasonable grounds relating to the protection of personal information within that period. The parties will discuss the objection in good faith, and if it cannot be resolved, the Customer may cancel the affected Order Form without charge and receive a refund of any prepaid fees for the period after cancellation.

5.3 Flow-down. Sercha will engage each sub-processor under a written agreement that imposes obligations on the protection of personal information that are no less protective than this DPA, and remains responsible to the Customer for each sub-processor's performance.

6. Location and cross-border disclosure

6.1 Storage in Australia. Customer Personal Information is stored and hosted in Australia.

6.2 Processing outside Australia. Some sub-processors, such as AI model providers, may process Customer Personal Information outside Australia, transiently and only to perform processing requested through the Service. Schedule 3 identifies each such sub-processor and where it processes data. Sercha will take reasonable steps, as required by APP 8.1, to ensure each overseas recipient does not breach the Australian Privacy Principles in relation to that information, including by contract terms that prohibit it from retaining Customer Personal Information beyond what is needed for the processing or using it to train its models.

7. Data breaches

7.1 Notification. Sercha will notify the Customer without undue delay, and in any event within 72 hours, after becoming aware of any unauthorised access to, unauthorised disclosure of, or loss of Customer Personal Information (a Security Incident).

7.2 Information and assistance. Sercha will give the Customer the information reasonably available to it about the Security Incident, including its nature, the information and individuals likely to be affected, and the steps taken to contain it, and will update the Customer as more information becomes available. Sercha will take reasonable steps to contain and remediate the Security Incident and will cooperate with the Customer's assessment of whether it is an eligible data breach under Part IIIC of the Privacy Act, so the Customer can complete that assessment within 30 days.

7.3 Notifying others. The Customer decides whether to notify the Office of the Australian Information Commissioner or affected individuals. Sercha will not notify them, or make any public statement about a Security Incident that identifies the Customer, without first consulting the Customer, unless the law requires it.

7.4 No admission. Sercha's notification of a Security Incident is not an admission of fault or liability.

8. Audits and information

8.1 Information. On request, and no more than once in any 12 months, Sercha will provide a written summary of its security measures and complete a reasonable security questionnaire.

8.2 Audits. Where the information provided under clause 8.1 is not sufficient to demonstrate Sercha's compliance with this DPA, following a Security Incident, or where a regulator requires it, the Customer may, on at least 30 days' notice, have Sercha's compliance audited by an independent auditor bound by confidentiality. Audits are conducted at the Customer's cost, during business hours and in a manner that minimises disruption, and do not extend to other customers' data.

9. Return and deletion

9.1 During the term. The Customer may export Customer Personal Information at any time through the Service or by request. Sercha will delete specified Customer Personal Information on the Customer's written request, for example where a transaction does not proceed and data room materials must be returned or destroyed, and will confirm the deletion in writing.

9.2 After termination. After the Agreement ends, Sercha will retain Customer Personal Information for the period set out in the Order Form (or, if none, 90 days) so the Customer can obtain an export, and will then permanently delete it, or delete it earlier on written request. Copies in backups are deleted in the ordinary course of backup rotation, within [35] days, and remain protected by this DPA until deleted.

9.3 Retention required by law. Sercha may retain Customer Personal Information where the law requires it, and will continue to protect it under this DPA and use it only for the purpose of that retention.

10. Other privacy laws

If the Customer is subject to a privacy law outside Australia, such as the EU or UK General Data Protection Regulation, in respect of Customer Personal Information, the parties will agree in writing any supplementary terms that law requires before that information is uploaded to the Service.

11. Liability, precedence and term

11.1 Liability. Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement.

11.2 Precedence. This DPA prevails over the MSA and any Order Form to the extent of any inconsistency in respect of the handling of personal information.

11.3 Term. This DPA applies for as long as Sercha holds Customer Personal Information, including after the Agreement ends.

12. Definitions

Australian Privacy Principles or APPs means the principles in Schedule 1 to the Privacy Act.

Customer Personal Information means personal information contained in Customer Data.

Personal information has the meaning given in the Privacy Act.

Privacy Act means the Privacy Act 1988 (Cth), including the Australian Privacy Principles and any binding code or regulations made under it.

Sub-processor means a third party engaged by Sercha that handles Customer Personal Information in providing the Service.

Schedule 1 — Details of handling

Subject matter	Provision of the Service described in the Order Form, including ingestion, organisation, extraction, cross-checking, querying and export of documents.
Duration	The term of the Agreement and the retention period in clause 9.
Nature of handling	Collection from connected sources and uploads; storage; optical character recognition; automated extraction and classification; indexing; querying; display to authorised users; export; deletion.
Purpose	To provide, secure and support the Service for the Customer's internal business purposes.
Individuals concerned	Individuals named in documents the Customer processes (for example tenants, guarantors, directors, landlords, vendors' and advisers' personnel, and counterparties), and the Customer's own users.
Types of personal information	Names, contact details, signatures, roles and titles; lease, tenancy, rent, security and bank guarantee details relating to individuals; other information contained in documents the Customer processes; user account and usage information.
Sensitive information	Not intended to be processed. Any sensitive information incidentally contained in documents is handled under this DPA.

Schedule 2 — Security measures

- **Encryption:** Customer Data is encrypted in transit and at rest using industry-standard encryption [confirm: e.g. TLS 1.2 or higher in transit, AES-256 at rest].
- **Access control:** role-based access, least-privilege administrative access, multi-factor authentication for Sercha personnel with production access, and prompt removal of access when no longer needed.
- **Separation:** each customer's data is logically separated, and within a customer account, each asset is held in its own access-controlled partition.
- **Logging and monitoring:** audit logging of access to Customer Data and monitoring for suspicious activity.
- **Resilience:** regular backups, stored in Australia, and tested restoration procedures.
- **Vulnerability management:** timely application of security patches and regular review of dependencies and configurations.
- **Secure development:** code review and separation of development, test and production environments. Customer Data is not used in development or test environments without the Customer's consent.
- **Incident response:** a documented process for identifying, containing, assessing and notifying Security Incidents, consistent with clause 7.
- **Personnel:** confidentiality obligations, security and privacy training, and need-to-know access.
- **Suppliers:** due diligence on sub-processors and written terms consistent with this DPA.

Schedule 3 — Approved sub-processors

Sub-processor	Purpose	Data location
[Cloud hosting provider]	Hosting, storage and backups of Customer Data	**Australia [region]**
[AI model provider]	Document understanding, extraction and query processing	**[Australia or location of processing]**
[OCR provider, if separate]	Text recognition from scanned documents	**[location]**
[Email or support tooling]	Support communications and notifications	**[location]**

This addendum follows the structure of the Common Paper Data Processing Agreement (Version 1.1), available at commonpaper.com/standards/data-processing-agreement, which is licensed under CC BY 4.0. It has been substantially modified and adapted to the Privacy Act 1988 (Cth) by Sercha Technologies, and is not endorsed by Common Paper.