A. 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 / Moodle India Information Solutions Pvt Ltd 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 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 Trust Centre at: https://trust.moodle.com/ 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.

THIS DPA IS **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 and/or Moodle India Information Solutions Pvt Ltd of 1-3-183/40/90, Ranga Residency, SBI Colony, Gandhi Nagar, Hyderabad, India – 500080 as appropriate (hereinafter referred to as **Processor**);

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

WHEREAS:

B. You Process the Personal Data as Controller;

C. You have appointed Moodle Pty Ltd and/or Moodle US LLC and/or Moodle India Information Solutions Pvt Ltd 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;

D. 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) **Affiliate** means an entity that controls, or is controlled by, or is under common control with a party.

(b) **Controller Affiliate** means any entity which directly or indirectly controls, is controlled by, or is under common control with the You, where “control” means ownership of more than 50% of the voting rights or the ability to direct the management of that entity.

(c) **Data Protection Law** means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) US state privacy laws including the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (iii) the Swiss Federal Act on Data Protection, and (iv) the UK Data Protection Act 2018, in each case as updated, amended or replaced from time to time. **EEA** means the European Economic Area.

(d) **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.

(e) **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.

(f) **Restricted Transfers** means a transfer of Personal Data that is subject to restrictions under Data Protection Law, including any transfer of Personal Data from the EEA, UK or Switzerland to a country or territory that has not been deemed to provide an adequate level of protection under applicable Data Protection Law.

(g) **SCCs** means, as applicable, (i) the Standard Contractual Clauses approved by the European Commission under Commission Implementing Decisions (EU) 2021/914 of 4 June 2021, and/or (ii) the UK International Data Transfer Addendum or equivalent approved mechanism under UK Data Protection Law, in each case as amended, replaced or superseded from time to time.

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

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

(j) **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 and/or Moodle US LLC and/or Moodle India Information Solutions Pvt Ltd is the Processor of Your Personal Data and You are the Controller.

2.2 The Processor shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Schedule 1, (ii) in a manner inconsistent with this DPA or any other documented instructions provided by You, or (iii) in violation of Data Protection Laws. You hereby instruct the Processor to process Personal Data in accordance with the foregoing and as part of any processing initiated by You in Your use of the Services. If Data Protection Laws require the Processor to process Personal Data in a manner that conflicts with the instructions provided by You, the Processor will inform You of that legal requirement before processing, unless prohibited from doing so by applicable law. Schedule 1 contains details of the processing activities You have engaged the Processor to perform including the categories of Data Subjects, the types of PersonalData and the purpose and nature of the Processing.

2.3 The Processor shall not sell, share, train artificial intelligence models on, mine, or otherwise use Your Personal Data for the purposes of targeted advertising, profiling, data monetisation or for any purpose other than the performance of the Services as expressly documented by You.

2.4 The Processor shall not make any solely automated decisions including profiling, that produces legal or similarly significant effects concerning Data Subjects.

2.5 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, this DPA and Your documented instructions, unless required to do so by applicable law to which the Processor is subject, in which case the Processor shall (to the extent permitted by law) inform You of that legal requirement before carrying out such Processing;

(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 without undue delay if it is unable to comply with this DPA, any applicable Data Protection Law, or Your instructions, or if it becomes aware that legislation applicable to it is likely to have a a substantial adverse effect on its ability to comply with this DPA or otherwise prevents it from fulfilling Your instructions. Where 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 all applicable Data Protection Laws, particularly in relation to the disclosure and transfer of your Personal Data to Processor ; (ii) You warrant that Your instructions for the Processing of Personal Data will at all times comply with Data Protection Law; and (iii) You shall promptly inform the Processor without undue delay, of 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 acknowledge that the process may (i) engage its Affiliates as Subprocessors and (ii) may engage third parties as Subprocessors. By way of this DPA, You, as the Controller, grant the Processor general written authorisation for the engagement of Subprocessors, including its Affiliates, for the Processing of Personal Data under this DPA. This includes intended changes concerning the addition or replacement of Subprocessors, subject to the following conditions:

(a) the Processor shall remain fully liable to You for fulfilment of the obligations of the Subprocessor; and
(b) the Processor shall ensure that it has entered into a written agreement with each Subprocessor that imposes obligations on the Subprocessor comparable to those imposed on the Processor under this DPA, including 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.

(b)

5.2 A list of the Processor's Subprocessors is available here/Schedule 1.. You hereby authorise the Subprocessors on this list. The Processor may engage new Subprocessors from time to time. If the Processor intends to instruct a Subprocessor, 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 the list of Subprocessors as may be made from time to time. You may object to such an engagement by informing the Processor in writing within ten (10) days of receipt of the aforementioned notice by the Processor, provided such objection is based on reasonable grounds relating to data protection. You acknowledge that certain Subprocessors are essential to providing the Services and that objecting to the use of a Subprocessor may prevent the Processor from offering You some of all of the Services. If You object to an engagement, and the Processor cannot provide a commercially reasonable alternative within a reasonable period of time, You may discontinue the use of the affected Service by providing written notice to the Processor. Discontinuation shall not relieve Customer of any fees owed to Vanta under the Agreement.

5.3 Where the parties have entered into Standard Contractual Clauses as described in Clause XXX, (i) the above authorisations will constitute Your prior written consent to the subcontracting by the Processor of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Subprocessors that must be provided to You pursuant to Clause 9(c) of the EU SSC's may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Processor beforehand, and that such copies will be provided by the Processor only on Your reasonable request.

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. The Processor shall also make available, upon reasonable request and at reasonable intervals, certifications or attestations of compliance with recognised data protection or security standards, where available.

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. Such audits shall occur no more than once in any 12-month period unless otherwise required by Data Protection Law or by a competent supervisory authority and shall be restricted to data relevant to You. You will be responsible for the costs and expenses of such audit (or the fees and costs of the third party performing the audit) and a reimbursement for any time expended by the Processor, to the extent legally permitted. 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.

6.3 In the event You conduct an audit through a third party independent authority or a third party accompanies You or participates in such audit, such third party shall be required to enter into a confidentiality agreement to protect the Processors confidential information. For the avoidance of doubt, regulators shall not be required to enter into a confidentiality agreement.

7. Data Transfers

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

7.2 The Processor shall, upon reasonable request, provide commercially reasonable assistance to You in completing any transfer impact assessments required under applicable Data Protection Law, including to assess the laws of the destination country and, where required, implement appropriate supplementary measures in good faith.

7.3 To the extent that any such transfer involves a country that has not been deemed to provide an adequate level of protection by the European Commission, UK Government or Swiss Federal Data Protection and Information Commissioner (as applicable), and where no other legal derogation or safeguard applies under Articles 45, 46 and 47 of the GDPR (or their UK/Swiss equivalents) the Parties hereby agree to enter into the SCCs, as provided for in Schedule 3. The SCCs are hereby deemed incorporated into and form part of this DPA.

7.4 Where the Processor engages a iSubprocessor located outside of the EEA, UK or Switzerland, and such transfer is not otherwise subject to an adequacy decision or appropriate safeguard, the Processor is hereby authorised to enter into SCCs (and where applicable, the UK and Swiss Addendum) with such Subprocessor in Your name and on Your behalf.

7.5 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.

7.6 If the SCCs or any other transfer mechanism used pursuant to this DPA is amended, invalidated, replaced or otherwise requires updates in light of guidance or requirements from a competent supervisory authority, the Parties agree to cooperate in good faith to update this DPA accordingly and implement an alternative transfer mechanism that ensures compliance with applicable Data Protection Law.

7.7 The Processor shall implement appropriate technical, contractual or organisational supplementary measures where required under guidance from any competent data protection authority to ensure the level of protection essentially equivalent to that guaranteed by GDPR.

8. Termination, 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.

11. Miscellaneous

11.1 Interpretation Authority: In the event of any conflict between Data Protection Laws, the GDPR and UK GDPR shall prevail to the extent they provide a higher level of protection to Personal Data.

11.2 Conflicts: In the event You believe that You cannot satisfy Your other obligations under the Agreement while complying fully with this DPA, You must notify the Processor immediately and shall not proceed with any act that would violate this DPA until the issue is resolved to the Processor's reasonable satisfaction.

11.3 Survival: The obligations of the Processor under this DPA which, by their nature, are intended to survive expiry or termination of the Master Agreement, including without limitation the obligations relating to confidentiality, data protection, audit rights, data return or deletion, and

liability shall survive such expiry or termination for so long as the Processor continues to process Personal Data, or for the duration required under applicable Data Protection Laws.

11.4 Authority to Execute: The Parties represent and warrant to each other that each has the legal power and authority to enter into this DPA.

11.5 Entire Agreement: This DPA is made of part of but does not supersede the Master Agreement between the Parties, except with respect to the subject matter of this DPA.

11.6 Precedence: In the event of any conflict between the provisions of the Master Agreement and the provisions of this DPA, to the extent the conflict involves a provision of the Standard Contractual Clauses, such provision shall take precedence, otherwise the provisions which provide greater protection for Your Personal Data shall take precedence.

11.7 Severability: If any provision of this DPA shall be unlawful, void, or for any reason unenforceable, then that provision or part provision shall be severable from these terms and shall not affect the validity and enforceability of any remaining provisions of this DPA or the Master Agreement.

11.8 Amendment: This DPA cannot be modified, amended or changed except in writing and signed by the Parties.

11.9 Assignment: Neither the rights nor the obligations of either Party may be assigned or delegated in whole or in part without the prior written consent of the other Party unless otherwise expressly permitted under the Master Agreement. Any delegation without written permission shall be null and void and of no effect unless otherwise expressly permitted under the Master Agreement.

11.10 No Third Party Beneficiaries: Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA. Notwithstanding, where the Services include the Processing of Your Personal Data on behalf of any Controller Affiliate, each such Controller Affiliate shall be entitled to enforce the terms of this DPA as a third-party beneficiary solely in respect of its own Personal Data, as if it were a party to this DPA and the Agreement. No Controller Affiliate shall otherwise have any rights under this Addendum. The Controller shall remain solely responsible for all acts and omissions of any Controller Affiliate.

11.11 No Waiver: A waiver by a Party of any term or condition of this DPA in any instance shall not be deemed or construed to be a waiver of such term or condition of the future or any subsequent breach thereof.

11.12 Counterparts: This DPA may be executed in counterparts, each of which shall be deemed as an original, but all of which together shall constitute one and the same instrument.

11.13 Further Assurances: The Processor acknowledges that a Controller Affiliate may, pursuant to applicable Laws, be required to enter into a direct data processing agreement with the Processor. In such circumstances, and only upon the Controller's written request, the Processor shall enter into a separate data processing agreement with the relevant Controller Affiliate solely to the extent required by applicable Laws, and on terms substantially equivalent to this Addendum (subject only to any amendments strictly necessary to comply with applicable Laws) and without creating any additional obligations or liabilities for the Processor. The Processor shall do so within a reasonable period of time following such request.

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, any appropriate State of Australia, or any appropriate State or Union Territory of India.

Signed on behalf of You (the Data Controller)	**Agreed and accepted by Moodle (the Data Processor)**
By Your Authorised Representative: _____	By Moodle's Authorised Representative: _____ Full Name / Title:

Full Name / Title: _____ Date: _____	**Chris Brown / Privacy Officer** Date:

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.
For Airnotifier (Push Notifications) customers while using Moodle mobile apps (Moodle mobile app, Workplace mobile app, Branded Moodle App and Premium app)	**Description of all Personal Data accepted from the Data Controller:** In order to use the Moodle mobile apps (Moodle mobile,Workplace app, Branded Moodle App and Premium app) Your hosting provider (whether that be Yourself, a Moodle Certified Partner, Moodle US, Moodle India or Moodle via MoodleCloud) will have Your Administrator profile details and potentially personal profiles for each of Your students, employees, customers or end users. The only function within Moodle mobile apps that involves Processing by Moodle is the Airnotifier service (Push Notifications). If You determine to utilise the Airnotifier feature the following data will be Processed by Moodle via Amazon Web Services servers in Ireland: Your website URL, Your Administrator's email address,a "Pushid" (the "device token", a unique identifier of the device in Google or Apple system) and the Push notifications content. You warrant that You have received all necessary consents from those end users or third parties as applicable. **Description of Processing activities:** This is explained in the previous section. Moodle uses various third party subprocessors to provide data storage and certain functionality which allows the features of the Moodle mobile apps service to perform. Such subprocessors are outlined in the Register of GDPR Information maintained and updated on Moodle's website at: https://moodle.com/privacy-notice/ and includes: ● Airnotifier, an Open Source application server operating on Amazon Web Services' Irish servers, provides a unified interface to send real-time push notifications to end user devices as determined solely by their administrators upon enable of Mobile notifications at the Moodle site. ● Airnotifier uses Google or Apple notification servers (depending on end users' Android or IOS platform) to deliver push notification to the user device. ● Amazon Web Services as a hosting provider, acting as a subprocessor for all data uploaded to Airnotifier to utilise the push notifications service. ● the wholly owned subsidiary Moodle Spain Technologies S.L., Carrer Arago 264, 7o 2a/3a Barcelona Spain 08007 where employees of that entity are utilised by Moodle Pty Ltd and/or Moodle US LLC and/or Moodle India Information Solutions Pvt Ltd for performing the BMA services. **Data encryption:** ● Moodle LMS and the Moodle app versions 4.2 and onwards support end-to-end encryption for Push Notifications. If enabled, data will be encrypted in origin (Moodle site) and decrypted in destination (Moodle app) by using a key-pair (public key stored in the Moodle site and private key stored in the user device).

For Customers of MoodleCloud™ Services	**Description of all Personal Data accepted from the Data Controller:** In order to use MoodleCloud services You will need to set up an Administrator profile and each of Your students, employees, customers or end users will need to set up a personal profile in order to interact with You and the Moodle-hosted learning platform. As Data Controller, You instruct Moodle, as Data Processor, to Process any and all Personal Data needed to maintain the platform. The Personal Data required may include: First name; Surname; email address; phone number; mobile phone; address; Country; time zone; City/Town; End user profile and picture; webpage; ID number; Institution; Department, opinions and comments in forums and publications. You warrant that You have received all necessary consents from those end users or third parties as applicable. There are support tools in the Moodle platform to assist with managing data privacy matters. **Description of Processing activities:** The MoodleCloud services are intended to allow You to customise the nature of data processed according to Your usage needs. Depending on Your chosen settings, the Processing activities may include the collection, compilation, upload and storage of Personal Data, including content from participation in forum discussions, participation in examinations or assessment procedures and video webinars (including Personal Data of the participants and observers of the webinar). Moodle uses various third party subprocessors to provide data storage and certain functionality which allows the features of the MoodleCloud™ learning platform to perform. Such subprocessors are outlined within the Register of GDPR Information maintained and updated on Moodle's website at: https://moodle.com/privacy-notice/. They include: ● Amazon Web Services as a hosting provider, acting as a subprocessor for Moodle in respect of all data uploaded to the MoodleCloud Service. ● Blindside Networks Inc, a Canadian company which enables the "BigBlueButton" web conferencing service on all Moodle websites. This includes voice, video, audio and chat messages. All the data involved is processed on the Blindside Networks Inc servers and is stored for potentially up to a maximum of 365 days before deletion. A separate DPA is provided by Blindside Networks Inc. at https://blindsidenetworks.com/dpa-moodle-free-tier/ ● Google Analytics is used to measure pageviews on all Moodle websites and solely for statistical purposes on an aggregated basis. This data may include a user's IP address, geographical location and browser information. ● Airnotifier uses Google or Apple notification servers (depending on end users' Android or IOS platform) to deliver push notification to the user device. ● LogsHero Ltd. is an Israeli company providing log aggregation services for monitoring purposes. ● NewRelic Inc. is a United States company in San Francisco providing system performance monitoring. ● Intercom Engage as onboarding experience for new users of MoodleCloud services by providing support and guidance on how to use MoodleCloud effectively.
For Moodle Services provided by Moodle US LLC or Moodle India Information Solutions Pvt Ltd	**Description of all Personal Data accepted from the Data Controller:** Moodle US or Moodle India maintains databases to provide ongoing Moodle Services such as hosting to its customers (Customers) and in the process collects and stores a range of information, including but not limited to the following information: ● the names, addresses, and websites of Customers and potential 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 identified; ● contracts, bid documents and electronic communications relating to all work proposed or done for all Customers; and ● any and all documents and correspondence evidencing the software and services provided to Customers. **Description of Processing activities:** Moodle US or Moodle India provides processing services to its Data Controllers in response to their instructions and requests as provided for by the Moodle platform. Processing activities may include the collection, compilation, upload and storage of Personal Data, including content from participation in forum discussions, participation in examinations or assessment procedures and video webinars (including Personal Data of the participants and observers of webinars). It provides aggregated financial records to its parent company Moodle Pty Ltd to ensure accurate and timely regulatory reporting but any personal information transferred is only upon specific audit request and under confidentiality obligations.

	Moodle US or Moodle India uses various third party subprocessors to provide data storage and certain functionality which allows the features of the Moodle LMS or Moodle Workplace platforms to perform. Such subprocessors are outlined within the Register of GDPR Information maintained and updated on Moodle's website at: https://moodle.com/privacy-notice/. They include: ● Amazon Web Services as a hosting provider, acting as a subprocessor for Moodle in respect of all data uploaded to the Moodle LMS or Moodle Workplace platforms. ● Blindside Networks Inc, a Canadian company which enables the "BigBlueButton" web conferencing service on all Moodle websites. This includes voice, video, audio and chat messages. All the data involved is processed on the Blindside Networks Inc servers and is stored for potentially up to a maximum of 365 days before deletion. A separate DPA is provided by Blindside Networks Inc. at https://blindsidenetworks.com/dpa-moodle-free-tier/ ● Google Analytics is used to measure pageviews on all Moodle websites and solely for statistical purposes on an aggregated basis. This data may include a user's IP address, geographical location and browser information. ● Airnotifier uses Google or Apple notification servers (depending on end users' Android or IOS platform) to deliver push notification to the user device.
For Moodle Community Sites (Moodle Academy™, MoodleNet™ & Moodle.org)	**Description of all Personal Data accepted from the Data Controller:** These community platforms allow you to create a user name and password (with minimum profile details required) so that you may interact with Moodle, Moodle Certified Service Providers and other users. A range of unrequired profile details may also be provided at the user's own discretion. Any information you post on public chat forums is only stored as reasonably required on the legal basis of informed consent or as necessary for the delivery of the applicable service. There is no other data Processing undertaken nor use of third party subprocessors. **Description of Processing activities:** Moodle does not store or process any data (other than as stated above). There is no other data Processing undertaken nor use of third party subprocessors.
Moodle Corporate Activities outlined in the Register of GDPR Information	Other corporate activities that are detailed in Moodle's Register of GDPR Information (where Moodle is the Controller, rather than the Processor) include the following (and in some instances, a link to their terms): ● Atlassian Pty Ltd and Atlassian, Inc. (for Jira, Confluence, Opsgenie) in which are utilised for internal knowledge base, project management, Change Advisory Board, internal notifications. ● Calendly LLC for calendar scheduling tool to assist sales and customer success operations. ● Freshworks Inc. for customer support to assist sales and customer success operations. ● Other corporate activities that are detailed in Moodle's Register of GDPR Information (where Moodle is the Controller, rather than the Processor) include the following Mailchimp/Mandrill,Intercom, Freshdesk, Google Workspace, Matrix, SalesForce, Site24x7,Slack, Stripe, Teamwork, Telegram, Toggl, HubSpot Xero, Zoom, Chargebee and BraintreeGateway. Such Processors are subject to change from time to time and do not require formal approval from You. We endeavour to reflect identical protection of data obligations in accordance with the terms of this Agreement with all Processors engaged by Moodle.

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.