GDPR Questionnaire	
Request for clarifications	**Supplier Remarks/Answer**
What is the GDPR?	The General Data Protection Regulation (GDPR) is a regulation in Europen Union law on data protection and privacy in the European Union and the European Economic Area. The full text of the GDPR can be found here.
Is Moodle subject to the requirement of appointing a DPO (Data Protection Officer) under GDPR art. 37?	Yes. We have appointed an independent Data Protection Officer who has been monitoring and auditing Moodle's data protection practices for a number of years. The details of our external independent DPO is: Data Compliance Europe Ltd. 12 City Gate Lower Bridge Street Dublin 8, Ireland Email: moodle@datacomplianceeurope.eu
Provide a general description of the information security measures that Moodle offers.	Moodle undertakes a range of security measures to protect the data of its customers. As outlined in Moodle's standard DPA (available in its Privacy Notice on its website), where Moodle is the Data Processor, the following matters are taken into consideration: (1) the nature of the Personal Data; (2) the nature, scope, context and purposes of the Processing activity; and (3) the harm that might result from unlawful or unauthorised Processing or accidental loss, damage or destruction of the Personal Data. Specific actions undertaken by Moodle that will also 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.

GDPR Questionnaire	
Request for clarifications	**Supplier Remarks/Answer**
Describe how the principles of Data Protection by design and default, as described in Art 25 of GDPR have been or may be implemented in the services that Moodle offer.	We undertake Data Protection Impact Assessments (DPIAs) with each new process, product or service offering by MoodleHQ. Using DPIAs we consider how user data is captured, stored and can be retrieved or removed as required to comply with the law. To help organisations ensure that their privacy compliance also extends to installed plugins external to Moodle LMS, we've created a Privacy API that plugin developers can implement to ensure their add-ons are GDPR compliant. See: https://docs.moodle.org/400/en/Privacy Our leading privacy features ensure that your Moodle LMS is GDPR compliant and adheres to local privacy legislation requirements. At https://docs.moodle.org/400/en/Policies we provide functionality so that you may write multiple policy documents (including site policy for guests) ensuring that you can be completely transparent with your learners, educators and anyone who visits your site on how you collect, use or disclose their data. We provide protection functionality for digital minors with age-of-consent checks and ability to manage access for minors who require parental agreement to access your learning management system. We provide you with the ability to handle all data requests from your users and keep track of retention periods in a centralised place. We enable your users to easily request to access or download their data, to see the policies they've agreed to and to contact your Data Protection Officer. See https://docs.moodle.org/400/en/Privacy for more information. At Moodle we do not collect, use or monetise any student data or anyone's personal information from any of the thousands of Moodle LMS sites that exist worldwide. As an open source platform, Moodle LMS enables your organisation to have complete control over your data, including how and where you store it. And, on top of that, we provide you with the best features and tools to ensure you can keep your learners' data private and secure. As part of Moodle's security procedures, we've set up a security program with Bugcrowd that enables global security researchers to test our platform continuously, easily submitting any security issue through our Vulnerability Disclosure Program. The Moodle Bugcrowd program allows us to streamline the way in which we detect, triage and fix any vulnerabilities, ensuring that we're always on top of security to keep your data safe. In the development of open source software like Moodle LMS, security is an ongoing process. Unlike proprietary software, where the code is hidden and bugs might be exploited, the Moodle community is constantly monitoring the source code and collaborating in making it more secure through public, well-established processes. This means that any bugs are detected and fixed quickly, reducing the impact of vulnerabilities and security breaches. Moodle is widely used in military, banking and other high-security environments, and they frequently conduct penetration testing and report findings to our core team. Our fixes are reported globally through the global CVE network, and applied to supported past releases to make sure they reach as many sites as possible.

GDPR Questionnaire	
Request for clarifications	**Supplier Remarks/Answer**
Our company requires transfer outside of the EEA to have a valid legal basis. Please describe the legal basis for each of the countries that personal data is transferred to.	Moodle will not Process or transfer the Data outside of the European Economic Area except for limited specified purpose and with the express consent of your organisation. If Moodle (on a rare occasion) was required to subprocess any Personal Data outside the EEA it would rely on the Standard Contract Clauses (SCCs) annexed to the relevant Data Processing Agreement with its subprocessor. Those terms are outlined here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en
Describe how Moodle will be able to delete or fully anonymise Personal Data elements or Personal Data relating to specific individuals from the information systems that will be used to deliver the services to our company, both during the engagement and upon termination. In addition, please describe how deletion or anonymisation will cover Personal Data held in any back-up copies or by any (sub) processors.	On termination of the underlying agreement for services or earlier if requested by you, Moodle contractually obligates itself to 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 Moodle's possession, custody and control, except for such information as must be retained under applicable law and insofar as is technically possible. 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 Data Processing Agreement 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.
Is Moodle currently, or has Moodle been involved in any legal proceedings, civil or public, relating to processing of Personal Data in connection with the services that you offer, in the last five years? If so, please elaborate on the nature and document the outcome of these proceedings.	No, not as of the date that this was published (as noted at commencement of the Privacy Notice).
Is Moodle aware of any legal proceedings, civil or public, that any of your (sub) processors have been involved in, relating to processing of Personal Data in connection with the services that you offer, in the last five years? If so, please elaborate on the nature and outcome of these proceedings.	No, not that we are aware of as of the date that this was published (as noted at commencement of the Privacy Notice).
Has Moodle reported any Personal Data Breaches, as defined in art. 4 (12) of the GDPR, relating to your processing of personal data in connection with the services that are offered, to any of your Customers, any Data Protection Authorities or any Data Subjects, in the last five years? If so, please elaborate on the nature of the breach(es).	No, not as of the date that this was published (as noted at commencement of the Privacy Notice).

GDPR Questionnaire	
Request for clarifications	**Supplier Remarks/Answer**
Describe the certifications and audit scheme that Moodle has in place to allow companies to verify compliance with applicable law and the Data Processing Agreement during the contract period.	Moodle undertakes weekly or fortnightly meetings with its External DPO to address ongoing privacy practice measures designed to continue evolving Moodle's privacy procedures with matters including audit outcomes with regard to information security, data protection compliance and undertake such audits on a periodic basis.
Does Moodle process Personal Data on behalf of companies for its own purpose, such as product development, research or analytics, and if so, what is the legal basis for such processing?	No, not without prior informed consent. We process (collect, store and use) the information you provide in a manner compatible with the EU's General Data Protection Regulation ("GDPR").
Do all subcontractors / subprocessors undertake similar terms as outlined in your DPA.	The terms of our Data Processing Agreement as published on our website within our Privacy Notice are functionally mirrored with our subprocessors. That is, we confirm that the text outlined in the Data Processing Agreement represents the written terms to which any sub-contractors or agents are subject to regarding their processing of data on our instruction.
Has Moodle updated its policies to reflect changes to the law since the General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 came into force?	Yes, we have adopted the following pivotal legislation: EU's General Data Protection Regulation 2016/679 ("GDPR"), UK General Data Protection Regulation ("UK GDPR") and the California Consumer Privacy Act 2018 ("CCPA").
Do Moodle team members receive training on data protection and information security?	Yes. As you might imagine, Education is one of our central values. We have a team member online course that all participants undertake which includes directives and learnings from our privacy officers.
Does Moodle allow team members to access your systems remotely? If so, do you have appropriate software and controls in place to ensure secure access?	Yes, with appropriate software and controls.
Does Moodle have appropriate firewalls, intrusion detection software and antivirus software installed on your network and all devices used to access personal data?	Yes, we employ Amazon SecurityHub, Inspector, System Manager, CloudTrail, GuardDuty, and Network Access Controls for a suite of security functionality including Cloud Workload Protection and access control to all servers.
Does Moodle limit access to data on a 'need to know' basis?	Yes, all Moodle team members are limited in their access to data on a 'need to know' basis. User access is restricted by profile status relevant to specific company roles.
Does Moodle have a procedure in place to deal with requests from individuals to exercise their rights under GDPR?	Yes, Data subject access request policy.
Does Moodle have insurance in place for cyber breaches and data breaches?	We have a USD 3,000,000 Cyber Info Security policy that covers all services in the United States territory.
Does Moodle share data with third parties based outside of the EEA? If yes, which of the required safeguards under GDPR are in place with each of those third parties?	Moodle will not Process or transfer the Data outside of the European Economic Area except for limited specified purpose and with the express consent of your organisation. If Moodle (on a rare occasion) was required to subprocess any Personal Data outside the EEA it would rely on the Standard Contract Clauses (SCCs) annexed to the relevant Data Processing Agreement with its subprocessor. Those terms are outlined here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

GDPR Questionnaire	
Request for clarifications	**Supplier Remarks/Answer**
What process does Moodle have in place to ensure that customers are notified when Moodle believes that the processing was not compliant with GDPR?	We only process in accordance with the Data Processing Agreement or your instructions. In fact, the only processing will occur through MoodleCloud or your use of our forums. There is built-in tech to allow users to delete their profile and Terms of Service for MoodleCloud.
Does Moodle carry out regular audits of data protection, privacy and security processes and the systems used to process personal data?	Policies and procedures are reviewed every 6-12 months and updated as necessary.
What process does Moodle have in place for supporting Data Controllers in fulfilling its obligations with regard to data subject rights ie. Right of Access, Right to Erasure etc.	Refer to our Data Processing Agreement which is outlined on our website at: https://moodle.com/privacy-notice/ There you will find many obligations undertaken by Moodle to support Data Controllers and their Data Subjects with queries regarding the Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable). In particular see clause 3.1(c) of the DPA.
Does Moodle archive any personal data that you process on behalf of our company? If yes, where is this data archived and for how long?	Our internal ROPAs provide various deletion periods. Moodle only keeps personal data related to financial / tax information for accounts / audit purposes. On termination of your account, Moodle may retain limited account information, or other documents as required by specific laws or regulations in accordance with applicable statutory periods. Further, where a DPA is enacted: clause 8 of the Data Processing Agreement provides that ".. 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. At Your request, the Processor will provide You with written confirmation of such destruction."
Does Moodle have a process in place for deleting personal data on the request of end users?	Yes. There is a 'Delete my account' function in the top right corner (when logged in), click Your Name, Settings. Scroll down the page to Privacy and policies. Click Delete my account. You can also delete your entire Moodle site from within the applicable Moodle platform.
If Moodle's contract with our company was to terminate, what process do you have in place to ensure that all personal data that you process on behalf of our company is removed and returned to our company or deleted from your systems and what evidence could you provide to confirm that this has been done?	As per clause 8 of our Data Processing Agreement, 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. At Your request, the Processor will provide You with written confirmation of such destruction.
Do the contracts of employment issued to Moodle employees require them to adhere to your data protection rules of behaviour and do they contain confidentiality clauses?	All team members sign confidentiality agreements as part of their onboarding.
Does Moodle conduct regular reporting on security incidents/data breaches involving personal data?	We maintain a security incident register that includes 'near misses'. To date we are proud to say, the register is without material entry.
Who is the person responsible for managing any security incidents/data breaches within Moodle?	Team Lead/Application Security Engineer. Ultimately, Moodle's Privacy Officer is charged with informing Moodle's independent DPO in Ireland, who ultimately informs the Data Protection Authorities. All contacts are made available on our website at: https://moodle.com/privacy-notice/

GDPR Questionnaire	
Request for clarifications	**Supplier Remarks/Answer**
What process does Moodle have in place to enable you to notify companies of a data breach relating to their users?	As per clause 4.2 of our Data Processing Agreement we 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.
From which countries are Moodle employees processing our data?	We have a diverse workforce at Moodle with team members located globally. They login to systems hosted and maintained in specific hubs.
What is the primary location(s) of Moodle's corporate infrastructure?	Moodle predominantly use's AWS servers to host data on behalf of Customers in locations closest to the Customers. Such locations usually include AWS Ireland (for EAA), AWS Sydney (for APAC) and AWS Oregan (for the US).