

**Customer terms and conditions –
Cogniti software as a service**

Last updated: 2 October 2026

Contents

Contents 1

Cogniti Subscription Service 2

Cogniti Subscription Agreement: hosted by the University of Sydney 9

Privacy Policy..... 28

Cookies and Similar Technologies 40

Data Processing Addendum..... 42

Change history 59

Cogniti Subscription Service

Bracketed User Pricing: The subscription fee is calculated based on the total number and classification of Authorised Users designated by Customer, subject to minimum block purchases as described below. Pricing applies per the following user-volume brackets:

For Tertiary Education Providers (Universities, Institutes, Colleges)

User bracket	Annual Price per User in this bracket (AUD)
1st–2,000th user	\$20
2,001st–5,000th user	\$12
5,001st–15,000th user	\$8
15,001st–35,000th user	\$6
35,001st+ user	\$4

For Primary & Secondary Education Providers, and Providers with fewer than 5,000 EFTSLs¹

User bracket	Annual Price per User in this bracket (AUD)
1st–2,000th user	\$18
2,001st–5,000th user	\$10
5,001st–15,000th user	\$6
15,001st–35,000th user	\$4
35,001st+ users	\$2

Example: For 3,000 users in a tertiary institution: First 2,000 users are \$20 each = \$40,000; Next 1,000 users are \$12 each = \$12,000; Total: \$52,000 plus GST

¹ EFSTL = equivalent full time student load

Minimum Seat Purchase Requirements

- For Tertiary Education Providers and Other Providers with 5,000 or more EFTSLs: seats must be purchased in minimum blocks of 500 Authorised Users per order.
- For Primary and Secondary Education Providers, and Providers with fewer than 5,000 EFTSLs: seats must be purchased in minimum blocks of 100 Authorised Users per order.
- Seat reductions may only take effect at the start of a new billing cycle.
- Additional seat blocks may be added mid-cycle and will be pro-rated for the remainder of the billing cycle.

Billing Cadence and Discounts

- Annual billing with invoice issued upfront. Minimum term is 12 months.
- Half-yearly billing is available, by mutual agreement, to some Customers who have non-standard teaching sessions (for example students who are only enrolled for 15 weeks a year). For these situations, a 40% discount applies to the per-user amounts listed in the applicable bracketed pricing table for the half year (for example, a full year is \$20 per user per year, and is \$12 per user per half year). Half-yearly billing applies only to the Subscription Fee and does not apply to optional add-ons (such as training blocks), unless expressly agreed.

Usage Caps (Token Allowances)

The following usage limits apply based on the total number of seats purchased under this Order. For each block of 500 seats purchased, Customer will receive:

- Input Token Allowance: 200,000,000 tokens
- Output Token Allowance: 20,000,000 tokens

Overage Options and Commercial Consequences

If Customer exceeds any applicable token allowance, one of the following overage mechanisms will apply (as selected by Customer):

- Option A: Purchase Additional Token Bundles. Additional bundles may be purchased at the following rate:
 - Input tokens per bundle: 100,000,000 tokens
 - Output tokens per bundle: 10,000,000 tokens
 - Fee per bundle: cost price plus 20% overhead (please enquire)
- Option B: Purchase Additional Seat Blocks. Customer agrees to purchase additional blocks of seats at the applicable bracketed rate, which will increase the token allocations accordingly.

Throttling or Suspension Trigger

If Customer exceeds the allocated token caps and no overage arrangement has been agreed, the University may apply temporary throttling or temporary suspension of the affected features until additional commercial terms are agreed. The University will provide notice where practicable.

INCLUDED SUPPORT AND TRAINING

Standard support is included as described in the Support Schedule (SLA), including:

- Email/web support
- Response targets by severity as set out in section 4 of the SLA (Critical: 4 business hours)
- Access to documentation and knowledge base

Included Training Allocation:

- 4 hours of online training per year, delivered virtually
- Training covers platform onboarding, core features, and best-practice usage

OPTIONAL TRAINING ADD-ONS

Additional training blocks may be purchased at a rate of AUD \$1,000 plus GST per 2-hour block.

SUPPORT FOR IMPLEMENTATION, TRAINING, ONBOARDING, AND GENERAL QUESTIONS

Support Overview

Support and Assistance in onboarding Customer: During the Initial Term and at Customer's option, the University will provide Customer onboarding and training support of 4 hours.

Account Configuration: Following execution of this Order Form, the University will provide Customer access to a dedicated organisation within the Cogniti service, logically separated from other institutions and configured with default settings. The University will meet with Customer to discuss account configuration, including:

- Names and email addresses of designated account administrators;
- All company names, aliases, and domains;
- Access to particular AI models;
- Setting permissions; and

- Any single sign-on and integration specifications.

Training: The University's in-house team will train Customer's designated users through a virtual meeting (e.g. platform onboarding, core features, and best-practice usage).

Support: During the University's business hours and throughout the Subscription Term, the University will provide Customer support for general questions and issues by email (cogniti@sydney.edu.au) or web meeting.

SUPPORT AND SERVICE LEVEL SCHEDULE (SLA)

1. Purpose and Scope

This Support & Service Level Schedule ("SLA") sets out the service levels, support entitlements, maintenance practices, and operational commitments applicable to the Services. This SLA forms part of, and is governed by, the Agreement.

Capitalised terms have the meaning given in the Agreement unless otherwise stated.

2. Service Availability

Availability Target

The University will use commercially reasonable efforts to make the core components of the Services available 99.5% each calendar month ("Availability Target"), excluding Permitted Downtime.

Permitted Downtime includes:

- Scheduled maintenance;
- Emergency maintenance;
- Downtime caused by Customer systems, networks, or misuse;
- Unavailability caused by Sub-Processor outages outside the University's reasonable control;
- Force majeure events; and
- Suspension or throttling permitted under the Agreement (e.g., misuse, quota breach, or security reasons).

Measurement

Availability is measured at the service endpoint of the University's hosting environment (currently Microsoft Azure), excluding Customer's own networks or connections.

Performance

The University targets page load and API response times of under 5 seconds under normal operating conditions, measured at the service endpoint. Actual performance

may vary based on payload complexity, AI model processing time, Customer network conditions, and concurrent usage. The University will monitor system performance and investigate sustained degradations reported by Customer.

Service Credits for Missed SLAs

If the Services fail to meet the Availability Target in any calendar month (excluding Permitted Downtime), Customer may request a service credit as follows:

- Monthly Availability below 99.5% but at or above 99.0%: credit of 5% of that month's pro-rated Fees
- Monthly Availability below 99.0% but at or above 95.0%: credit of 10% of that month's pro-rated Fees
- Monthly Availability below 95.0%: credit of 25% of that month's pro-rated Fees

Credits must be requested in writing within 30 calendar days of the affected calendar month. Credits may not exceed 25% of that month's pro-rated Fees and are not redeemable for cash. Service credits are Customer's sole and exclusive remedy for failure to meet the Availability Target.

3. Maintenance and Change Management

Scheduled Maintenance

The University may perform scheduled maintenance during a window notified in advance. The University will provide at least 48 hours prior notice of Scheduled Maintenance expected to affect availability.

Maintenance Categories

- Routine maintenance
- Security patches
- Infrastructure upgrades
- Feature updates

Emergency Maintenance

The University may perform emergency maintenance at any time where necessary to address urgent security, stability, or performance risks. Notice will be provided as soon as reasonably practicable.

4. Incident Classification and Response

Severity	Description	Target Response Time (Business Hours)	Target Action
Critical (S1)	Complete service outage; no workaround; significant operational impact	4 business hours	Continuous efforts until restoration
High (S2)	Key functionality impaired; workaround available	1 business day	Work begins next business day
Medium (S3)	Partial functionality issue; low impact	2 business days	Resolution in standard release cycle
Low (S4)	Non-critical issue; cosmetic or general inquiries	5 business days	Guidance or fix as appropriate

Support hours: Monday to Friday 9:00 am to 5:00 pm Sydney Time

5. Support Channels Support is available via:

- Email: cogniti@sydney.edu.au
- Online meeting by appointment
- In-product and online self-service support mechanisms, as applicable

6. Included Support Services

The following support is included during each Subscription Term:

6.1 General Support and Account Configuration

- Incident management in accordance with Section 4
- Guidance on configuration and user administration
- Access to documentation, knowledge bases, FAQs
- Administrator setup, aliases, permissions, integrations

6.2 Onboarding Assistance and training

- Virtual onboarding support and training
- Initial account provisioning
- Administrator setup and permission configuration
- Training topics as agreed between the parties

7. Suspension and Throttling

The University may suspend or throttle access to the Services where:

- Usage materially exceeds allocated token or quota limits;
- Misuse or breach of the Agreement, including the use restrictions in Sections 2.8(b) and 2.9 of the Subscription Agreement, is identified;

- A security incident or threat requires protective action;
- Customer fails to pay Fees when due.

The University will provide reasonable notice where practicable.

8. AI Model Updates and Behaviour Changes

The University will use reasonable efforts to provide 5 days' notice of material updates including changes to AI models where such changes are expected to materially impact Customer. Model selections, exclusions or restrictions recorded in the Order are not changed without Customer's written agreement.

9. Exclusions

This SLA does not apply to:

- Beta or experimental features;
- Connectivity issues in Customer's networks;
- Third-party systems not controlled by the University;
- Issues caused by Customer misuse, configuration errors, or failure to follow guidance;
- Delays caused by Customer's failure to provide information or access;
- Force majeure events.

10. Changes to this SLA

The University may update this SLA from time to time.

Material changes that adversely affect Customer will be notified at least 30 days prior to taking effect and will generally apply at the next renewal unless otherwise agreed.

Cogniti Subscription Agreement: hosted by the University of Sydney

Introduction

In this Cogniti Subscription Agreement (this “**Agreement**”), the University of Sydney (“**the University**”), provides Cogniti, a generative artificial intelligence powered learning and teaching support platform. The University hosts and operates Cogniti on Microsoft Azure. The University takes the privacy and security of data seriously (see our [Privacy Policy](#)).

1. Background

1.1 The Parties. This Agreement is between the University and the entity (or entities) identified in the relevant Order (“**Customer**”) or similar document that references this Agreement and is executed by the parties (“**Order**”). This Agreement is effective as of the effective date of the first Order entered into between the University and Customer (“**Effective Date**”). The term of this Agreement (the “**Term**”) begins on the Effective Date and continues until terminated in accordance with Section 5.

1.2 Applicable Terms. This Agreement sets forth the terms and conditions under which the University agrees to provide, and Customer agrees to receive and pay for, access to and use of the Services (defined in Section 2.1 below) described herein and in the relevant Order. Capitalised terms (whether in the singular or plural) will have the meanings assigned in the text of this Agreement or in the Order.

1.3 Controlling Terms. If there is a direct conflict between the documents comprising this Agreement, they will control in the following order of precedence:

- (a) any Order
- (b) this Subscription Agreement (including all incorporated schedules, annexes, and addenda);
- (c) the Schedules referenced in this Agreement, including the Data Processing Addendum (DPA), Support & Service Level Schedule, and any Responsible Use or Acceptable Use Policy expressly incorporated by reference; and
- (d) any University policies or FAQs referenced in an Order or this Agreement.

2. Services and Each Party’s Responsibilities

2.1 Orders and Applicable Services. Each Order will set forth the University offerings (the “**Services**”) of Cogniti. Each Order constitutes Customer’s binding commitment to purchase the items described on such Order and is incorporated into this Agreement by reference. During the Subscription Term (defined in Section 5 below) set out in the

relevant Order, the University will make available to Customer the Services set forth in such Order under the terms of this Agreement.

2.2 AI Inference and Model Selection. The Services use artificial intelligence inference hosted primarily in Microsoft Azure – Australia East. Where required for resilience, capacity, or model availability, the Services may use inference in other regions or global standard deployments. Customers may elect to opt in or opt out of specific AI models made available through the Services. Any customer-specific model selections, exclusions, or restrictions will be recorded in the relevant Order.

2.3 Service and Support Levels. Standard support for the Services is included as described in the Support and Service Level Schedule included in these terms. The Support & Service Level Schedule sets out the University’s support model, support hours, response targets, and service level commitments. Additional support services or training packages may be purchased as set out in the relevant Order.

2.4 Customer’s Rights to Use the Services. Subject to the terms of this Agreement, the University hereby grants Customer a limited, non-exclusive, non-transferable, worldwide license during the relevant Subscription Term to access and use the Services and permit the number and type of individual users (“**Authorised Users**”) specified in the Order to access and use the Services solely for internal purposes of education and institutional operations. Authorised Users may include Customer’s or Customer’s Affiliates’ (defined below) designated employees, contractors, or consultants. An “**Active User**” means an Authorised User who, during the applicable billing cycle, logs into the Services and performs at least one interaction with a Cogniti asset, feature, or AI interaction capability. Each purchased seat is deemed consumed upon the first login and first interaction of an Authorised User (“**Seat Activation**”). Seat Activations are fixed for the remainder of the applicable billing cycle and are not transferable between users except as expressly permitted in the Order.

2.5 Usage Limits, Token Quotas and Overage. The Services are subject to usage limits, including token quotas, rate limits, and other consumption thresholds applicable to Customer’s subscription. The specific numeric token allocations, rate limits, or other quantitative limits applicable to the Customer will be as set out in the relevant Order. If Customer exceeds any applicable usage limits, the University **will apply the Overage mechanism in the Order**, and may apply temporary throttling or suspension of access to the relevant functionality until such additional commercial terms are agreed. The University will, where practicable, provide reasonable notice to the Customer before applying any such throttling or suspension, unless immediate action is required for system integrity or security.

2.6 Suspension for Misuse or Security Incidents. The University may suspend or restrict access to the Services, in whole or in part, with immediate effect where the

University reasonably determines that: (a) Customer or any Authorised User is misusing the Services or violating this Agreement; (b) such suspension is necessary to address or mitigate a security incident, data breach, or material vulnerability; or (c) continued access would create a material legal, regulatory, or compliance risk for the University. The University will provide Customer with reasonable notice of any suspension where practicable, and will restore access promptly once the underlying issue has been resolved.

2.7 Use of the Services by Customer Affiliates and Authorised Users. Customer may permit its Authorised Users, designated Affiliates, and Authorised Users of such Affiliates to access and use the Services pursuant to the terms of this Agreement; provided that additional fees may apply and such allowance does not expand the University's liability under Section 8 below, the DPA (**Data Processing Addendum**), and volume of claims, and any claim under this Agreement, an Order, or DPA must be brought by Customer unless an Affiliate has separately signed an ordering document directly with the University for Services. Customer must notify the University of the identity of any Affiliates exercising rights granted to Customer hereunder. Customer is liable for all Affiliates and Authorised Users compliance with Customer's obligations under this Agreement and the DPA. Customer must take reasonable steps to prevent unauthorised access to the Services, including, without limitation, by ensuring that all access credentials are kept confidential. No Authorised User will share its credentials or permit another individual to circumvent the privileges restrictions pertaining to the Services. Customer is liable to the University for all activity that occurs with Customer's credentials or otherwise through or in connection with Customer's or its Affiliates or Authorised Users' accounts, including, without limitation, any unauthorised use or access of the Services through Customer or its Affiliates or Authorised Users' accounts by Customer or any third parties. If Customer discovers any vulnerabilities or breaches related to Customer's, an Affiliate's, or an Authorised User's use of the Services, Customer will: (a) promptly contact the University and provide details of the vulnerability or breach; and (b) cooperate with the University to remediate such vulnerability or breach. "**Affiliate**" of a party means any other entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such entity, and "control" (including as used in the terms "controlled by" and "under common control with") means the ownership, beneficially or of record, of more than fifty percent (50%) of the voting securities of an entity.

2.8 Customer Obligations When Using the Services.

(a) Customer understands that it has control over who are designated as Authorised Users and their specific roles and access rights, the files, information, or other data that's uploaded, inputted, or otherwise processed in, through, and to the Services (together, "**Customer Content**"), and the specific purpose of how the Services are

configured and used. Accordingly, in addition to Customer's other obligations under this Agreement, in connection with Customer's use of the Services, Customer agrees as follows:

- (i) Customer will ensure that it has obtained all requisite consents to enable the University to provide the Services;
- (ii) Customer will not use the Services in a manner that generates inquiries from a law enforcement or other regulatory agency or triggers such an agency to request the suspension of the Services;
- (iii) the Services may not be used to violate system or network security, including, but not limited to, transmitting files or messages containing computer viruses or propagating worms, Trojan horses, or "spyware" programs;
- (iv) Customer may not perform any audits, penetration testing, or make any other intrusion attempts on the Services without the University's prior written consent;
- (v) the Services may not be used to transmit any Customer Content that violates or infringes the intellectual property, proprietary, or other rights of third parties, or that is offensive, illegal, or otherwise reasonably objectionable to any person or entity; and
- (vi) Customer will not upload any of the following types of information: personally identifiable health information, financial account numbers (such as credit card or bank account numbers), or any other information or combinations of information that falls within the definition of "special categories of data" under applicable European Data Protection Law (defined in the DPA) or "sensitive information" under any other applicable law.
- (vii) Customer must inform its students, staff, and other Authorised Users about the nature of the Services and for obtaining all notices, consents, and permissions required under applicable privacy, education, or institutional policies prior to allowing them to use the Services. Customer is responsible for ensuring that its use of the Services, and the use by its Authorised Users, complies with all applicable student-privacy, data-collection, and consent requirements.

(b) The following describes general use restrictions for the Service. Except as expressly allowed under this Agreement, Customer will not, directly, indirectly or through its Affiliates, Authorised Users, employees, or independent contractors:

- (i) attempt to sell, transfer, assign, rent, lend, lease, sublicense or otherwise provide third parties the benefit of the Services;

- (ii) “frame,” “mirror,” copy or otherwise enable third parties to use the Services (or any component thereof) as an outsourced service;
- (iii) allow access to the Services by multiple individuals impersonating a single end user;
- (iv) modify or use the Services in a manner that interferes with, degrades, or disrupts the integrity or performance of any of the University services, systems or other offerings, including, without limitation, data transmission, storage, and backup;
- (v) use the Services to develop a product or service that competes with any of the University’s products or services;
- (vi) circumvent or disable any security features or functionality associated with the Services;
- (vii) access the Services or associated data through web scraping or any undocumented process or API;
- (viii) use the Services in any manner prohibited by applicable law or treaties; or
- (ix) attempt to extract, reconstruct, infer, or reverse engineer the underlying models, model weights, training data, embeddings, or other proprietary components of the Services.

2.9 Responsible and Acceptable Use. Customer acknowledges that the Services incorporate artificial intelligence capabilities and agrees to use the Services in a responsible, lawful, and educationally appropriate manner. In addition to the obligations in Section 2.7, Customer agrees:

- (a) that it and its Authorised Users must not use the Services to: (i) engage in any unlawful, fraudulent, or harmful activity; (ii) create, generate, or disseminate disinformation, misleading content, or deceptive synthetic content intended to mislead or cause harm; (iii) engage in harassment, bullying, discrimination, or threats; (iv) generate, upload, or distribute harmful, abusive, or violent material; (v) generate content intended to automate or facilitate academic misconduct; or (vi) perform any other activity reasonably deemed by the University to present a material ethical, legal, or safety risk. The University may publish a non-exhaustive Prohibited Uses list and update it from time to time, and such list is incorporated by reference into this Agreement; and
- (b) to retain appropriate human oversight when using the Services for any high-impact decisions relating to education, assessment, academic progression, or student welfare. The Services are intended to support, not replace, professional

judgment, and Customer is responsible for ensuring that Authorised Users apply suitable review and oversight in their use of AI-generated outputs.

2.10 Optional Use of Beta Services. The University may offer a product, service, integration, or other feature available to Customer to try at Customer's election that is designated as beta, experimental, preview, trial, or other similar description ("**Beta Service**"). Beta Services are intended for evaluation purposes only and not suitable for production use. Unless otherwise agreed by the parties, use of any Beta Service will expire upon the earlier of: (a) the date provided by the University in an email notice; and (b) the date a version of the Beta Service becomes generally available without the applicable Beta Service designation. The University may discontinue a Beta Service at any time in its sole discretion. Customer understands that Beta Services are under development and may have flaws. As such, all Beta Services are provided "AS IS," and Sections 6, 7, and 8.2(a) will not apply to Customer's use of any Beta Service, except that to the extent a Beta Service processes Customer Confidential Information (defined in Section 9 below) or Personal Data (defined in the DPA) this Section 2.10 will not limit the University's obligations under this Agreement regarding compliance with applicable laws and obligations under the DPA and under Section 9 below regarding the confidentiality of Customer Content.

3. Fees and Payment Terms

3.1 Fees and Taxes. In consideration of the rights granted herein and access to and use of the Services, Customer will pay the University the amounts specified in an Order for the Services provided thereunder ("**Fees**"). Fees are non-refundable and non-cancellable unless expressly agreed otherwise under this Agreement. Taxes are continually evolving and vary by jurisdiction. As such, Fees specified in an Order are exclusive of any applicable sales, use, import or export taxes, duties, fees, value-added taxes, tariffs, or other amounts attributable to Customer's execution of this Agreement or purchase or use of the Services (collectively, "**Taxes**"). Customer is solely responsible for the payment of any applicable Taxes. The University is responsible for any taxes based on the University's net income, assets, payroll, property, and employees. If the University is required to pay Taxes on Customer's behalf, Customer will promptly reimburse the University for all amounts paid.

3.2 Billing and Payment Terms. Fees are payable in Australian Dollars. If Customer reasonably disputes an invoice, Customer must deliver a written statement to the University no later than ten (10) days prior to the due date of such invoice listing all disputed items and providing a reasonably detailed description of each disputed item. In such event, the parties will work together in good faith to resolve any such dispute. If Customer does not so notify the University of its dispute of an invoice within such time period, such invoice is deemed undisputed and the right to dispute such invoice is waived. The University reserves (among other rights and remedies) the right to suspend

Customer's access to the Services if undisputed Fees are not paid when due. Amounts payable to the University will continue to accrue during any period of suspension and must be paid as a condition precedent to reactivation. Customer's failure to pay any undisputed Fees when due is deemed a breach of a material obligation under this Agreement.

3.3 AI Infrastructure Cost Adjustment

The Fees set out in this Agreement also include the University's third-party artificial intelligence processing, inference, token consumption, GPU compute, and related cloud infrastructure costs applicable as at the Effective Date.

Customer acknowledges that the Services rely on third-party artificial intelligence and cloud infrastructure providers whose pricing and commercial models may change during the Term beyond the University's reasonable control.

If, during the Term, the University's third-party costs of providing the Services increase by more than fifteen percent (15%) compared to the third-party costs as at the Effective Date, due to:

- (a) increases imposed by third-party AI model or cloud providers;
- (b) increases in token consumption pricing;
- (c) changes in model pricing structures or inference pricing;
- (d) increases in GPU, compute, or related infrastructure costs; or
- (e) other external infrastructure cost increases beyond the University's reasonable control,

then the University may notify Customer and provide supporting evidence of such increase.

Within two (2) weeks of such notification, the parties must commence negotiating in good faith an adjustment to the Fees, usage allowances, service configuration, or other relevant terms, with a view to agreeing upon commercially reasonable adjustments to maintain continuity of the Services.

Customer acknowledges that there may be adjustments incapable of implementation through the Azure Marketplace billing framework, in which case any adjustment agreed under this Section will be documented in a separate written addendum, order form, or statement of work between the parties and may be invoiced separately from any Azure Marketplace transaction or subscription billing mechanism.

Customer agrees that during the negotiation period and until any agreed adjustment is documented:

- (i) this Agreement will remain in force;

- (ii) the University may recover up to seventy-five percent (75%) of the increase to third-party costs through a temporary surcharge applied prospectively; and
- (iii) the University may implement commercially reasonable measures to optimise AI model usage, routing, or processing efficiency, provided that there is no material degradation to the core functionality of the Services. For the avoidance of doubt, permissible optimisations include switching AI models, adjusting inference parameters, implementing caching or batching strategies, and routing queries to more cost-effective infrastructure, provided that the performance of the Services is not materially degraded and subject to any model selections, exclusions or restrictions recorded in the relevant Order.

If the parties do not agree on an adjustment within sixty (60) days after notice is given by the University under this Section, the matter must be escalated for good-faith negotiation between senior representatives of each party in accordance with Section 10.3 (Dispute Resolution, Governing Law and Venue). If no agreement on the adjustment is reached within a further thirty (30) days after escalation, the University may, upon two (2) weeks written notice, either:

(A) terminate the affected Order or Subscription upon sixty (60) days' notice without liability (other than refunds for prepaid fees attributable to the terminated period), or

(B) implement revised Fees reflecting the increase of third-party costs, subject to Customer's right to terminate the affected Order or Subscription upon thirty (30) days' written notice following such adjustment, in which case Customer will receive a prorated refund of any prepaid Fees attributable to the terminated period.

4. Proprietary Rights and Data Protection

4.1 Rights to Customer Content. As between the parties, any rights in and to Customer Content are retained by Customer. For clarity, Customer and its Authorised Users retain all rights, title and interest in their content, prompts, messages, and any outputs generated through their use of the Services. The parties agree that Usage Data (defined as follows) and Feedback (defined in Section 4.4 below) are not considered Customer Content for purposes of this Agreement. As used herein, “**Usage Data**” means data and other information pertaining to Customer’s use of the Services, including, but not limited to, the number of assets created, the number of users, the number and frequency of interactions with AI, and the number of other interactions with the Services.

4.2 License to Customer Content. Customer, on behalf of itself and all authorised Affiliates, hereby grants to the University a limited, non-exclusive, royalty-free, worldwide license to use, copy, store, modify, distribute, transfer, and display all Customer Content solely for the purpose of providing and improving the Services.

Customer understands that to build and deliver a great product, the University improves the Services using Usage Data and aggregated and anonymised Customer Content. Accordingly, notwithstanding the foregoing, in compliance with applicable laws, this Agreement, and the DPA, the University may: (a) during and after the Term, use Usage Data to develop, improve, support, secure, market, and operate the Services, except that any Usage Data shared externally must be aggregated and anonymised and in a format that is not traceable back to Customer; and (b) improve the Services by using Customer Content that has been de-identified, anonymised, or aggregated so that it does not identify Customer, Customer Affiliates, Authorised Users, or any other individual person. The University agrees that once Usage Data and Customer Content are converted to a de-identified, anonymised format (together, “**De-Identified Data**”), it cannot be re-identified. Notwithstanding any other term of this Agreement, the University will not use Customer Content, Personal Data, or institution-identifiable data to train or fine-tune any models. For clarity, the University may continue to use Usage Data and De-Identified Data to maintain, secure, and improve the Services, provided that such data does not identify Customer, Customer Affiliates, Authorised Users, or any individual.

4.3 The University’s Proprietary Rights. Customer understands that the Services, AI, and underlying technology are core to the University’s business. As such, all rights (including all ownership rights) not expressly granted to Customer under this Agreement or in an Order are reserved by the University, its suppliers, and licensors. The University and its licensors retain all right, title, and interest in and to the University’s name, logo, and other marks, the Services, any documentation related thereto, all underlying software, De-Identified Data, methodologies, and all components, updates, modifications, derivative works, and manifestations to the foregoing, including, but not limited to, all intellectual property and proprietary rights in the foregoing (including, without limitation, any changes which incorporate any Feedback) (collectively, “the **Cogniti Technology**”).

4.4 Feedback. Customer and any Authorised User may submit comments, suggestions, ideas, or other feedback to the University related to the Services or any of the Cogniti Technology (together, “**Feedback**”). Customer hereby grants the University a perpetual and irrevocable license to use and exploit any portion of Feedback in any manner without any obligation, royalty, or restriction based on intellectual property rights or otherwise. Any Feedback provided by Customer is AS IS and the University will not attribute to Customer any Feedback used.

4.5 Data Processing, Privacy, and Security. The Data Processing Addendum (“**DPA**”) (available at [Data Processing Addendum](#)) includes terms required under applicable laws and regulations and contains security-related provisions. The DPA will be updated from time to time to meet the requirements of new Applicable Data Protection Laws

(defined in the DPA). The parties agree that the terms of the DPA are hereby incorporated by reference. The University may engage third-party service providers, including cloud infrastructure providers such as Microsoft, to support the hosting, processing, or delivery of the Services (“**Subprocessors**”). The University will remain responsible for the performance of its Subprocessors and for ensuring that any Subprocessor is bound by written obligations that provide a level of protection for Customer Content and Personal Data that is materially no less protective than those set out in this Agreement and the DPA. As described in the DPA, the University will maintain reasonable administrative, technical, and physical safeguards designed to protect Customer Content and any Personal Data processed, stored, collected, or transmitted by the Services. The University will notify Customer without undue delay, and in any event no later than seventy-two (72) hours after confirming a Security Incident (as defined in the DPA) that materially affects the confidentiality, integrity, or availability of Customer Content or Personal Data, in accordance with the DPA, except to the extent such notification is delayed or restricted by applicable law or law-enforcement requirements. Such notice will describe, to the extent known at the time, the nature of the incident and the steps the University is taking to investigate and mitigate its impact. The University protects Customer Content using industry-standard encryption technologies, including encryption in transit using TLS 1.2 or higher and encryption at rest using AES-256 or equivalent modern cryptographic standards. The University will maintain these or materially equivalent protections during the Term. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by the University, the Standard Contractual Clauses (as defined in the DPA) will apply, as further set forth in the DPA. For purposes of the Standard Contractual Clauses, Customer and its applicable Affiliates are each the data exporter, and Customer’s acceptance of this Agreement, and an applicable Affiliate’s execution of an Order, is treated as its execution of the Standard Contractual Clauses and Appendices.

5. Subscription Term and Termination Rights

5.1 Subscription Term. Each Subscription to the Services begins on the Subscription Start Date specified in the relevant Order and continues for an initial minimum Subscription Term of twelve (12) months, unless a different minimum term (for example, six (6) months for non-standard teaching arrangements) is expressly stated in the Order. Unless otherwise stated in the Order, each Subscription will automatically renew for successive periods equal to the length of the initial Subscription Term at the then-current fees, unless either party provides written notice of non-renewal no later than thirty (30) days prior to the end of the then-current Subscription Term.

5.2 Termination for convenience. Either party may elect not to renew a Subscription by providing the other party with at least thirty (30) days’ written notice prior to the end of

the then-current Subscription Term. A termination for convenience takes effect only upon expiry of the current Subscription Term. Except as expressly stated in an Order, neither party may terminate a Subscription for convenience during a Subscription Term, and no refunds or credits are payable for the unexpired portion of the Subscription Term.

5.3 Termination for cause. Without limiting other remedies it may have, either party may terminate this Agreement or any Order with immediate effect by written notice if (i) the other party materially breaches the Agreement or an Order, and fails to cure the breach within 30 days after receipt of notice of the breach; or (ii) the other party becomes Insolvent. Upon such termination:

(a) All licenses granted under this Agreement will terminate immediately, except for any fully-paid, perpetual licenses expressly identified in an Order.

(b) All undisputed amounts due and payable as at the termination date become immediately due. For metered or usage-based Offerings, Customer must immediately pay for all usage up to the termination date.

(c) If the University is the breaching party, Customer will receive a prorated refund or credit of any prepaid subscription fees attributable to the unused portion of the applicable Subscription Term after the effective date of termination.

5.4 Effect of Termination. Upon expiration or termination of this Agreement, or of a Subscription under any Order, Customer and all Authorised Users will discontinue all use of the Services. For ninety (90) days following the expiration or termination of this Agreement or the relevant Subscription, at no charge and subject to the functionality limitations of the Services, the University will make Customer Content available for export using the in-product export tools or other processes made available by the University from time to time, in one or more commonly used, machine-readable formats (such as CSV, JSON, or other standard formats supported by the Services at the time of export). After that ninety (90) day period the University will delete Customer Content from the production Services within a further thirty (30) days, except to the extent retention is required by law, in accordance with the Data Processing Addendum. Copies of Customer Content held in encrypted backups expire under the University's backup retention schedule and are not restored except for disaster recovery. Any Customer Content retained for legal reasons will continue to be protected by the applicable terms of this Agreement and the DPA. Any Customer Content retained by the University for the foregoing reasons will continue to be protected by applicable terms of this Agreement and the DPA and will remain subject to confidentiality obligations set out in Section 9 below. The parties agree that definitions, payment obligations of either party, Sections 1, 2.6, 3, 4.2, 4.3, 4.4, 5.3 and 6-10, and other provisions that reasonably should survive to interpret the obligations or parties' intent of this Agreement will survive any expiration

or termination of this Agreement. For clarity, expiration of a Subscription Term following a non-renewal under Section 5.2 does not constitute a termination for cause.

6. Indemnification from third-party claims

6.1 Protection of Customer from third-party claims. Subject to the terms set forth in this Section 6, at its expense, the University will defend Customer and its personnel, successors, and assigns from and against any Customer Claim (defined below) brought against them, and indemnify them for any judgment that a court of competent jurisdiction grants a third-party on such Customer Claim or that's awarded to a third-party under any the University-approved settlement of any such Customer Claim. A **"Customer Claim"** means a third-party claim, suit, or proceeding (which, for purposes of Section 6 of this Agreement, a "third-party" is a party that is not a party to this Agreement or Order (or such party's Affiliate)) alleging that the Services, when used as intended, infringe or misappropriate the intellectual property rights of a third-party. If any portion of the Services is subject to a Customer Claim that prohibits or impairs Customer's use of the Services, the University will, at its own cost and discretion, either procure for Customer the right to continue the Services or modify the Services so that they are non-infringing but retain materially equivalent functionality. If neither of the foregoing options are available on terms that are commercially reasonable for the University, then the University may terminate Customer's right to access and use such portion of the Services subject to the Customer Claim, and the University will refund Customer any prepaid Fees for the unused portion of the applicable terminated Service's Subscription Term, prorated from the effective date of termination.

6.2 Protection of the University from third-party claims. Subject to the terms set forth in this Section 6, at its expense, Customer will defend the University and its personnel, successors, and assigns from and against any the University Claim (defined below) brought against them, and indemnify them for any judgment that a court of competent jurisdiction grants a third-party on such the University Claim or that's awarded to a third-party under any Customer-approved settlement of any such the University Claim. A **"the University Claim"** means a third-party claim, suit, or proceeding alleging that the Customer Content, when processed or used as allowed under this Agreement, violates, misuses, infringes, or misappropriates the intellectual property, propriety, privacy, or other rights of a third-party.

6.3 Tendering Claims. A party seeking indemnification hereunder (**"Indemnitee"**) must promptly notify in writing the other party (**"Indemnitor"**) of any claim for which defence and indemnification are sought per this Section 6. Each party agrees that it will not, without the other's prior written consent, enter into any settlement or compromise of any claim that: (a) results, or creates a likelihood of a result, that in any way diminishes or impairs any right or defence that would otherwise exist absent such settlement or compromise; or (b) constitutes or includes an admission of liability, fault, negligence or

wrongdoing on the part of the other party. Indemnitor has the sole right to control the defence of any claim for which it is providing indemnification hereunder with its choice of counsel, and such control extends to all negotiations relating to the settlement of any such claim (except that Indemnitor may not make any admissions on Indemnatee's behalf or settle the claim unless the settlement unconditionally releases Indemnatee of all liability). Indemnatee understands that Indemnitor's obligations under this Section 6 is limited to the extent a court of final jurisdiction finds that Indemnatee contributed to the claim. Indemnatee may, at its own cost and expense and election, participate in the defence of any such claim. To the extent covered under this Section 6, indemnification is each party's sole and exclusive remedy under this Agreement for any third-party claims.

6.4 Mutual Limitation to Obligations. Neither party's defence or indemnification obligations under this Agreement or the DPA will apply or will be comparatively reduced to the extent the underlying allegation arises from the Indemnatee's fraud, gross negligence, wilful misconduct, violation of any applicable law, or breach of any of its obligations under this Agreement. The University's defence and indemnification obligations will not apply or will be comparatively reduced to the extent a Customer Claim arises from: (a) any Customer Content if used by the University as permitted under this Agreement; (b) any modification to the Services made by Customer, its Authorised Users, or a party at the direction of Customer or its Authorised Users without the University's prior written consent if the Customer Claim would have been avoided in the absence of such modification; or (c) Customer's use of the Services in breach of this Agreement (any of the foregoing subsections (a) to (c) are "**Exclusions**").

7. Warranties and Disclaimers

7.1 Warranties. Each party warrants to the other that it is duly authorised to execute this Agreement and perform the obligations set forth herein. Customer warrants that it has all rights and permissions to grant to the University the license and rights in and to Customer Content expressly set out in this Agreement. The University warrants to Customer that (a) the University will not knowingly introduce any "back door," "time bomb," "Trojan horse," "worm," "virus," or other computer software routines within the Services that are intentionally designed to permit unauthorised access to or use of either the Services or Customer's computer systems. In the event of any breach of the foregoing warranties, the University will, as its sole liability and Customer's sole remedy diligently remedy any deficiencies that cause the Services, to not conform to the foregoing warranty. If the University determines this remedy to be impracticable or otherwise is unable to provide a workaround within thirty (30) days of Customer notifying the University of the defect, then Customer may terminate the relevant Order as an uncured material breach in accordance with Section 5.3 above. The University will

not be liable to the extent that any breach of the foregoing warranties is caused by any Exclusions.

7.2 Disclaimers. Except for the express warranties set forth herein, the Services are provided on an “AS IS,” “AS AVAILABLE” basis. To the maximum extent allowed under applicable law, the express warranties in this Agreement are the exclusive warranties offered by either party and neither party makes any warranties of any kind, whether express, implied, statutory, or otherwise, and each party disclaims all implied warranties, including, without limitation, any warranties of fitness for a particular purpose, accuracy, quiet enjoyment, title, non-infringement, merchantability and those that arise from any course of dealing or course of performance are hereby disclaimed. For clarity, Customer acknowledges that the Services may generate content using artificial intelligence techniques, and that such content may be inaccurate, incomplete, or require interpretation or verification. Customer and its Authorised Users are responsible for independently reviewing and verifying any AI-generated outputs and for determining their suitability for Customer’s and Authorised Users’ intended use.

8. Mutual limitations on liability

8.1 Aggregate liability and exclusion of certain types of damages.

(a) TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW AND SUBJECT TO SECTION 8.2 BELOW, THE TOTAL AGGREGATE LIABILITY OF EACH PARTY AND ITS SUPPLIERS AND LICENSORS RELATING TO, ARISING OUT OF, IN CONNECTION WITH, OR INCIDENTAL TO THIS AGREEMENT, WHETHER FOR BREACH OF CONTRACT, BREACH OF WARRANTY, OR ANY OTHER CLAIM WILL BE LIMITED TO THE ACTUAL AND PROVEN DIRECT DAMAGES INCURRED, UP TO THE AGGREGATE AMOUNTS PAID OR PAYABLE BY CUSTOMER HEREUNDER AND ALL ORDERS DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE INCIDENT GIVING RISE TO THE APPLICABLE CLAIM. THE EXISTENCE OF MULTIPLE CLAIMS OR SUITS UNDER OR RELATED TO THIS AGREEMENT WILL NOT ENLARGE OR EXTEND THIS LIMITATION OF DAMAGES.

(b) TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW AND SUBJECT TO SECTION 8.2 BELOW, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT OR PUNITIVE DAMAGES, LOST PROFITS OR LOST REVENUE ARISING OUT OF OR RELATED TO THE SUBJECT MATTER OF THIS AGREEMENT OR THE USE OF OR INABILITY TO USE THE SERVICES. THE FOREGOING EXCLUSION AND LIABILITY LIMITATIONS APPLY EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IN THE EVENT OF STRICT OR PRODUCT LIABILITY.

8.2 Exceptions and interpretation.

(a) Notwithstanding anything to the contrary in this Agreement and to the maximum extent allowed under applicable law, Section 8.1 above will not apply to: (i) the amounts incurred by a party when acting as an Indemnitor under Section 6 above; (ii) Customer's obligation to pay all Fees due under this Agreement and all Orders; or (iii) actual and proven damages incurred by a party arising from the other party's intentional misconduct, fraud, or gross negligence. Notwithstanding anything to the contrary in this Agreement and to the maximum extent allowed under applicable law, a party's aggregate liability to the other arising out of claims pursuant to: (A) its breach of its confidentiality obligations as a Receiving Party set forth in Section 9 below, will be limited to actual and proven damages in an amount not to exceed one (1) time the amount paid or payable by Customer to the University under this Agreement during the 12-month period immediately preceding the incident giving rise to the claim; and (B) a breach of its obligations under the DPA will be in accordance with limitation of liability terms set forth in the DPA.

(b) The parties agree that: (i) for purposes of this Agreement and the DPA, a breach of confidentiality claim described in Section 8.2(a)(A) is distinct and separate from a breach of DPA claim described in Section 8.2(a)(B); (ii) the limitations in Sections 8.1(a) and 8.1(b) above are independent of each other; and (iii) the limitation of damages set forth in Section 8.1(a) shall survive any failure of essential purpose of the limited remedy in Section 8.1(b). The parties agree that they have entered into this Agreement in reliance on the terms of this Section 8, and these terms form an essential basis of the bargain between the parties.

9. Mutual confidentiality obligations

9.1 Meaning of Confidential Information. Each party (as "**Receiving Party**") agrees that all code, inventions, know-how, business, technical, and financial information it obtains from the disclosing party ("**Disclosing Party**") constitute the confidential property of the disclosing party (together, "**Confidential Information**"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be Confidential Information due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any Service performance information, pricing terms, and documentation is deemed Confidential Information of the University. Customer Content is deemed Customer's Confidential Information.

9.2 Standard of care. Except as expressly authorised herein, the Receiving Party will hold in confidence and not use or disclose any of the Disclosing Party's Confidential Information for any purpose outside the scope of this Agreement, will use the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but in no event less than reasonable care), and will limit access

to Confidential Information of Disclosing Party to those of its employees, contractors, advisors, and agents with a need to know or who need access for purposes consistent with this Agreement and who are bound by confidentiality obligations at least as protective to those in this Agreement. The Receiving Party's nondisclosure obligation will not apply to information which the Receiving Party can document: (a) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (b) is or has become public knowledge through no fault of the Receiving Party; (c) is rightfully obtained by the Receiving Party from a third-party without breach of any confidentiality obligation; or (d) is independently developed by employees or contractors of the Receiving Party who had no access to such information.

9.3 Compelled disclosure and equitable relief. A Receiving Party may disclose Confidential Information if required pursuant to a regulation, law, or court order, but only to the minimum extent required to comply with such regulation or order and with advance notice to the Disclosing Party. The Receiving Party acknowledges that disclosure of Confidential Information could cause substantial harm for which damages alone would not be a sufficient remedy, and therefore upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law in any court of competent jurisdiction.

10. General Provisions

10.1 Notices. Either party may give notice to the other party by means of electronic mail which will constitute written notice under this Agreement. Customer must give notice to the University in writing to cogniti@sydney.edu.au. The University will provide notice to Customer at the email address designated on the most current Order (or the then-current address provided by Customer).

10.2 Additional or amended terms. The parties may amend or supplement the terms of this Agreement at any time by signing a written addendum, which is deemed incorporated by this reference upon execution. Unless expressly stated otherwise in an applicable addendum, all addenda will terminate upon the expiration or termination of this Agreement. The University will not be bound by any subsequent terms, conditions or other obligations included in any Customer purchase order, vendor portal, receipt, acceptance, confirmation or other correspondence from Customer unless expressly assented to in writing by the University and counter-signed by its authorised agent.

10.3 Dispute Resolution, Governing Law and Venue.

(a) If a dispute arises out of or in connection with this Agreement or any Order, the parties must first attempt to resolve it through good-faith negotiations between senior representatives of each party.

(b) If the dispute is not resolved within thirty (30) days after written notice of the dispute, either party may refer the dispute to mediation. Mediation will take place in New South Wales and be administered by a mediator agreed by the parties, or if the parties cannot agree, appointed by the Resolution Institute.

(c) If the dispute is not resolved within thirty (30) days after the appointment of a mediator (or such longer period as the parties agree in writing), either party may commence court proceedings.

(d) This Agreement is governed by the laws of New South Wales, and the parties submit to the exclusive jurisdiction of the courts of New South Wales.

(e) Nothing in this section prevents either party from seeking urgent injunctive or equitable relief from a court of competent jurisdiction.

10.4 Change control.

(a) The University may change the Services, pricing, or the terms of this Agreement. The University will provide Customer with at least thirty (30) days' written notice of any material change that adversely affects Customer's existing Subscription, unless a longer notice period is required by applicable law.

(b) Unless the parties agree otherwise in writing in the relevant Order, any material change that adversely affects an existing Subscription will take effect only upon renewal of the applicable Subscription Term, and will not apply during the then-current Subscription Term.

(c) For clarity, changes that do not materially reduce the functionality, security, or performance of the Services, or that are required to comply with applicable law or regulatory requirements, may be implemented during a Subscription Term.

10.5 Assignment. Neither party may assign its rights or delegate obligations hereunder to a third-party except (a) as may be expressly permitted in this Agreement or an Order, (b) to a successor-in-interest pursuant to a merger, acquisition, reorganisation, or sale of all or substantially all of such party's assets, or (c) in the case of University, to a company spun out from the University, provided that such entity executes a written agreement assuming all of the University's rights and obligations under this Agreement, upon which the University will be released its obligations under this Agreement. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties' respective successors and permitted assigns.

10.6 Trade mark rights. Customer agrees that the University may identify Customer as a University customer in or on the University's website or other promotional materials. The University's use of Customer's name and logo will be in accordance with any Customer supplied guidelines. Upon Customer's written request, the University will remove Customer's name or any Customer marks from the University's website, and to

the extent feasible, any the University marketing materials. Customer owns and retains all rights in and to its name, logo, and other trademarks.

10.7 Third-party systems. Customer understands that while the Services integrates with many third-party systems, the University isn't responsible for applications, services, software, or other products supplied by a third-party (excluding the University's licensors and contractors engaged to provide services or technology to deliver the Services) (each a "**Third-party Service**") that Customer chooses to integrate with the Service (including, without limitation, a learning management system, third-party communication service) even if Customer uses the University's API to enable the integration with a Third-party Service. Use of a Third-party Service is subject to the terms of the agreement between Customer and the Third-party Service provider.

10.8 Miscellaneous. The failure of either party to enforce any right or provision in this Agreement will not constitute a waiver of such right or provision. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be modified by the court and interpreted to best accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement will remain in effect. Except as otherwise provided in this Agreement, there are no third-party beneficiaries under this Agreement. Any claims brought against the University may only be brought by the Customer entity that executed the relevant Order. No joint venture, partnership, employment, agency, or exclusive relationship exists between the parties as a result of this Agreement or use of the Services. Customer agrees that its purchase of the Services under this Agreement is neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by the University regarding future functionality or features. Each party will comply with the export laws and regulations of Australia and other applicable jurisdictions in providing and using the Services. Without limiting the foregoing, (a) each party represents that it is not named on any Australian government list of persons or entities prohibited from receiving exports, and (b) Customer will not permit any Authorised Users to access or use the Services in violation of any Australian export embargo, prohibition, or restriction. Customer agrees not to export, re-export or transfer any part of the Services in violation of export laws and regulations.

10.9 Entire agreement. This Agreement, together with all Orders comprises the entire agreement between Customer and the University and supersedes all prior or contemporaneous negotiations, discussions, or agreements, whether written or oral, between the parties regarding the subject matter contained herein.

Privacy Policy

Thank you for taking the time to read this Privacy Policy. This Privacy Policy applies to the personally identifiable information that the University of Sydney (“**the University**,” “we”, “us,” or “our”) collects or receives through our interactions with you, your use of our website **app.cogniti.ai**, Cogniti software application, or other websites that we link this Privacy Policy to (“**Site**”), your use of any University service, application, platform, and other products that display or link to this Privacy Policy, your registration or attendance to any of our demonstrations, webinars, or other events related to Cogniti (collectively, “**Services**”).

This Privacy Policy describes the information that we collect, how we use it, how we protect it, and the choices you can make about your information. If you do not agree with any of the terms of this Privacy Policy, you should immediately stop using our Services and the Site.

This Privacy Policy does not apply to personal information that has been aggregated and anonymised where such information is no longer capable of identifying a specific individual.

Information We Collect

The University collects the following types of personally identifiable information in the manner described below.

1. **Information You Provide to Us.** You may voluntarily provide us with personally identifiable information, including: (a) your name, email address, and any other information that you provide when you access the Site or Services, register to use the Site or a Service, or fill out forms that we make available via the Site or Services; (b) information that you provide to us when you contact us, including when you communicate with any automated support service we may offer from time to time; or (c) any other information you voluntarily provide us while using the Site or Services, including documents, and document metadata.
2. **Information We Collect Automatically.** We automatically collect information that may personally identify you through tracking technologies (see the section “Cookies, Other Storage and Web Beacons” for more information). We collect the following types of information automatically through tracking technologies: Your Internet Protocol address; Domain name of your Internet service provider; Your approximate geographic location; The website you came from, the pages that you visit on the Site, and the time of your visit to the Site; Information about your Internet connection, browser, or similar kinds of information; and Aggregated information that cannot be used to specifically identify you when you

use or visit the Site or a Service that may be combined with information that does identify you.

We may combine the information we collect from or about you with information that we receive from other sources and use it in the manner described in this Privacy Policy.

How We Use Your Information

Your personal information is not used to train artificial intelligence models.

The University uses the personally identifiable information that we collect for the following purposes:

1. The purposes for which you provided it, including, provide you a demo, the Site or the Service, invite you to an event, or provide you access to content related to the Services;
2. To administer and provide you with information about your account, including, updated Site or Service terms or for billing and accounting purposes;
3. To send you information about your relationship with us;
4. To inform you about upcoming events or webinars or new features, products, or services;
5. To develop new products, features and services;
6. To conduct research and development endeavours that aid understanding of usage and impact that aid Service development and improvement;
7. To process and respond to your inquiries or comments;
8. To personalise and enhance your experience using the Site and Services;
9. To manually review your documents for the purposes of improving the Services, including, but not limited to, the quality and completeness of your document metadata;
10. To generate and review reports and data about our user base and service usage patterns;
11. To deliver targeted communication to you relating to the Services;
12. To determine the effectiveness of our communications;
13. To compile aggregated and fully anonymised data for the purposes of improving and extending the Site or Services, including, but not limited to, securing the Site and Services;

14. For legal reasons, including to carry out our legal obligations and enforce our rights, investigate misuse or misconduct, protect you or other third parties, to monitor, detect and prevent fraud, malicious activity, or for other privacy or security-related concerns;
15. With your consent, to fulfill the purposes for which you provided the information, or in ways that we disclose to you when you provide the information; and
16. To administer, operate and improve the Site and Services and for internal business purposes.
17. To investigate and protect against fraudulent, harmful, unauthorised, or illegal activity.

How Your Information is Disclosed

Personally identifiable information may be disclosed to third parties in accordance with this Privacy Policy, and, if applicable, subject to the terms of your agreement with us if you are a Cogniti user. You may choose not to share certain information as described in the “Your Choices Regarding Your Information” section below.

1. **Third-Party Service Providers.** We may use third-party service providers and business partners to perform functions in connection with the Site or Services. Examples include running our Services on cloud providers, using account management ticketing products, and sending you email notifications via messaging providers. The categories of third parties we may share personal information with may include but are not limited to: Cloud Computing Services; Data Storage Service Providers; Performance Monitoring Tools; Testing Tools; Website Hosting Service Providers. Our hosting and AI processing provider is Microsoft Azure, and our database provider for the hosted service is MongoDB Atlas. A current list of our sub-processors is in Annex C of our Data Processing Addendum.
2. **Business Partners.** We may share your information with third party business partners, including referral partners, resale partners, or similar kinds of business partners.
3. **Third Party Social Media or Analytics Services.** We may use cookies, pixels, or other tracking technologies provided by third party providers, including, without limitation, Google or LinkedIn, these third parties may use the personally identifiable information that they receive from automatic tracking technology on our Site for their own purposes. Please see the section titled “Cookies, Other Storage, and Web Beacons” below and our Cookie Policy for more information.
4. **Business Changes.** If we become involved in a merger, acquisition, sale of assets, bankruptcy, reorganisation, dissolution, or other transaction or if the

ownership of all or substantially all of our business otherwise changes, we may transfer your information to a third-party or parties in connection therewith.

5. **For Legal Purposes.** We reserve the right to investigate fraud, abuse, illegal activities, violation of our policies or terms and conditions, or security incidents. We may disclose information about you to third parties if we have a good faith belief that such disclosure is reasonably necessary to: Take action regarding suspected illegal activities; Enforce or apply this Privacy Policy, our policies or terms and conditions; Comply with the law or guidance and cooperate with government or law enforcement officials or private parties; Protect our rights, reputation, safety, and property, or that of users or other third parties; Respond to claims and legal process (for example, subpoenas); and/or Protect against legal liability.

Cookies, Other Storage, and Web Beacons

We, along with our third-party service providers, third party advertising, social media, or analytics service providers, and business partners, use cookies, web beacons, and other tracking technologies on the Site and Services. These technologies are used to deliver the features and functionality of the Service and the Site, including tracking, analytics and personalisation, and optimisation of the Site and Services. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our [Cookie Policy](#).

Security

We protect personal information with encryption in transit and at rest, access controls, security monitoring, and regular independent security testing, as described in our Data Processing Addendum. While we have implemented security measures to protect the information we process, we cannot guarantee against loss, theft and unauthorised use, disclosure, or modification. No transmission over the Internet or email is ever fully secure or error free. You should use caution whenever submitting information online and take special care in deciding what information you provide us.

To the extent permitted under applicable law, we assume no liability or responsibility for disclosure of your information due to errors in transmission, unauthorised access by third parties, or other causes beyond our control. By using our Services, you acknowledge and accept that your use of our Services is ultimately at your own risk.

Please note that you are responsible for managing access to any accounts that you use to access our Services. Failure to limit access to your devices or browser might enable third parties to have unauthorised access to your personal information.

Data breaches

If we become aware of a data breach affecting your personal information that is likely to result in serious harm, we will notify the affected institution and, where required, the Office of the Australian Information Commissioner or other regulators, in accordance with the Privacy Act 1988 (Cth) and our Data Processing Addendum.

Links to Other Sites

This Privacy Policy applies only to the Site and Services. The Site may contain links to third-party websites that we do not own or operate. We do not guarantee that we have endorsed or reviewed any links to third-party websites. The policies and procedures we describe here do not apply to third-party websites. We cannot control nor are we responsible for the privacy practices or content of these third-party websites. We suggest contacting these websites directly for information on their privacy policies and practices.

Your Choices Regarding Your Information

You have choices regarding the use of information on our Site and Services. You may have additional rights, as explained below, if you are a resident of the European Economic Area, Switzerland, Canada, certain U.S. states.

1. **Changing Your Information.** You may log into the Service to modify certain profile information that you have provided at any time.
2. **Email Communications.** To change your information regarding certain email communications, please unsubscribe from the footer of that communication. However, we may still communicate with you — for example, to send you service-related messages that are necessary for the administration and use of your account, to respond to support requests, or for other purposes related to providing the Service to you.
3. **Cookies, Other Storage, and Web Beacons.** Please see the “Cookies, Other Storage, and Web Beacons” section above.
4. **Closing Your Account.** Subject to the terms of your agreement with us, you may close your Cogniti account by contacting your account administrator or contacting us at cogniti@sydney.edu.au. Note that even if you request to close your Cogniti account, you may still have obligations under any subscription agreement with us.
5. **Withdrawing Consent.** If we have relied on your consent to process your personal information (which may be express and/or implied consent depending on the applicable law), you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us at cogniti@sydney.edu.au.

EU Data Subject Rights

If you are a resident of Switzerland, the United Kingdom, or a country within the European Economic Area (EEA), you may have rights under European data protection laws regarding the processing of your personal information. You have the right to access the personal information that we process, and, in some cases, you may have the right to ask that your personal information be corrected, erased, or transferred (subject to limitations under applicable law). You may also have the right to object to or request that we restrict the processing of your personal information. If we collect personal information based on your consent, you have the right to revoke your consent.

If your Personal Information has been submitted to us by a Cogniti user and you wish to exercise any rights you may have under applicable data protection laws, please inquire with the applicable Cogniti user directly.

Residents of the United Kingdom, any country within the EEA, or Switzerland may file a complaint with a data protection authority. The data protection authority will require you to first attempt to resolve any complaint with us. Any other dispute arising out of or related to this Privacy Policy will be handled in accordance with the dispute resolution process indicated in our terms of service or website terms, as applicable.

1. **Lawful Basis.** If you reside in the European Economic Area or Switzerland (collectively the “EU”), where we are the data controller we rely on the following lawful grounds under the General Data Protection Regulation, the United Kingdom General Data Protection Regulation, or the Swiss Data Protection Act (collectively referred to in this Privacy Policy as “GDPR”) to process (collect, store, and use) your personal information: (a) it is necessary for the performance of a contract with you; (b) our or a third-party’s legitimate business interest; (c) your consent; or (d) our vital interests. Our Cogniti users determine the lawful grounds for the processing of personal information submitted through their use of our Services and we limit such processing to our Cogniti users’ instructions.
2. **Data Transfer Notice.** We are located in Australia and transfer your personal information for processing in Australia. We make the transfer to Australia in the absence of an adequacy decision because it is necessary for the performance of a contract with you, or with your explicit consent. We also use model contractual clauses (or the then-lawful data transfer mechanism recognised under GDPR or other applicable law) with our Cogniti users to provide adequate protection for the transfer and processing of your personal information in Australia. We also use the model contractual clauses with our subprocessors to provide adequate protection for the transfer and processing of your personal information.
3. **Overseas disclosure.** Cogniti and its data are hosted in Australia. Our subprocessors are listed in Annex C of our Data Processing Addendum. Microsoft,

MongoDB and HubSpot process data in Australia; Google processes pseudonymised website analytics globally, including in the United States. Where we disclose personal information overseas we take reasonable steps to ensure the recipient handles it in accordance with the Australian Privacy Principles.

4. **Individual Rights and Data Requests.** Depending on your location, your jurisdiction, and subject to applicable law, you may have the rights below with regard to the Personal Information we control about you. We will respond to your requests within the appropriate timeline under applicable law:

The right of access means that you have the right to request that we disclose what personal information we have collected, used and disclosed about you;

The right of deletion means that you have the right to request that we delete personal information collected or maintained by us, subject to certain exceptions.

The right to non-discrimination means that you will not receive any discriminatory treatment when you exercise one of your privacy rights;

You can also ask us to correct or update your personal information, object to the processing of your Personal Information, ask us to restrict processing of your personal information or request the portability of your personal information;

While you cannot opt out of service-related emails if you are an account holder, as this is an essential part of the Services, you have the right to opt-out of marketing communications we send you at any time. You can exercise this right by clicking on the “unsubscribe” or “opt-out” link in the marketing e-mails we send you, or you can contact us using the contact information below;

If our lawful basis is your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your Personal Information conducted in reliance on lawful processing grounds other than consent; and

You have the right to complain to a data protection authority about our collection and use of your personal information.

5. **Exercising Your Rights.** We provide features in our Services to allow Cogniti users to respond directly to data subject requests to access, transfer, rectify or erase their personal information, or to restrict or object to the processing of their

personal information. You may also contact us at cogniti@sydney.edu.au to request access to, transfer of, and rectification or erasure of your personal information, or restriction of processing, or to object to processing of your personal information, to the extent that we process such information on our own behalf. Please specify the nature of your request and the information that is the subject of your request. We may require you to submit additional information necessary to verify your identity and status as an EU data subject. If we are processing your personal information for a Cogniti user, we will forward your request to our Cogniti user and assist the Cogniti user in responding within 30 days. If you are a Cogniti user, we will respond to your request directly within 30 days. If we are processing your personal information based upon the lawful ground of your consent, you have the right to withdraw your consent for such processing at any time without affecting the lawfulness of processing based on consent before it is withdrawn. To withdraw consent, please email us at cogniti@sydney.edu.au.

6. **Retention.** At a minimum and to the extent allowed under applicable law, we will retain your personal information for as long as necessary for the purpose in which it was collected, such as to deliver a Service, perform our obligations under a contract, for our or a third party's legitimate interest, or your consent.

US State Privacy Law Rights

California Resident Privacy Rights

If you are a California resident, the California Consumer Protection Act (CCPA), as amended by the California Privacy Rights Act (CPRA), may provide you with additional rights regarding your personal information. The rights outlined in this section do not apply to information exempted under the CCPA, including aggregated data, or to individuals who are not residents of California.

To the extent provided under the CCPA, and subject to applicable exceptions, California residents have a right to request information about our collection, use, and disclosure of their personal information. Specifically, California residents have the following rights:

1. The right to know the categories and specific personal information we have collected, the categories and sources from which we collected the personal information, the categories of third parties with whom we share personal information, and the business or commercial purpose for collecting or selling (if applicable) personal information;
2. The right to request a copy of the personal information that we collected during the past 12 months;

3. The right to opt out of sales of personal information or sharing personal information for cross-contextual behavioural advertising (in each case, where applicable and in accordance with CCPA);
4. The right to request that we delete the personal information that we have collected from you, subject to certain exceptions;
5. The right to correct inaccurate personal information that we maintain about you;
6. The right to limit the disclosure of your sensitive personal information, if we use or disclose sensitive personal information;
7. The right to request information about and opt out of automated decision making (if applicable); and
8. The right to exercise the rights described above free from discrimination or retaliation, as prohibited by the CCPA.

California privacy laws define a “sale” as disclosing or making available to a third party, personal information in exchange for monetary or other valuable consideration, and “sharing” includes disclosing or making available personal information to a third party for purposes of cross-context behavioural advertising. We do not disclose personal information to third parties in exchange for monetary compensation. As defined by CCPA, we may “sell” or “share”: (a) Category A “Identifiers,” (b) “Personal Information, as Defined in the California Customer Records Law,” (c) Category D “Commercial information,” (e) Category F “Internet or Other Similar Network Activity Information,” and (f) Category K “Inferences Drawn from Other Personal Information,” to or with third-party analytics providers. We do not “sell” or “share” (as defined by the CCPA) sensitive personal information, nor do we “sell” or “share” any personal information about individuals who we know are under 16 years old.

We have collected the following categories of personal information in the past 12 months:

Category	Examples	Collected
A. Identifiers	Contact details, such as name, Internet Protocol address, email address	YES
B. Personal information categories listed in the California Customer Records statute	Name, contact information	YES

C. Protected classification characteristics under California or federal law	Gender, date of birth, race, disability	NO
D. Commercial information	Transaction information, purchase history related to Cogniti	YES
E. Biometric information	Fingerprints and voiceprints	NO
F. Internet or other similar network activity	Interactions with our website/applications and systems	YES
G. Geolocation data	Device location (not precise geolocation)	YES
H. Audio, electronic, visual, thermal, olfactory, or similar information	Images and audio, video or call recordings created in connection with our business activities	NO
I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level or job with us	NO
J. Education Information	Records about students	YES
K. Inferences drawn from other personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's learning preferences and educational characteristics	YES
L. Sensitive Personal Information	Social security number, government issued ID, financial account information, health, genetics, or biometric information, precise geographic location, contents of electronic messages, information	NO

	about race religion, or trade union membership, or sexual orientation.	
--	--	--

We have disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months: (a) Category A “Identifiers,” (b) Category B “Personal Information, as Defined in the California Customer Records Law,” (d) Category D “Commercial Information,” (e) Category F “Internet or Other Electronic Network Activity Information,” (f) Category I “Professional or Employment Information,” Please see the section “How Your Information is Disclosed” above for more information.

Exercising Your US Privacy Rights

California residents may exercise their CCPA rights by contacting us by email as indicated in the “Contact Us” section below. Your rights may only be exercised by you or by your designated agent. You may only submit a CCPA request to know twice within a 12-month period.

Your request must include enough information to allow us to reasonably verify that you are the person about whom we collected personal information or an authorised representative, which may include: (a) verifying your account information if you have an account with us; or (b) requesting two forms of identification that are reliable for verification purposes, unless the request includes sensitive information and, in which case, we may require three forms of verification and a signed declaration. The information included in your request must allow us to properly understand, evaluate, and respond to it.

We cannot respond to your request if we cannot verify your identity or authority to make the request and confirm that the personal information relates to you. If we cannot verify your identity or authority, we will not fulfill your request. We will only use personal information provided in the request to verify the requestor’s identity or authority to make it.

You may submit a request through a designated agent. You must instruct that agent that they will need to state that they are acting on your behalf when making the request, have reasonably necessary documentation, and be prepared to provide the necessary personal information to identify you in our database.

Children

Our Services are not intended for minors under the age of 18 without parental or guardian consent. We do not knowingly collect information from children under 18. By using our Services, you represent that you are at least 18 or that you are the parent or

guardian of such a minor and consent to their use of our Services. If you are a parent or guardian and believe your child under the age of 18 has used our Services and provided personal information to us through our Services without your consent, please contact us immediately at cogniti@sydney.edu.au, and we will take reasonable measures to delete this information.

Data Retention

How long we retain your information depends on the type of data and the purpose for which we process the data. We will retain your information for the period necessary to fulfill the purposes outlined in this Privacy Policy and our agreement with you unless a longer retention period is required or permitted by applicable law.

Rights of Cogniti users

If you have purchased a subscription to a Service that is subject to and governed by a separate agreement between you and the University, to the extent that there's a direct conflict between this Privacy Policy and the terms of that agreement, the terms of that agreement will control and supersede this Privacy Policy.

Complaints

If you believe we have breached the Australian Privacy Principles or this Privacy Policy, contact us at cogniti@sydney.edu.au or the University of Sydney Privacy Officer at privacy.enquiries@sydney.edu.au. We will acknowledge your complaint within 5 business days and aim to respond within 30 days. If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (www.oaic.gov.au). Residents of the United Kingdom, the EEA or Switzerland may also complain to their local data protection authority.

Changes to Privacy Policy

We reserve the right to update or modify this Privacy Policy at any time and from time to time to ensure it's easy to understand, aligns with our current practices and operations, and complies with continually evolving laws and regulations. Please review this Privacy Policy periodically, and especially before you provide any information. Your continued use of our Site and Services constitutes your agreement to this Privacy Policy and any updates to this Privacy Policy.

How to Contact Us

If you have any questions about our Privacy Policy or requests regarding your personal information, please email cogniti@sydney.edu.au.

Cookies and Similar Technologies

This Cookie Policy explains how the University of Sydney (“**the University**,” “we,” “us,” or “our”) uses cookies and other similar technologies to recognise when you visit our website at cogniti.ai or use the Cogniti software application (“**Cogniti**,” “our Website”). This Cookie Policy describes what these technologies are, why we use them, and your rights to control our use of them. Capitalised terms used herein and not defined will have the meaning given to such terms in our Terms of Service or Privacy Policy.

What are cookies?

Cookies are small data files placed on your computer or mobile device when you visit a website. Website owners widely use cookies to make their websites work, to work more efficiently, and to provide reporting information. Cookies set by the website owner (in this case, the University of Sydney) are called “first-party cookies.” Cookies set by parties other than the website owner are called “third-party cookies.” Third-party cookies enable third-party features or functionality on or through the website (e.g. analytics). The parties that set these third-party cookies can recognise your computer when it visits our Website and certain other websites.

Why does Cogniti use cookies and other Similar Technology?

A lot of different reasons. Some cookies are required for technical reasons for our Website to operate, and we refer to these as “essential” or “necessary” cookies. Other cookies also enable us to perform analytics of usage patterns. This is described in more detail below.

What types of cookies are there?

ESSENTIAL OR NECESSARY COOKIES

These cookies are needed to help you access and move around our Website. Without these cookies, our Website would not work, and you would not be able to use some critical features. They include cogniti_session (your authenticated session; expires within 24 hours) and the cookie-consent preference cookie (records your cookie choices; retained for 180 days).

PERFORMANCE AND FUNCTIONALITY COOKIES

These cookies are used to remember your choices on the Websites. These preferences are remembered using persistent cookies so that you will not have to set them again the next time you visit our Website.

ANALYTICS COOKIES

These cookies help us understand how our Website is being used so that we can make improvements. These cookies can provide anonymous information to help us understand which parts of our Website interest our users and if they experience any errors. Analytics cookies (Google Analytics) are set only after you accept analytics cookies in the consent banner, and only on deployments where analytics is enabled. You can change your choice at any time from the cookie settings link.

How can I control cookies on my browser?

As to how you can refuse cookies through your web browser controls, which vary from browser to browser, you should visit your browser's help menu for more information. Please note that disabling cookies may impair the Website's functionality for you, or render it inoperable.

What about other tracking technologies, like web beacons?

Cookies are not the only way to recognise or track visitors to a website. We may use other, similar technologies from time to time, like web beacons (sometimes called "tracking pixels" or "clear gifs"). These tiny graphics files contain a unique identifier that enables us to recognise when someone has visited our Website or opened an email including them. This allows us, for example, to monitor the traffic patterns of users from one page within a website to another, to deliver or communicate with cookies, to improve site performance, and to measure the engagement with email campaigns. These technologies often rely on cookies to function correctly, so declining cookies will impair their functioning.

How often will you update this Cookie Policy?

We may update this Cookie Policy from time to time to reflect, for example, changes to the cookies we use or for other operational, legal, or regulatory reasons. Therefore, please revisit this cookie policy regularly to stay informed about our use of cookies and related technologies. The date at the top of this Cookie Policy indicates when it was last updated. If you have any questions about our use of cookies or other technologies, please email us at cogniti@sydney.edu.au.

Data Processing Addendum

This Data Processing Addendum, including the selected modules of the Standard Contractual Clauses and the attached Annexes (this “**DPA**”) supplements the Cogniti Subscription Agreement or other agreement entered into between the University of Sydney and Customer, including all Orders entered into between the parties.

The Cogniti Subscription Agreement and all Orders will be referred to in this DPA as the “**Agreement**.” The Agreement governs the provision, use, and purchase of Cogniti products and services described in the Agreement (“**Services**”). This DPA addresses the specific requirements of Applicable Data Protection Laws and applies solely to the extent that Customer uses a Cogniti Service that processes Data subject to an Applicable Data Protection Law.

1. Definitions

In this DPA, the following terms shall have the meanings below. Any capitalised terms used herein and not defined will have the meanings given to such terms in the Agreement.

“**Applicable Data Protection Law**” means all international, federal, national, and state privacy and data protection laws that apply to the processing of Personal Data that is the subject matter of the Agreement (including but not limited to, where applicable, European Data Protection Law and U.S. Data Protection Law (as defined below)).

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, as amended by the California Privacy Rights Act (“CPRA”), and its implementing regulations.

“**Controller**” means the entity that determines the purposes and means of the processing of Personal Data.

“**Customer**” means the legal entity that entered into and signed an Order with the University for the purchase and use of the Services.

“**Data Subject**” means a natural person whose Personal Data is processed in the context of this DPA.

“**European Data Protection Law**” means: (i) prior to 25 May 2018, the EU Data Protection Directive 95/46/EC, and any applicable national implementation of it; (ii) on and after 25 May 2018, the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation)(“**EU GDPR**”); (iii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom’s

European Union (Withdrawal) Act 2018 (the “**UK GDPR**”); (iii) the E.U. e-Privacy Directive (Directive 2002/58/E.C.); and (iv) the Swiss Federal Data Protection Act (“**Swiss DPA**”).

“**Personal Data**” shall have the meaning given to such term under Applicable Data Protection Law, but generally means any information relating to an identified or identifiable natural person where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Processor**” means an entity that is engaged to process Personal Data on behalf of the Controller, including, as applicable, any “service provider” as that term is defined by the CCPA.

“**Security Incident**” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data (as defined in Section 2.1 below) transmitted, stored, or otherwise processed by the University or its Sub-Processors. “Security Incident” does not include unsuccessful attempts or activities that do not compromise the security of Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“**Standard Contractual Clauses**” means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (E.U.) 2016/679 of the European Parliament and of the Council (“**EU SCCs**”); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (“**UK SCCs**”); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (“**Swiss SCCs**”).

“**Sub-Processor**” means an entity engaged by the Processor to process Data on behalf of, and under the instructions of, the Controller in connection with the provision of the Service. Sub-Processors exclude employees, consultants, or independent contractors of the University where such individual performs services equivalent to those performed by an employee.

“**U.S. Data Protection Law**” means the data protection or privacy laws and regulations applicable to the processing of Personal Data in force within the United States, including, but not limited to, (i) the CCPA, (ii) the Virginia Consumer Data Protection Act (“**VCDPA**”), (iii) once in effect, the Colorado Privacy Act, Connecticut Act Concerning

Personal Data Privacy and Online Monitoring, Utah Privacy Act, and (iv) any rules or regulations implementing any of the foregoing.

2. General Data Processing Requirements

2.1 Relationship of the parties. As between the parties and for the purposes of this DPA, Customer is the Controller, with respect to E.U. Data Protection Law and VCDPA, and a “business” with respect to CCPA, of the Personal Data that is included in Customer Content (“**Data**”) and appoints the University as a Processor, with respect to E.U. Data Protection Law and VCDPA, and a “service provider” with respect to CCPA, to process Data on behalf of Customer.

2.2 Responsibilities of the parties. The University will not sell Personal Data as the term “sell” is defined by the CCPA. The University will not disclose or transfer Personal Data to other parties that would constitute “selling,” as the term is defined by the CCPA. Customer shall comply with its obligations under Applicable Data Protection Law, including, but not limited to, providing notice to Data Subjects and obtaining Data Subjects’ consent for processing of Data Subjects’ Personal Data, where required. Customer represents that its use of the Service will: (i) not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data to the extent applicable under the CCPA; and (ii) not violate the rights of any Data Subject that has not opted into the processing of sensitive personal data to the extent applicable under the VCDPA. Customer, as a Controller or as a “business,” (as defined by the CCPA) is responsible for: (i) the accuracy, quality, and legality of the Data; (ii) how Customer acquired Data; (iii) the instructions Customer provides to the University regarding the processing of Data; (iv) providing all legally required notices to individuals and obtaining all legally required consents which may be necessary for the University to process Data; (v) ensuring that Customer’s processing instructions are lawful and do not violate Applicable Data Protection Laws; and (vi) ensuring that Data is provided to the University for a valid “Business Purpose,” as defined in the CCPA. Customer will not provide or make available to the University any Data in violation of the Agreement or provide any Data that is inappropriate for the nature of the Services. Customer is solely responsible for informing students and other Data Subjects about the processing of their Personal Data in the Services and for obtaining all required consents or authorisations under Applicable Data Protection Law, including any obligations relating to student privacy.

2.3 Processing instructions; Purpose limitation.

2.3.1 The University shall process the Data as a Processor in accordance with the documented instructions of Customer (including those in this DPA and the Agreement) or with Customer’s written instructions and only for the following purposes: (i) as necessary to perform the Services for Customer under the Agreement; (ii) to perform

any steps necessary for the performance of the Agreement; (iii) any processing initiated by an Authorised User in their use of the Service; and (iv) to comply with other reasonable, lawful instructions provided by Customer (e.g., via email, phone, support tickets, or online tool). Customer shall only give lawful instructions to the University that comply with Applicable Data Protection Law. **Annex A**, attached hereto, includes certain details of the processing of Data, as required under Applicable Data Protection Law.

2.3.2 The University may process Personal Data for its own legitimate business purposes, as an independent Controller, solely when the processing is strictly necessary and proportionate, and if the processing is for one of the following purposes:

- Billing, account and customer relationship management (including marketing communications), support, and related correspondence;
- Complying with and resolving legal obligations, tax requirements, and in connection with any disputes;
- Monitoring and protecting the confidentiality, privacy, and security of the Services;
- Internal reporting, financial reporting, revenue planning, and forecast modeling;
- Receiving feedback regarding the Services and incorporating feedback (excluding Personal Data) into product development; and
- other uses permitted by Customer in the Agreement or other terms entered into between the University and Customer.

2.3.3 The University will not use Personal Data or institution-identified data for training AI models. The University may use De-Identified Data for service improvement as permitted under the Agreement.

2.4 Confidentiality of processing. The University shall ensure that any person that it authorises to process Data (including the University's staff, agents, and subcontractors) shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process Data who is not under such a duty of confidentiality.

2.5 Security standards. The University shall implement appropriate technical and organisational measures intended to protect Data from: (i) accidental or unlawful destruction; and (ii) loss, alteration, unauthorised disclosure of, or access to Data. At a minimum, such measures shall include the security measures identified in **Annex B ("Security Measures")**. At a minimum, Customer's Personal Data will be encrypted in transit using TLS 1.2 or higher, and encrypted at rest using AES-256 or an equivalent industry-standard encryption method.

3. Sub-Processors and Subcontracting

3.1 Subject to the terms and conditions set forth in this DPA, Customer generally authorises the University to continue to use and disclose Data to Sub-Processors engaged by the University in the context of providing the Services and processing activities. Customer approves the use of Sub-Processors described in Annex C. The University remains fully liable for the acts error and omissions of its Sub-Processors in relation to the processing of Data to the same extent the University would be responsible if performing the processing itself.

The University will maintain an up-to-date list of third-party AI model providers and other subprocessors used in connection with the Services, which will be made available to Customer upon request or through a publicly accessible webpage. Such providers may include Microsoft Azure OpenAI or other AI services.

3.2 The University shall not subcontract any processing of Data to a third-party Sub-Processor unless: (i) such Sub-Processor is subject to an agreement with the University that contains data protection terms not less protective as those provided for by this DPA with respect to the protection of Data to the extent applicable to the nature of the service provided by such Sub-Processor, and, to the extent the CCPA applies, each written agreement with a Sub-Processor will comply with the CCPA, designate the Sub-Processor as a “service provider” or “contractor,” and prohibit the Sub-Processor from selling Customer’s Data or using Customer’s Data for any purpose not authorised by the CCPA; and (ii) the University provides Customer prior notice (where notice will be provided by the University by email or by an in-product notification within the Service) of the addition or replacement of such Sub-Processor (including the details of the processing it performs or will perform, and the location of such processing) before authorising any new Sub-Processor(s) to process Customer’s Data in connection with the provision of the applicable Service.

Notwithstanding the foregoing, in the event of an emergency concerning Service availability or security, the University is not required to provide prior notice but shall provide notification within seven (7) business days following the change in Sub-Processor.

Customer will notify the University within ten (10) business days of receipt of the University’s notice of a new Sub-Processor if it objects to the addition or replacement of a Sub-Processor. Customer’s objection should be sent to cogniti@sydney.edu.au and explain the reasonable grounds for the objection. If Customer objects to the University’s appointment of a third party Sub-Processor on reasonable grounds relating to the protection of Data, and the University is unable to adequately address the reasonable grounds (e.g., make available to Customer a reasonable change to Customer’s configuration or use of the Service to avoid the processing of Data by the objected-to

new Sub-Processor without unreasonably burdening Customer), then the University will not engage the Sub-Processor, or Customer may elect to suspend or terminate its subscription to the impacted Service without penalty. If Customer does not object to a Sub-Processor within thirty (30) days of the University's notice as described in this Section 3, then the Sub-Processor will be deemed accepted by Customer.

4. International Transfers of Data

To perform the Services for Customer under the Agreement, the University may transfer Personal Data to the countries in which the Sub-Processors listed in Annex C process data. The University will ensure that such transfers are made in compliance with Applicable Data Protection Law and this Addendum. Customer authorises such cross-border Personal Data transfers and represents, warrants, and covenants that Customer will comply with any requirements under Applicable Data Protection Law regarding such Personal Data transfers. For such cross-border Personal Data transfers subject to Applicable Data Protection Law, the University and Customer agree to be bound by:

(i) in the case of GDPR, the EU SCCs then-current and applicable module and terms of the Standard Contractual Clauses published by the European Commission and located as of the date of this DPA at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

(ii) in the case of UK GDPR, the UK SCCs; and

(iii) in the case of Swiss DPA, the Swiss SCCs. In connection with the Standard Contractual Clauses referred to in (i) and (ii) of this Section 4, the parties agree to the following, as applicable:

The University will host Customer's Data primarily in Microsoft Azure's Australia East region. Customer acknowledges that limited transfers outside Australia may occur for support, resilience, or vendor processing purposes as permitted under Section 4 below, and such transfers will be conducted in compliance with Applicable Data Protection Law.

4.1 With respect to Data processed by the University pursuant to Section 2.3.1:

- Module Two of the EU SCCs will apply;
- in Clause 7, the optional docking clause will apply;
- in Clause 9, the Option 2 will apply;
- in Clause 11, the optional language will not apply;
- in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law;

- in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vi) Annex 1 will be deemed completed with the information set out in Annex A (Details of Processing) of this DPA;
- Annex 2 (Security Measures) will be deemed completed with the information set out in Annex B of this DPA; and
- Annex 3 (Sub-Processors) will be deemed completed with the information set out in Section 3 of this DPA.

4.2 With respect to Personal Data processed by the University pursuant to Section 2.3.2:

- Module One of the EU SCCs will apply;
- in Clause 7, the optional docking clause will apply;
- in Clause 11, the optional language will not apply;
- in Clause 17, the Standard Contractual Clauses will be governed by Irish law;
- in Clause 18(b), disputes shall be resolved before the courts of Ireland;
- Annex 1 will be deemed completed with the information set out in Annex A (Details of Processing) of this DPA; and
- Annex 2 (Security Measures) will be deemed completed with the information set out in Annex B of this DPA.

4.3 With respect to Personal Data subject to UK GDPR, the UK SCCs will apply and:

- the EU SCCs will also apply to transfers of Personal Data; and
- (ii) Table 1 to 3 of the UK SCCs will be deemed completed with the relevant information from the EU SCCs completed as set forth in 2.7.1 and the option “neither party” is checked in Table 4. The start date of the UK SCCs in Table 1 will be the date of this DPA.

4.4 With respect to Personal Data subject to Swiss DPA, the Swiss SCCs will apply and:

- the EU SCCs will apply and any references in the EU SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” will be interpreted as references to the Swiss SCCs;
- references to “EU,” “Union,” “Member State,” and “Member State Law” will be interpreted as references to “Switzerland” and “Swiss law,” as the case may be; and
- references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the FDIPC and competent courts in

Switzerland, unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss SCCs, in which event the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in Annex A and Annex B to this DPA.

4.5 To the extent the University adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Applicable Data Protection Laws) for the transfer of Personal Data (“**Alternative Transfer Mechanism**”), the Alternative Transfer Mechanism will automatically apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Laws applicable to the European Economic Area and extends to territories to which Customer’s Personal Data is transferred).

5. Cooperation and Individuals’ Rights

Taking into account the nature of the processing and the information available, the University shall provide all reasonable and timely assistance to enable Customer to respond to: (i) any request from an individual to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, inquiry, or complaint received from a regulator or public authority, Data Subject, or another third party, in connection with the processing of the Customer’s Data. If any such communication is made directly to the University, the University shall promptly and without undue delay (and in any event, no later than within forty-eight (48) hours of receiving such communication) provide Customer full details of the same and shall not respond to the communication unless specifically required by law or authorised by Customer.

6. Data Protection Impact Assessment

Taking into account the nature of the processing and the information available to the University, the University shall provide Customer with reasonable and timely assistance with any data protection impact assessments and, where necessary, consultations with data protection authorities.

7. Security Incident

Upon becoming aware of a Security Incident affecting Data, the University shall:

- (i) inform Customer without undue delay (and in any event, no later than the earlier of (A) within seventy-two (72) hours after confirming a Security Incident affected Data, and

(B) the notice timescales required of the University by Applicable Data Protection Law); and

(ii) provide sufficient available information and cooperation to enable Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law.

The University shall further take such measures and actions as are necessary to contain, investigate, remedy, and mitigate the Security Incident and shall keep Customer informed of all material developments in connection with the Security Incident. The University shall not notify any third parties of a Security Incident affecting Data unless and to the extent that:

(a) Customer has agreed to such notification, or

(b) notification is required to be made by the University under Applicable Data Protection Laws. Customer is responsible for its secure use of the Services, including, but not limited to, securing its account authentication credentials and protecting the security of Data transmitted via the systems Customer administers and maintains (i.e., email encryption).

8. Deletion or Return of Data

Upon termination or expiry of the Agreement or upon the Customer's request, the University shall (at Customer's election and in accordance with the terms of the Security Measures and the Agreement) delete or return all Data, including copies, in its possession or control. This requirement shall not apply to the extent that the University is required by Applicable Data Protection Laws to retain some or all Data, in which event the University shall isolate and protect Data from any further processing except to the extent required by such law.

Unless otherwise required by Applicable Data Protection Law, the University retains Customer Data only for the duration of the Agreement and for up to ninety (90) days after expiration or termination to enable export by Customer. After this period, the University will securely delete Customer Data in accordance with its data destruction procedures.

9. Audit Rights and Reports

9.1 Solely to the extent required to comply with Applicable Data Protection Law, and to the extent the Reports do not satisfy Applicable Data Protection Law, Customer may audit (including by an independent third-party engaged by Customer) the University's compliance with this DPA. In the case of such audit, the University shall make available all such information, systems, and staff reasonably necessary to allow Customer to conduct such audit. Customer shall not exercise its audit rights more than once per calendar year except following a Security Incident or following an instruction by a

regulator or public authority. Customer shall give the University at least forty-five (45) days prior written notice of its intention to audit pursuant to this DPA, conduct its audit during the University's normal business hours, and take all reasonable measures to prevent unnecessary disruption to the University's operations and to ensure the protection of the data (which may include Personal Data) of the University's employees, contractors, suppliers, or other users or customers. Customer and the University shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to an audit. Customer understands and agrees that its right to audit a Sub-Processor's compliance with this DPA will be subject to the audit provisions in the data processing terms between the University and such Sub-Processor, and that Customer may be required to execute a non-disclosure agreement and other related terms directly with such Sub-Processor to receive access to Sub-Processor's reports and policies.

9.2 Customer shall reimburse the University for all costs and expenses in connection with an audit carried out by Customer under this DPA, except that the University will provide Customer the Reports at no cost. Customer agrees that any of its audit rights set out in the Standard Contractual Clauses and other Applicable Data Protection Law shall be subject to, and carried out in accordance with, the terms of this Section 9.

10. Compliance with Applicable Laws

10.1 The University will process Data in accordance with this DPA and Applicable Data Protection Laws applicable to its role under this DPA. The University is not responsible for complying with Applicable Data Protection Laws uniquely applicable to Customer by virtue of its business or industry. The University will promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Laws.

10.2 With respect to the CCPA, except to the extent Section 2.3.2 applies, the University will: (i) comply with sections of the CCPA applicable to "service providers" as defined by the CCPA; (ii) process Data solely to provide the Services to Customer, consistent with Section 1798.140(e)(5) of the CCPA; and (iii) not sell Data, or retain, use, or disclose Data for any purposes other than to perform the Service or as otherwise permitted under Agreement or this DPA.

10.3 With respect to the VCDPA, the University will: (i) comply with sections of the VCDPA applicable to "processors" as defined by the VCDPA; and (ii) process Data solely to provide the Services to Customer.

10.4 To the extent that Section 2.3.2 applies, the University shall comply with the CCPA sections applicable to a "business" and the VCDPA sections applicable to a Controller.

10.5 The University will process Personal Data in accordance with the University of Sydney Privacy Policy and the Australian Privacy Principles (“APPs”) under the Privacy Act 1988 (Cth), to the extent applicable to the University’s role under this DPA.

10.6 This DPA is intended to align with, and provide protections consistent with, the European Data Protection Law to the extent applicable to the Customer.

11. Indemnification for Third Party Claims

Subject to the terms of the Agreement (e.g., process for tendering indemnity claims) and relevant sections of this DPA, the University will defend and hold harmless Customer against any Third Party Claim brought against Customer arising from the University’s breach of its obligations under this DPA, and indemnify Customer from the resulting costs and damages awarded against Customer to the third party raising such Third Party Claim by a court of competent jurisdiction or agreed to in settlement.

12. Costs Allocation and Liability

12.1 Each party will bear the costs of the investigation, remediation, mitigation, and other related costs to the extent a Security Incident is caused by such party.

12.2 Each party will bear the costs of any fines, penalties, damages, or other related amounts imposed by an authorised regulatory body, governmental agency, or court of competent jurisdiction to the extent arising from such party’s breach of its obligations under this DPA.

12.3 To the maximum extent allowed under Applicable Data Protection Law and other applicable laws or regulations, each party’s liability under this DPA will be limited to actual and proven damages in an amount not to exceed one (1) times the amount paid by Customer to the University under the Agreement for the Services during the 12-month period immediately preceding the incident giving rise to the claim.

13. Miscellaneous Provisions

13.1 The obligations placed upon the University under this DPA shall start when the University or its Sub-Processors process Data on Customer’s behalf in connection with the Services, and will survive for so long that the University or its Sub-Processors process Data on Customer’s behalf. Any claims against the University or its Affiliates under this DPA may only be brought by the Customer entity that is a contracting party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

13.2 Except for the changes made by this DPA, the Agreement continues to govern the provision and use of the Service and remains unchanged and in full force and effect (including, for the avoidance of doubt, the limits on liability provisions in the Agreement). If there is any direct conflict between a provision in this DPA and a

provision in the Agreement, the provision in this DPA shall prevail solely to the extent of that conflict only.

13.3 Other than as required by the Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto, respective permitted successors, and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

13.4 Other than as required by the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Agreement govern any dispute pertaining to this DPA.

ANNEX A: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex A includes certain details of the processing of Personal Data as required by the Standard Contractual Clauses and Article 28(3) GDPR. The parties agree that this Annex forms a part of the Standard Contractual Clauses.

A. List of Parties

Data exporter(s): Customer

Role: Controller or Processor (if processing contracts on behalf of a Customer Affiliate)

Contact Information: As outlined in the Agreement

Data importer(s): the University of Sydney

Role: Processor for purposes of Section 2.3.1 and Controller for purpose of Section 2.3.2

Contact Information: As outlined in the Agreement

B. Description of Transfer

Subject matter and duration of the processing of Data: The subject matter and duration of the processing of Customer's Data are set out in the Cogniti Subscription Agreement, the applicable Order, and this DPA.

The nature and purpose of the processing of Data: The nature and purpose of the processing of Customer's Data are set out in the Cogniti Subscription Agreement, the applicable Order, and this DPA.

The types of Data to be processed: Customer may submit its prompts, course materials, student IDs, and feedback that may include Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

- Identification and contact data (name, email address);
- Purchase and usage history data;

- Contractual obligation data (persons and their business relationship with Customer, such as employee, consultant, the University, customer);
- IT information (IP address, log files, session and usage records recorded for operation, security and service-improvement purposes);
- Prompts, conversation messages and AI-generated responses; educator-authored agent instructions and uploaded course materials.

The categories of Data Subject to whom the Data relates: Customer's students, educators and administrators and other Authorised Users; Customer's staff who administer or support the Services; and other individuals whose Personal Data is contained in Customer Content, the extent of which is determined and controlled by Customer in its sole discretion.

The obligations and rights of Customer: The obligations and rights of Customer are set out in the Cogniti Subscription Agreement, applicable Order Forms, and this DPA.

Data subjects

The personal data transferred concern the following categories of data subjects: Customer's students, educators and administrators and other Authorised Users; Customer's staff who administer or support the Services; and other individuals whose Personal Data is contained in Customer Content, the extent of which is determined and controlled by Customer in its sole discretion.

Categories of data

The personal data transferred concern the following categories of data: Customer may submit its prompts, course materials, student IDs, and feedback that may include Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

- Identification and contact data (name, email address);
- Purchase and usage history data;
- Contractual obligation data (persons and their business relationship with Customer, such as employee, consultant, the University, customer);
- IT information (IP address, log files, session and usage records recorded for operation, security and service-improvement purposes).
- If the parties mutually agree on expanded use case, financial information (account details, payment information).

- Prompts, conversation messages and AI-generated responses; educator-authored agent instructions and uploaded course materials.

Special categories of data (if appropriate)

The personal data transferred concerns the following special categories of data: None.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The personal data transferred to or accessed by the data importer will be used only for the purposes of providing the Services to the data exporter: hosting and operating the Services; generating AI responses to Authorised Users' prompts through the model providers listed in Annex C; storing and retrieving Customer Content; authentication and authorisation; support, maintenance and security monitoring; and export and deletion at the data exporter's instruction. To this end, personal data may be accessed, processed, or disclosed as necessary by the data importer's duly authorised staff or Sub-Processors, strictly for the purpose of providing services to the data exporter and in accordance with the data exporter's instructions.

ANNEX B: SECURITY MEASURES

The University maintains at least the following measures for the Services: encryption in transit (TLS 1.2 or higher) and at rest (AES-256); the application reachable only through Azure Front Door with a Web Application Firewall, with application servers not directly reachable from the internet; databases and configuration stores restricted to the application's network; uploaded files served only through short-lived signed links; authentication through Customer's identity provider (SAML 2.0, OIDC or LTI 1.3) with no local passwords; role-based access within the Services; secrets held in Azure Key Vault and accessed by managed identity; malware scanning of uploaded files; centralised security logging with Microsoft Sentinel detection and alerting; encrypted, geo-redundant backups with tested failover; independent penetration testing at least annually and continuous vulnerability scanning; staff access to production on a least-privilege basis with multi-factor authentication and logging; and documented incident response, business continuity and disaster recovery plans exercised annually. Further detail is provided under NDA. University cyber security policies are available at <https://www.sydney.edu.au/about-us/governance-and-structure/cybersecurity.html> and are the University's Confidential Information.

ANNEX C: SUB-PROCESSORS

The University of Sydney ("the **University**," "we," "our," or "us"), shares this list of third-party suppliers that enable us to provide the Cogniti product and service ("**Cogniti**") for transparency with our users and to comply with our obligations under applicable laws

and to our customers. These third-party suppliers perform the general function and processing activities described below and are considered sub-processors under certain applicable laws (“sub-processors”), including the European Union’s data privacy regulation known as the General Data Protection Regulation (“**GDPR**”), because they process personal data in the course of our delivery of our products and services to customers.

When we use the terms “process,” “processing,” “processed” and “personal data” in our terms with you, those terms have the meaning given to them under GDPR and applicable laws. We require our sub-processors to implement appropriate security measures to safeguard personal data and to comply with relevant obligations. Further information about our sub-processors are available at their respective websites. For your convenience, we have shared links to our sub-processor’s data processing terms.

Back-End Infrastructure and Product

Like many cloud-based solutions, Cogniti uses suppliers that provide back-end infrastructure for our products’ production systems and for data storage. We also engage suppliers to allow us to analyze the performance and usage of our products and enhance certain product capabilities. These tools enable our product and engineering teams to develop new and improved features and create better user experiences. These suppliers possess an extensive set of security certifications with regular auditing to ensure compliance. More importantly, these suppliers allow us to deliver to customers better performing products.

Sub-processor: Microsoft Corporation

Processing location: Australia

Processing Activities / General Function: Azure AI services, Azure container application services, Azure database services, Azure communication services

Data Processing Terms: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

Sub-processor: Optional, determined by Customer: OpenAI, Anthropic, Mistral AI, Google

Processing location: Per the provider's terms

Processing Activities / General Function: Generation of AI responses, only where Customer elects to connect its own account with the provider under Section 2.2 of the Agreement; not used by default.

Data Processing Terms: the provider's applicable data processing terms.

Sub-processor: MongoDB

Processing location: Australia

Processing Activities / General Function: For Cogniti SaaS product: Database storage

Data Processing Terms: <https://www.mongodb.com/legal/data-processing-agreement>

Sub-processor: Google LLC

Processing location: Global

Processing Activities / General Function: Google Analytics is used to collect pseudonymised usage data (e.g. page views, feature engagement, and session activity) to help us improve the user experience. No directly identifiable information (such as names or email addresses) is collected through this service.

Data Processing Terms: <https://business.safety.google/processor/terms/>

Other Providers

To support a remote / hybrid work environment amongst our team, enable collaboration, and allow for data-driven and prompt client and relationship management, we use various cloud-based tools.

Sub-processor: Microsoft Corporation

Processing location: Australia

Processing Activities / General Function: Business productivity (e.g. email, document hosting)

Data Processing Terms: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

Sub-processor: Hubspot

Processing location: Australia

Processing Activities / General Function: Business productivity and customer engagement and support

Data Processing Terms: <https://legal.hubspot.com/dpa>

Change history

5 June 2026

First consolidated version.

30 September 2026

Document	Clause or section	Change	Effect
Order terms	Included support and training	Support response time stated by severity per the SLA (Critical: 4 business hours) instead of "24 business-hour"	One consistent response commitment
Order terms	Account configuration	"Dedicated tenancy" replaced with "dedicated organisation within the Cogniti service, logically separated from other institutions"	Accurate description of the hosting model
Order terms	Overage options	Duplicate throttling paragraph removed; throttling applies only where an allowance is exceeded and no overage arrangement is in place	Clearer throttling conditions
Support and Service Level Schedule	Section 7	"Responsible Use Policy" replaced with the use restrictions in clauses 2.8(b) and 2.9	Suspension grounds fully stated in the agreement
Support and Service Level Schedule	Section 8	Model selections, exclusions or restrictions in the Order are not changed without the customer's written agreement	Customer's model restrictions are protected
Subscription Agreement	1.3(c)	"Service Description" removed from the list of schedules	Removes a reference to a non-existent document
Subscription Agreement	2.3	SLA described as "included in these terms" rather than "referenced in Appendix A of the Order"	Confirms the SLA forms part of the package
Subscription Agreement	2.5	Typographical fix	None

Subscription Agreement	3.3(iii)	Cost optimisations, including model switching, are subject to any model restrictions in the Order; grammar corrected	Excluded models cannot be substituted during a cost adjustment
Subscription Agreement	4.5	Security incident notice changed from "approximately twenty-four (24) hours" to "no later than seventy-two (72) hours after confirming a Security Incident", matching DPA section 7	Single notification figure; the DPA already governed
Subscription Agreement	5.4	Export window extended from 30 to 90 days; deletion from the production service within a further 30 days; backup copies expire under the backup retention schedule and are not restored except for disaster recovery	Longer export window; defined deletion timing; backup handling stated
Privacy Policy	How your information is disclosed	Microsoft Azure and MongoDB Atlas named; pointer to DPA Annex C	Hosting providers identified
Privacy Policy	Security	Sentence added describing the protections applied	Protections stated
Privacy Policy	Data breaches (new)	Commitment to notify the affected institution and, where required, the OAIC or other regulators	Breach notification stated
Privacy Policy	Overseas disclosure (new)	Where each sub-processor processes data, and the safeguards applied	Australian Privacy Principle 1.4 requirement met
Privacy Policy	Complaints (new)	How to complain, response timeframes, escalation to the OAIC or an EU, UK or Swiss authority	Complaints route for all users
Cookies	Essential and analytics cookies	Names and lifetimes of essential cookies; analytics cookies set only after consent	Cookies identified; analytics is opt-in
Cookies	Definitions	"Website Terms of Use" corrected to "Terms of Service"	None

Data Processing Addendum	Section 4	Transfers limited to the countries in which the Annex C sub-processors process data	Narrower transfer scope
Data Processing Addendum	Section 10.5 (new)	Personal Data processed in accordance with the University's Privacy Policy and the Australian Privacy Principles under the Privacy Act 1988 (Cth)	Express Australian privacy law commitment
Data Processing Addendum	Annex A	Data types, data subjects and processing operations rewritten to describe Cogniti	Accurate processing record
Data Processing Addendum	Annex B	Link to University policy pages replaced with a list of security measures maintained for the service	Measures stated in the contract
Data Processing Addendum	Annex C	Zoho removed (no longer used; data deleted); optional AI model providers listed as engaged only where the customer connects its own account	One fewer sub-processor; AI providers disclosed

2 October 2026

Document	Clause or section	Change	Effect
Data Processing Addendum	Annex B	Clarify what is reachable through the internet	More accurate representation