DATA PROCESSING AGREEMENT

HOW TO EXECUTE THIS AGREEMENT

This data processing agreement (**DPA** or **Agreement**) has been pre-signed by Moodle. If Moodle receives the completed and signed DPA, it will become a legally binding addendum to the Master Agreement (defined below) between the parties. To incorporate this DPA into the Master Agreement, You as Data Controller may:

- complete the information in the signature block of this DPA and have an authorised representative sign and return it to Moodle at privacy@moodle.com; or
- agree to this DPA via checking the respective box that permits you to enter into the Master Agreement with Moodle and demonstrating your acceptance to these terms by performance of the Master Agreement.

SCOPE OF THIS AGREEMENT

This data processing agreement (**DPA** or **Agreement**) forms part of the terms of use, service terms or other master agreement between You as Data Controller and Moodle Pty Ltd / Moodle US LLC as Data Processor (**Master Agreement**). In such a case any reference to Master Agreement in this DPA shall be construed as reference to the existing contractual arrangement(s) that applies between the Parties pursuant to which the Processor has agreed to process Personal Data on behalf of You. In the absence of an executed master service agreement this DPA shall act as a standalone data processing agreement.

This Agreement may be updated from time to time, with any such amended Agreement being dated and available on our website with our Privacy Notice at https://moodle.com/privacy-notice/. We endeavour to communicate amended Agreements to You via Your notification email provided. It is Your obligation to ensure that You have downloaded and signed the most up to date Agreement for your records.

BETWEEN:

(1) You or Your organisation, as a Data Controller under the GDPR, that has engaged with Moodle Pty Ltd or one of its affiliates to provide products or services (hereinafter referred to as the **Controller**); and

(2) Moodle Pty Ltd being a company registered under the laws of Western Australia with Australian Company Number 116 513 636 and/or Moodle US LLC of 8101 College Blvd, Suite 100 PMB1007, Overland Park, KS 66210 as appropriate (hereinafter referred to as **Processor**);

individually referred to as a **Party** and together as **Parties**.

WHEREAS:

A. You Process the Personal Data as Controller;

B. You have appointed Moodle Pty Ltd and/or Moodle US LCC as Processor to provide services as referred to in the Master Agreement or other terms of use, whereby Processor will Process the Personal Data on behalf of You, the Controller;

C. The Parties have reached an agreement on the rights and obligations of Controller and Processor and now wish to record such rights and obligations in this DPA.

NOW THEREFORE THE PARTIES AGREE AS FOLLOWS:

1. Definitions & Interpretation

1.1 In this DPA, unless otherwise defined, all capitalised words and expressions shall have the following meaning:

(a) **Data Protection Law** means data protection legislation or any statutory equivalent in force applicable to the Processing of Your Personal Data, including the GDPR, the UK GDPR and Data Protection Act(s) and the Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) ("**CCPA**").

(b) **EEA** means the European Economic Area.

(c) **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The terms **Controller, Processor, Data Subject, Personal Data, Processing, Supervisory Authority** shall have the meanings given to them in the GDPR.

(d) **Personal Data Breach** means a Security Incident that has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Your Personal Data transmitted, stored or otherwise processed by the Processor.

(e) **SCCs** means the Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in non-adequate countries, as defined under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU) and as updated on the 4th June 2021 by Decision 2021/914, a link of which is provided in Schedule 3.

(f) **Security Incident** means any breach of security measures used by Processor to secure Your Personal Data.

(g) **Subprocessor** means a person or entity subcontracted by Data Processor to Process Your Personal Data.

(h) **Your Personal Data** means any Personal Data Processed by Processor on behalf of You pursuant to or in connection with any Master Agreement and/or this DPA.

1.2 Interpretation

(a) To the extent of any conflict or inconsistencies between the Master Agreement and this DPA, this DPA shall take precedence, unless otherwise specified herein.

(b) Unless the context indicates a contrary intention another grammatical form of a defined word or expression has a corresponding meaning.

2. Processing Your Personal Data

2.1 For the purpose of this DPA, Moodle Pty Ltd is the Processor of Your Personal Data and You are the Controller.

2.2 Schedule 1 contains details of the processing activities You have engaged Processor to perform including the categories of Data Subjects, the types of Personal Data and the purpose and nature of the Processing.

2.3 The Processor will (and will procure that Subprocessors will):

(a) have no independent rights in relation to Your Personal Data and only Process Your Personal Data on behalf of and for, Your benefit, in accordance with the terms of the Master Agreement and this DPA together with Your instructions, unless required to do so by applicable law to which the Processor is subject, in which case the Processor shall inform You of that legal requirement before the Processing of Your Personal Data;

(b) not assume any responsibility for determining the purposes for which and the manner in which Your Personal Data is Processed and will only Process Your Personal Data for purposes determined by You; and

(c) notify You promptly in the event that it is unable to comply with this DPA or its obligations under any Data Protection Law or if it has reason to believe that the legislation applicable to it is likely to have a substantial adverse effect on the obligations provided under this DPA or otherwise prevents it from fulfilling any instructions received from You. If this provision is invoked, Processor will not be liable to You for any failure to perform the applicable services until such time as You issue new instructions regarding the Processing with which the Processor is able to comply.

2.4 For clarity, within the scope of the Master Agreement and this DPA and in relation to Your use of the services: (i) You shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Your Personal Data to Processor; (ii) You agree that Your instructions for the Processing of Personal Data shall comply with Data Protection Law; and (iii) You agree to inform Processor without undue delay about any errors or irregularities related to the Processor's Processing of Your Personal Data

3. Rights and obligations of Processor

3.1 The Processor will:

(a) take reasonable and appropriate technical and organisational measures that are designed to adequately protect the security, integrity and confidentiality of Your Personal Data and guard against unauthorised or unlawful disclosure, access or Processing, or accidental loss, alteration,

damage or destruction as described in Schedule 2. Such measures shall include (as appropriate) the measures required pursuant to Article 32 of the GDPR;

(b) only grant access to Your Personal Data to persons under the Processor's authority who have committed themselves to confidentiality or who are under an appropriate statutory obligation of confidentiality. The classes of persons to whom access has been granted shall be subject to periodic review. Specifically, Subprocessors referred to in Schedule 1 are deemed approved by You;

(c) assist You by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of Your obligations to respond to requests by a Data Subject in relation to the exercise of their rights pursuant to Data Protection Law (including access, rectification, restriction, deletion or portability of Personal Data, as applicable) and will (i) inform You as soon as possible, and in any event, no later than one month, after receipt of a request from a Data Subject in respect of the Personal Data and (ii) unless otherwise instructed by You, advise the Data Subject to submit their request to You. Such assistance will be provided subject to agreement to any reasonable and duly evidenced cost being charged by the Processor for these services;

(d) maintain electronic records of complaints or requests from Data Subjects seeking to exercise their rights under Data Protection Law until such time as the records have been securely transferred to You. The Processor shall not respond and shall ensure that Subprocessors do not respond directly to requests from Data Subjects except upon Your written instructions or as required by Data Protection Law;

(e) assist You in data protection impact assessments (subject to agreement to any reasonable and duly evidenced cost being charged by the Processor for this assistance);

(f) assist You, at Your cost, in the event of an investigation or audit by a Supervisory Authority, to the extent that such investigation or audit relates to Processor's Processing of Your Personal Data and inform You as soon as possible if a Supervisory Authority requests an investigation or audit of Processor relating to Processor's Processing of Your Personal Data; and

(g) maintain records of all Processing operations under its responsibility that contain at least the minimum information required by Data Protection Law.

4. Security Incidents

4.1 The Processor will (and shall procure that all its Subprocessors will) maintain updated electronic records of all discovered Security Incidents in a register. The register shall contain at least a description of the Security Incident, including the date and time the Security Incident was discovered. If a Security Incident is a Personal Data Breach the register shall also contain an overview of the affected Personal Data and the categories and number of affected Data Subjects.

4.2 The Processor will (and shall procure that all its Subprocessors will) promptly, but in any event within 48 (forty-eight) hours of becoming aware of an actual or suspected Personal Data Breach, inform You in writing of such Personal Data Breach. The Processor will take prompt steps to remedy any Personal Data Breach and promptly provide You with all relevant information and assistance regarding any such actual or suspected Personal Data Breach. The Processor's notification of a Personal Data Breach to You will include information sufficient to allow You to meet Your obligations pursuant to Data Protection Law, and at a minimum:

(a) a description of the Personal Data Breach, including the date and time the Personal Data Breach was discovered;
(b) an overview of the affected Personal Data and the categories and number of affected Data Subjects;
(c) information on the (expected) consequences of the Personal Data Breach; and
(d) a description of the measures taken by the Processor to limit the consequences of the Personal Data Breach.

If the Processor is unable to communicate all required information relating to the Personal Data Breach simultaneously, the Processor shall provide the information as the information becomes available.

The Processor will not provide any statement, communication, press release or other public announcement relating to a Personal Data Breach without Your prior written consent unless otherwise required by law.

5. Subprocessors

5.1 You, as the Controller, grant the Processor general written authorisation for the engagement of Subprocessors and any intended changes concerning the addition or replacement of Subprocessors, subject to the proviso that the Processor shall remain fully liable to You for fulfilment of the obligations of the Subprocessor and that the Processor and the Subprocessor have entered into an agreement that imposes obligations on the Subprocessor that are no less restrictive than those imposed on the Processor under this DPA, and provides for sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of Data Protection Law and this DPA.

5.2 The Subprocessors referred to in Schedule 1 are hereby approved by You. If the Processor intends to instruct a Subprocessor other than the companies listed in Schedule 1, the Processor may notify You thereof in writing (either via email to the email address(es) on record in Processor's account information or via public notice on the Processor's website). Unless You otherwise object You will be deemed to have accepted any and all additions or amendments to Schedule 1 as may be made from time to time. You may terminate the Master Agreement if you object to such additions or amendments to Schedule 1 in accordance with the Master Agreement.

6. Audit Rights

6.1 Upon Your written request, and provided that the Parties have a confidentiality agreement in place, the Processor will provide You with the results of the most recent data security compliance reports (if any) or any audit performed by or on behalf of the Processor that assesses the effectiveness of the Processor's information security program, system(s), internal controls, and procedures relating to the Processing of Your Personal Data.

6.2 Upon reasonable advance written notice to the Processor, You may during normal business hours, attend on the Processor's facilities for the purpose of auditing the Processing and maintenance of Your Personal Data, and the Processor's compliance with its obligations under this DPA. You will be responsible for the costs and expenses of such audit (or the fees and costs of the third party performing the audit). If the Processor declines to address and correct all deficiencies identified in any such audit, You are entitled to terminate the Master Agreement and this DPA in accordance with its terms.

7. Data transfers

7.1 The Processor will comply with Data Protection Law regarding the transfer of Your Personal Data from the EEA to countries outside the EEA. Unless otherwise provided for in Schedule 1, the Processor will not transfer or process Your Personal Data outside of the territory of the EEA or outside the territories defined in Schedule 1 otherwise than set out in this Agreement. The Processor shall ensure that any such transfer/access is implemented in accordance with this Agreement.

7.2 To the extent that the Processor is based in a third country that does not provide an adequate level of protection, and the transfer of Your Personal Data is not covered by one or more safeguards provided for in Articles 45, 46 and 47 of the GDPR the Parties hereby agree to enter into the SCCs, as provided for in Schedule 3.

7.3 If the Processor intends to transfer Personal Data to an engaged Subprocessor located outside of the EEA and the Processor opts to have such transfer covered by the SCCs, the Processor is hereby authorised to enter into such SCCs in Your name and on Your behalf.

7.4 At Your request, and provided that the Parties have a confidentiality agreement in place, the Processor shall provide a copy of any document evidencing the implementation of any of the above-mentioned measures to cover the transfer/access of Your Personal Data.

8. Termination and erasure and return of data

8.1 On termination of the Master Agreement, or earlier as requested by You, the Processor will destroy, or upon Your written instructions, deliver to You, or enable You to delete by means of the functionality provided by the services, all Your Personal Data in the Processor's possession, custody and control, except for such information as must be retained under applicable law and insofar as is technically possible.

8.2 To the extent that the Processor retains any of Your Personal Data beyond termination or expiration of the Master Agreement or as earlier requested by You because such retention is required under applicable law, this DPA will remain in full effect and the Processor will promptly destroy all such Personal Data once such retention is no longer required under applicable laws insofar as is technically possible. At Your request, the Processor will provide You with written confirmation of such destruction.

8.3 This DPA will expire automatically upon Your Personal Data either being fully returned or destroyed except in so far as required for statutory or contractual purposes.

9. Liability

9.1 Notwithstanding provisions of the Master Agreement limiting Processor's liability (if any), the Processor will be liable only for any direct damages arising out of or in connection with the Processor's breach of (i) this DPA; (ii) Data Protection Law; or (iii) Your instructions under this DPA.

9.2 The Processor's aggregate liability pursuant to this DPA shall not exceed an amount equal to the total amount of the subscription fees or royalties fees paid or payable by You under the Master Agreement during the immediately preceding twelve (12) month period.

10. Jurisdiction and venue

10.1 This DPA and any dispute or claim arising out of it or in connection with it, its subject matter or formation shall be governed by and construed in accordance with the laws of Ireland and the Parties irrevocably submit to the non-exclusive jurisdiction of the Courts of Ireland.

Notwithstanding the foregoing, the Processor may, in its sole discretion, elect to nominate any proceedings in a mutually convenient alternative forum or jurisdiction, including any appropriate State of the USA.

Signed on behalf of You (the Data Controller)	**Agreed and accepted by Moodle Pty Ltd or Moodle US LCC as appropriate (the Data Processor)**
By Your Authorised Representative: _____ Full Name / Title: _____ Date: _____	By Moodle's Authorised Representative: Chris Brown _____ Full Name / Title: Chris Brown / Legal Counsel & Privacy Officer Date: 30 June 2022

Schedule 1

Details of processing activities

This Schedule 1 includes certain details of the Processing of Your Personal Data, as required by Article 28(3) of the GDPR.

For Moodle Certified Service Providers (Partners & Resellers)	**Description of all Personal Data accepted from the Data Controller:** Certified Service Providers ("Partners") are obligated to provide certain Customer Data (as defined under the Agreement) that relates to the Partner's certification and obligations under the Agreement, including but not limited to the following information: ● the names, addresses, and websites of all of the Partner's customers; ● an itemised list of all invoices sent to Customers (whether subsequently paid and unpaid), including invoice number, amounts and itemised details with the value of each Moodle Service type clearly identified and the Moodle flavour of Moodle Software; ● contracts, bid documents and electronic communications relating to all work done for all Customers; and ● any and all documents and correspondence evidencing the software and services provided to all of the Partner's customers and an itemised list of all revenue received by the Partner from: ○ Moodle Services; and ○ any services which are not considered Moodle Services. **Description of Processing activities:** Moodle maintains a securely restricted portal https://partners.moodle.com/login/index.php that is accessible only by Partners for the purpose (among other things) of meeting compliance with the obligation to pay Certification Fees in accordance with the Partnership Agreement. Moodle uses that portal to verify such compliance.

Schedule 2

Security Measures

1. The Data Processor will ensure that in determining the appropriate security measures for all Personal Data processed on Your behalf the following matters are taken into consideration:

   A. the nature of the Personal Data;
   B. the nature, scope, context and purposes of the Processing activity; and
   C. the harm that might result from unlawful or unauthorised Processing or accidental loss, damage or destruction of the Personal Data.

2. In assessing the appropriate level of security, the Data Processor shall:

   A. undertake a risk assessment of all new data Processing activities to allocate responsibility for implementing a relevant policy to specific individuals or team members;

   B. ensure appropriate security safeguards and virus protection are in place to protect hardware and software used in Processing Personal Data in accordance with best industry practice;

   C. ensure storage of Personal Data is maintained at secure and (where applicable) local locations to avoid unnecessary cross border data transfers in conformity with best industry practice and access by personnel to such Personal Data is password restricted and monitored;

   D. have secure methods in place for the transfer of Personal Data whether in physical form (for instance, by using couriers rather than standard post) or electronic form (for instance, by using encryption);

   E. take reasonable steps to ensure the reliability of all employees or other individuals who have access to Your Personal Data and to ensure such employees and individuals are informed of the confidential nature of the Personal Data and their compliance obligations in this Agreement; and

   F. have strong and concise systems and processes implemented for detecting and dealing with security breaches.

3. Specific actions undertaken by the Data Processor that will be expected of subprocessors include:

   A. When in transit, Personal Data is always encrypted by Transport Layer Security (TLS) Protocols and web secure (HTTPS) communications.

   B. Data in the Data Processor's possession is backed up daily and backups are checked regularly.

   C. All access to systems and services have password protection and multi-factor authentication (2FA) devices where available.

   D. Only authorised users can access storage and databases where Personal Data is stored.

   E. All logs (normal traffic, application and event logs) are copied to a centralised repository with a standard retention time of 6 months.

F. Configuration changes and default configuration are stored in a repository with change control mechanisms implemented. Changes are applied using a configuration manager tool to ensure audit trails to be maintained and configurations backed up.

G. Access to servers is restricted to IT personnel only. Users who ask for access need to use RSA authentication using SSH protocols with a private key.

H. Shared accounts are reduced to a minimum and users granted access on a minimalist and restrictive basis. All such accounts are logged and tracked.

I. No access information is shared between teams and/or locations across the Data Processor.

J. Systems in the Data Processor's main hosting subprocessor, Amazon Web Services (AWS), have automated, scheduled tasks configured to ensure all backups are cleansed and deleted after clearly defined deadlines (usually 6 months, maximum a year).

K. Critical systems have audit logs enabled: Google Workspace, Tracker, AWS ELB. All admin changes and user actions are audited. Internal accessed servers register all accesses and privileged commands.

Schedule 3 - Cross Border Data Transfers

Where Personal Data is required to be transferred to a location outside the EEA the Standard Contract Clauses (SCCs) as outlined on the Processor's website at https://moodle.com/privacy-notice/ as:

SCCs for Data Exporter; and/or

SCCs for Data Importer

are hereby incorporated and shall apply by reference thereto.

Where Personal Data is not transferred outside the EEA (or other safeguards have been implemented for the specific transfer in question) this Schedule 3 shall not apply.