ASIA-PACIFIC ECONOMIC COOPERATION (APEC)

PRIVACY RECOGNITION FOR PROCESSOR (PRP) SYSTEM

Self-Assessment Form

MindTickle, Inc.

535 Mission St, 14th Floor, San Francisco, California - 94105, United States of America

Scope: Mindtickle Subscription Services (Platform)

Website: https://www.mindtickle.com/

Privacy Notice: https://www.mindtickle.com/privacy-policy/

Contact information: Privacy Team, privacy@mindtickle.com

1. General Information

Name of Organisation	MindTickle, Inc.
Name of point of contact for PRP	Deepak Diwakar
Title	CTO & DPO
Email Address	privacy@mindtickle.com
Contact Number	(800) 231-5578
Company Registration Number	NA

2. APEC PRP System

List of subsidiaries and/or affiliates governed by your privacy policy to be covered by this certification, their location, and the relationship of each to you.

Name of subsidiary and/or affiliate	Location of subsidiary and/or affiliate	Relationship of subsidiary and/or affiliate to you
MindTickle Interactive Media Private Limited	India	Affiliate

For what offering(s) or type(s) of processing service(s) are you applying for recognition?	Mindtickle is a cloud-based SaaS platform (“Platform”) used by organizations to ensure the readiness of their customer-facing teams using training modules, assessment, role-plays, and 1:1 coaching. Mindtickle will process the Personal Data received from its customers for providing the services to its customers. Personal Data may be processed for the following Processing activities: storage and other Processing necessary to provide, maintain and improve the services that Mindtickle provides to its Customers.

SECURITY SAFEGUARDS (QUESTION 1 – 8)

#	Questions	Assessment Requirements (AR)	AR Met?	Controls implemented at Mindtickle
1	Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Where the Applicant answers **YES,** the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	☒ Yes ☐ No	• Mindtickle has a documented Security Policy which covers the personal information that is collected and processed on behalf of the customer. • This Security Policy document aims to define the security requirements for the proper and secure use of the Information Technology services in Mindtickle. • Mindtickle's Security Policy is located at https://www.mindtickle.com/security-policy/.
2	Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans) • Other (specify)	☒ Yes ☐ No	• Mindtickle has implemented Technical and Organizational Security Measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedom of natural persons. • The specific technical and organizational measures implemented by Mindtickle, are documented at- https://mindtickle.com/technical-and-organizational-security-measures/ • These controls are updated from time to time without reducing the overall security

		The Applicant must periodically review and reassess these measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.		posture that has been committed to the customers.
3	Describe how your organization makes employees aware of the importance of maintaining the security of personal information.	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	☒ Yes ☐ No	• The Information Security and Privacy Team at Mindtickle is responsible for ensuring that the employees are aware of the roles and responsibilities related to Information Security and Data Privacy. • Employees are required to undergo information security and privacy training upon hire and a refresher on an annual basis. • The reporting process, roles, and responsibilities regarding information security incidents are included in employee training and published on the company portal. • Information security training includes privacy and data protection related obligations.
4	Has your organization implemented measures to	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of	☒ Yes ☐ No	• Mindtickle uses a number of advanced, cloud-native security tools for ongoing

	detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this principle.		monitoring of malicious behaviour on its cloud infrastructure, where all customer data is hosted. • All application logs have "Who What Where When" information. • Mindtickle has set up following monitoring and alerting mechanisms on the logging services to notify any anomaly to relevant teams - ○ AWS Web Application Firewall on CloudFront, that monitors the requests that are forwarded to CloudFront and help control access to content. ○ AWS CloudTrail and Sumologic to maintain extensive audit logs, including those for system access and changes. ○ AWS CloudWatch is also used for analysing application logs, including those for events pipeline and lambdas. ○ AWS GuardDuty is used for ongoing threat & intrusion detection. ○ AWS Shield is used for DDoS protection, including always-on detection & automatic inline mitigations that provide comprehensive availability protection

				against all known infrastructure (Layer 3 and 4) attacks ○ AWS Inspector is used for automated, regular security assessment ○ CIS AWS foundation benchmark in AWS Security Hub ○ Datadog and PagerDuty are used for application performance monitoring and incident alerting ○ Checkmarx is used to perform vulnerability scanning of the code and third party libraries.
5	Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above?	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	☒ Yes ☐ No	• Mindtickle conducts Vulnerability Assessment and Penetration Testing of Mindtickle platform web applications, network infrastructure and mobile applications (both iOS and Android), covering OWASP top 10. • These assessments include testing for XSS, SQLi and parameter manipulation along with other applicable security vulnerabilities based on application profile. • These assessments are conducted by external independent third-party security auditors on an annual basis to obtain a detailed report on the security vulnerabilities and their status.

6	Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?	The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.	☒ Yes ☐ No	• Mindtickle has a documented Incident Response and Management policy to handle any security incident, covering Identification, validation & severity assignment, immediate resolution, root cause analysis & neutralization and long term resolution planning. This policy is reviewed and tested as part of our SOC2 audit on an annual basis. • Any breach of customers' confidential and private data will be notified to all affected customers within 48 hours of the breach being confirmed.
7	Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	☒ Yes ☐ No	• Mindtickle has a documented Data Retention policy, designed in compliance with all applicable regulations such as GDPR. • Upon contract termination, a customer's data is retained in an inactive state for up to 180 days, after which a hard delete is performed on the data, in accordance with contractual terms. • Active customers and their users can also request deletion of their personal data, including those in accordance with applicable regulations such as GDPR, CCPA and UK DPA 2018 through Mindtickle support team. • Upon request, Mindtickle can provide the customer data in a structured and

				machine readable mutually agreed format.
8	Does your organization use third-party certifications or other risk assessments?	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	☒ Yes ☐ No	• Mindtickle strives to deliver a cloud platform that the customers across the globe continue to trust to run business-critical services. • To this end, Mindtickle has invested heavily in building a highly scalable platform that has best-in-class security & privacy measures and meets the complex compliance needs of today's fast-evolving regulatory environment. ○ SOC2 Type 2 Audit - Mindtickle has audited its platform against the Trust Service Principles and Criteria prescribed by The American Institute of Certified Public Accountants (AICPA) and obtained a Service Organization Control 2 (SOC2) Type 2 report. This third-party assurance audit is performed on an annual basis to obtain an independent opinion on the suitability of the design and operating effectiveness of the implemented controls. ○ VAPT - Mindtickle conducts annual third party Vulnerability Assessment and Penetration Testing (VAPT) of its Web Application, Network Infrastructure and Mobile Application. These assessments are conducted by

				external independent third-party security auditors on an annual basis to obtain a detailed report on the security vulnerabilities and their status. ○ Mindtickle is compliant and certified as Level 1 with Security, Trust and Assurance Registry (STAR), an Open Certification Framework developed by Cloud Security Alliance (CSA) to promote best practice in the security assurance within Cloud Computing. • For additional information regarding security and privacy assessments you can refer to Mindtickle's Trust Page - https://www.mindtickle.com/trust/

ACCOUNTABILITY MEASURES (QUESTION 9 – 18)

#	Questions	Assessment Requirements (AR)	AR Met?	Controls implemented at Mindtickle
9	Does your organization limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant has policies in place to limit its processing to the purposes specified by the controller.	☒ Yes ☐ No	• Mindtickle's standard policy is to strictly use the data as per the contractual agreement. The PII collected from client is not used for any reason but to provide service to the said client, as per the contractual agreement. • Mindtickle, as a data processor, is using "Contract" as a legal basis for processing the personal records provided by Data Controllers.
10	Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	☒ Yes ☐ No	• Upon request by Data Subject, Mindtickle will provide information about whether we hold any of subject's Personal Information. • Further, if the data subject requires Mindtickle's assistance to access, correct, amend, remove, or limit the use or disclosure of any Personal Information that has been collected and stored by Mindtickle, the individual can reach out to us at privacy@mindtickle.com. • Mindtickle responds to data subject's request for change, correction, or deletion of information within 30 days of request and will notify them of the action taken. If the request is complex or we have received a number of requests from

				subject, we may require an additional time of up to 60 days to complete the request.
11	What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing?	The Accountability Agent must verify that the Applicant indicates the measures it takes to ensure compliance with the controller's instructions.	☒ Yes ☐ No	• Mindtickle has implemented the following controls to ensure compliance with the controller's instructions: ○ Mindtickle has implemented Technical and Organizational Security Measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedom of natural persons. ○ The specific technical and organizational measures implemented by Mindtickle, are documented at- https://mindtickle.com/technical-and-organizational-security-measures/ ○ The internal controls are aligned with the additional security and privacy requirements provided by the controller mentioned in the written agreement. ○ Mindtickle maintains a Record of Processing Activities (RoPA). The record of processing activities are automatically updated upon change in the fields and the purpose of

				processing is updated upon change in the privacy policy. ○ As per the instructions in the Data Protection Addendum (DPA), Mindtickle has aligned its internal controls regarding sub-processor communication and breach notification process. ○ Mindtickle employees are required to undergo information security and privacy training upon hire and a refresher on an annual basis. These trainings are conducted to ensure that employees are aware of the confidential nature of the Personal Data that has been received from the Data Controllers. ○ All the controls are tested on an annual basis during the SOC 2 Type 2 audit.
12	Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with the PRP. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with the PRP.	☒ Yes ☐ No	• Mindtickle's Privacy team along with the Data Protection Officer (DPO) are committed to ensure overall compliance with requirements of the PRP.

13	Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	☒ Yes ☐ No	• Mindtickle responds to data subject's request for change, correction, or deletion of information within 30 days of request and will notify them of the action taken. • In case a data subject requires Mindtickle's assistance to access, correct, amend, remove, or limit the use or disclosure of any Personal Information that has been collected and stored by Mindtickle, the individual can reach out to us at privacy@mindtickle.com. • In case where the data subject's details uploaded to Mindtickle platform are controlled by one of Mindtickle's Customer organizations and governed by customer agreement with the data subject (e.g. employee agreement, business partnership agreement, etc.), Mindtickle will forward such request details to the customer. • Upon confirmation from the customer, a suitable response is provided to the data subject and the if required, the data is deleted.
14	Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place for notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information, as	☒ Yes ☐ No	• Mindtickle responds to any law enforcement or government agency requests for data as per legal requirements and in conjunction with the contractual terms agreed with customer.

	require the disclosure of personal information?	well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.		• Further, our publicly hosted Privacy Policy provides details of the instances where data may have to be shared if required by law such as to comply with a subpoena, bankruptcy proceedings, or similar legal process. You can refer to the Privacy Policy on the following link - https://www.mindtickle.com/privacy-policy/. • Mindtickle also maintains a Transparency Report which can be accessed at - https://www.mindtickle.com/information-requests-transparency-report/.
15	Does your organization have a procedure in place to notify the controller of your engagement of sub-processors?	The Accountability Agent must verify that the Applicant has in place a procedure to notify controllers that the Applicant is engaging sub-processors.	☒ Yes ☐ No	• Mindtickle engages a third-party (sub-processor) only for the purpose of providing services to the customers. • Mindtickle performs a detailed evaluation, due diligence, risk assessment, information security approval, and legal reviews prior to onboarding a sub-processor, in accordance with our Vendor Management Policy. • Upon successful completion of the due diligence process, a sub-processor is onboarded and accordingly an advance notice is sent to the customers. • As per Mindtickle's internal process, a sub-processor communication is sent to

				all the customers 60 days prior to data sharing. • The sub-processor communication is sent with intent of providing the details regarding the sub-processors (name and purpose). • The customers have an option to object to onboarding of a sub-processor within 10 days of receiving the sub-processor communication.
16	Does your organization have mechanisms in place with sub-processors to ensure that personal information is processed in accordance with your obligations under the PRP?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such mechanisms is required for compliance with this principle.	☒ Yes ☐ No	• Mindtickle's vendor DPA contains the instructions that must be followed by the sub-processor during the duration of Agreement. • We have strong contractual controls in place to ensure that the sub-processors are aligned with global privacy frameworks such as GDPR, CCPA and APEC PRP. • Prior to onboarding a sub-processor, a due diligence process is performed which includes review of SOC reports of the vendor or its data centres - Information security policies and practices in line with Mindtickle's requirements. The sub-processor is onboarded only upon successful completion of the vendor due diligence process. • The DPA contains the list of Technical and Organizational Security Measures

				which must be implemented by the sub-processor internally to ensure customer data is protected.
17	Do the mechanisms referred to above generally require that sub-processors: (Please describe in the response box if applicable)	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.		
(a)	Follow-instructions provided by your organization relating to the manner in which personal information must be handled?		☒ Yes ☐ No	• All the instructions, related to security and privacy, that Mindtickle commits to its customers are transferred to the sub-processor through written agreements.
(b)	Impose restrictions on further sub-processing		☒ Yes ☐ No	• Mindtickle through contractual agreements with its sub-processors provides the controls which must be implemented at sub-processors organization in order to provide protection to the customer data. • The vendor DPA contains exhaustive list of controls around sub-processing which includes: ○ Implementation of Vendor due diligence process ○ Advance notice prior to onboarding a sub-processor

(c)	Have their PRP recognized by an APEC Accountability Agent in their jurisdiction?		☐ Yes ☒ No	• We have not assessed our sub-processors against this requirement, however, we perform a comprehensive due diligence for all our vendors prior to their onboarding to ensure that they are compliant with the requirements of global privacy frameworks like GDPR, APEC PRP and CCPA. • Mindtickle's vendor DPA contains the exhaustive list of the requirements that should be followed with the vendor throughout the duration of the contract. • These requirements include implementation of technical and organizational security measures, processes around incident management process, sub-processor due diligence process and confidentiality requirements in terms of security and privacy training.
(d)	Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts?		☒ Yes ☐ No	• All the sub-processors undergo a comprehensive security review prior to their onboarding by the Mindtickle's InfoSec Team. This review includes: ○ SOC reports of the vendor or its data centres ○ Information security policies and practices in line with Mindtickle's requirements • Post onboarding, Mindtickle conducts an annual security review of the all its sub-

				processor to ensure continued compliance with the instructions specified in the DPA.
(e)	Allow your organization to carry out regular spot checking or other monitoring activities?		☒ Yes ☐ No	• Mindtickle's vendor DPA contains the "Security Audit" clause which allows Mindtickle to conduct an on-site audit or assessment of the vendor at least once annually.
(f)	Other (describe)		☒ Yes ☐ No	• Mindtickle provides all the instructions related to data retention, handling data subject request as well data disclosure requests received from government or law enforcement authorities, to its sub-processors through the DPA.
18	Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this requirement.	☒ Yes ☐ No	• All the new joiners are required to attend the privacy training which is managed by Mindtickle's Information Security and Privacy team. • Mindtickle also conducts an annual refSresher training which includes privacy related obligations.

END OF DOCUMENT