INSTRUCTURE

Instructure Security

Instructure Security, Engineering, and Operations

June 2020

CANVAS PORTFOLIUM BRIDGE

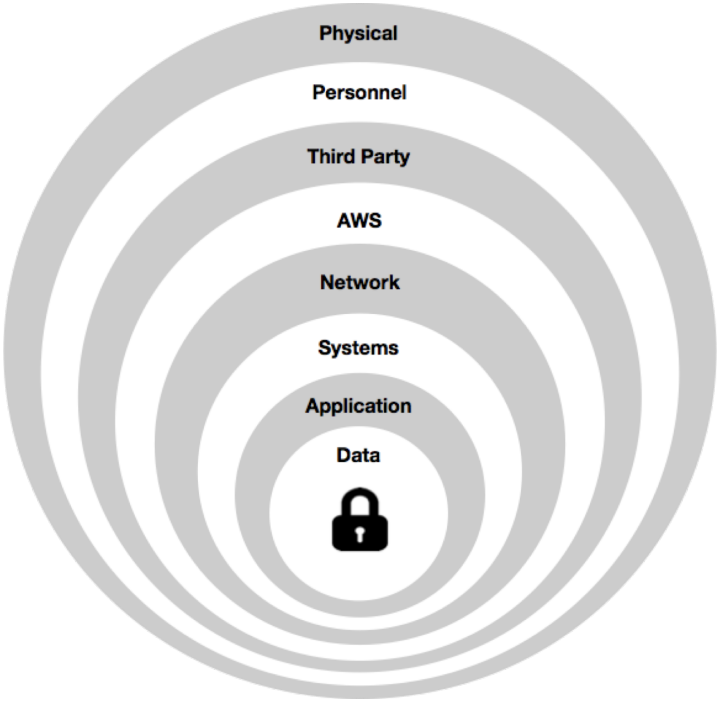
Table of Contents

Instructure Security Program

Instructure has built and operates a robust information security program, which is founded on the guidance provided by International Organization for Standardization's (ISO) 27000, NIST's Cyber Security Framework, AICPA's Trust Services Principles and Criteria, and SANS' CIS Critical Security Controls.

Instructure's security program is led by Instructure's Vice President of Security and has a team of talented, skilled, and experienced information security professionals. Instructure's information security team is responsible for establishing strong security practices throughout Instructure via governance, risk management, policy, education, security engineering, security compliance, security operations, and application security.

Instructure's approach to security includes implementing preventative and detective security mechanisms at each layer between plausible external and internal risks and Instructure's most valuable assets. The following image shows these layers:



This document describes Instructure's approach to securing each of these layers. By securing Instructure and its services in layers, Instructure is able to enact a defense-in-depth approach to protecting customer data.

Physical Security

Instructure hosts all customer-facing web applications and supporting infrastructure on AWS. The AWS infrastructure is highly stable, fault-tolerant, and secure. AWS publishes an insightful security whitepaper that describes how AWS implemented physical security and environmental protection mechanisms to protect AWS data centers throughout the world. Instructure relies on AWS' ability to design and operate these critical mechanisms and controls to protect physical access to data and availability of Instructure's services.

AWS data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards and access is authorized strictly on a least-privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Multiple geographic regions and Availability Zones provide resilience in the face of most failure modes including natural disasters or system failures.

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Generators provide backup power for the data centers of the entire facility.

Additionally, AWS' security controls have been audited by a reputable 3rd party assessment organization, and have produced the following (and many other) attestations and certifications:

- SOC 2 Type II report using the Service Organization Control framework put forth by the American Institute of Certified Public Accountants (AICPA)
- Certified ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)

Personnel Security

Instructure provides employees with security awareness training upon hire and annually thereafter. Included as part of Instructure's security awareness training are valuable insights and guidance related to keeping customer data and Instructure assets secure from the variety of common threats against these assets. Employees are made aware of Instructure's security and other policies, are made aware of common attacks (such as phishing and social engineering), and are required to acknowledge completion of training.

Third-Party Security

Instructure utilizes several third-party organizations to host its products for customers. As part of helping ensure third party organizations are securely providing services to Instructure, Instructure's security team performs thorough vetting prior to, and periodically after, using critical third parties who have access to data or provide essential services.

Instructure utilizes several third parties to provide support for Instructure's products. To help provide reasonable security assurance of the security practices and mechanisms at these third parties, Instructure requests and reviews copies of the third party assurance reports provided by these organizations on an ongoing basis to confirm these controls are operating effectively. Legal contracts with these third parties also include security provisions to help ensure the implementation and operation of effective security controls at the third party organizations.

AWS Security

Instructure products are hosted on the state-of-the-technology cloud infrastructure provided by Amazon Web Services (AWS). The AWS infrastructure is highly stable, fault-tolerant, and secure. For additional information about AWS' security program, certifications and standards compliance, please refer to http://aws.amazon.com/security and http://aws.amazon.com/compliance/.

AWS Network Security

The AWS cloud infrastructure provides extensive network and security monitoring systems to protect the production environment and its data. These systems protect against:

- **Man In the Middle (MITM) Attacks**: All of the AWS APIs are available via SSL- protected endpoints that provide server authentication. Amazon Elastic Compute Cloud (EC2) Amazon Machine Images (AMIs) automatically generate new Secure Shell (SSH) host certificates on first boot and log them to the instance's console.
- **IP Spoofing**: Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**: When port scanning is detected, it is stopped and blocked.
- **Virtual Private Cloud**: Instructure utilizes VPCs in order to further segment, protect, and isolate network traffic.
- **AWS GuardDuty**: Instructure uses AWS GuardDuty to alert and inform on security incidents occurring against Instructure's services hosted in AWS.

AWS Services

The AWS services used to host Instructure products include Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Auto Scaling Groups (ASG), Simple Storage Service (S3), Elastic Block Store (EBS), Virtual Private Cloud (VPC), Simple Email Service (SES), Identity and Access Management (IAM), and several others. Instructure's products are designed to make full use of the real-time redundancy and capacity capabilities offered by AWS, running across multiple availability zones in regions throughout the world. Primary storage is provided by Amazon S3, which is designed for durability exceeding 99.99999999%.

AWS Regions and Data Centers

Amazon Web Services has multiple locations (called "regions") worldwide. Each region is a separate geographic area, and each region has multiple, isolated locations known as Availability Zones. Instructure uses the following Amazon Web Services (AWS) regions:

- US East (N. Virginia) Region
- US East (Ohio) Region (Bridge Only)
- US West (Oregon) Region
- Canada Central (Montreal) Region
- EU West (Ireland) Region
- EU Central (Germany) Region
- Asia Pacific (Sydney) Region
- Asia Pacific (Singapore) Region

AWS Data Security

Data traffic in and out of Instructure's networks in AWS is encrypted using TLS 1.2, forward-secrecy-compliant ciphers whenever possible. The acceptable cipher list is constantly maintained to ensure that no vulnerabilities are present. Data is stored redundantly in multiple data centers and multiple geographic regions through Amazon S3. Instructure products replicate data in near real-time to backup and secondary databases, and data is backed up on a daily basis. Instructure creates daily database backups of data and content to Amazon S3. Data replication and backups ensure that, in the event of a necessary system restore, the potential of data loss would be limited.

Network and Systems Security

Instructure products have been designed to achieve a high level of security by providing an uncomplicated, usable approach to user authentication, system access, and role-based, hierarchical permissions. These products are designed to support institution's own internal security policies and to provide rigorous protection from internal or external intrusions. These products reinforce system security by presenting a simple security model to end-users because research shows that if users have to jump through too many security hoops, they will attempt to find ways to bypass security entirely.

System Access and Authentication

Instructure uses a multiple approval system for granting access to employees. The manager of the employee requesting access must fill out a ticket requesting detailed level of access to the system and specifying which parts, functions, and features are to be accessible by the employee. Clear, valid, and necessary business justification must be provided for the user in question. Other approvals are included as necessary and based on the access being requested. If all parties approve the employee's access, the respective technology team grants access as requested in the ticket. Per the employee exit policy, user accounts are deleted upon termination of employment.

All on-boarded Instructure employees are required to read, understand, and sign Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) compliance forms.

Instructure's technology teams facilitate the installation of keys for all employees with access to the servers. An automated configuration system installs employee public keys on a per-server basis based on need. This same configuration process automatically revokes keys globally when necessary. Employees are required to use full-disk encryption and password protection on their work machines to protect their private keys and other sensitive data. The private keys used for HTTPS are stored encrypted and decrypted by operations when deployed to the application servers.

Monitoring and alerts are in place to detect and warn of any changes to keys, users on the system, login and sudo attempts, and other events of concern.

Application Security

Secure Coding and Development Practices

Maintaining and enhancing security is a disciplined, continual, and ongoing process. Secure coding and security testing are, therefore, integral components of Instructure's engineering and development methodology. All code in the application must go through a developer peer review process before it is merged into the code base repository. The code review includes security auditing based on the Open Web Application Security Project (OWASP) secure coding and code review documents and other community sources on best security practices.

All developers are trained to identify and analyze security issues when writing and reviewing code. Members of Instructure's technology teams subscribe to security-focused lists, blogs, and other resources to maintain, expand, and share the collective body of knowledge. Instructure maintains an internal wiki to discuss and share best practices for the mitigation and prevention of security pitfalls and vulnerabilities. The security and engineering teams keep up-to-date on general security practices, on recent attack vectors, and on any security issues specifically related to the languages, web applications, frameworks, and environments that Instructure employs to develop, host, and maintain Instructure products.

Peer reviews of all source code changes are mandatory. Multiple peer reviews are conducted for each change to the code base to detect and correct any bugs, security flaws, and any other code defects. Changes to code must be validated by peer review before the code is approved and committed to the code base repository.

Testing and Quality Assurance

Once new code has passed peer review, the code is incorporated into the code base and submitted to testing and quality assurance. The new code is deployed to a continuous integration server where it is immediately tested. Instructure's testing team runs the following:

- Unit tests (testing code with code)
- Integration tests (testing code with integrations with other code)
- Selenium tests (testing how code works in the browser) on all the different environments and across different databases.

After passing these tests, the code is incorporated in the main code branch for formal quality assurance (QA). The QA team tests the new code on all supported platforms and browsers.

Customer Identity and Access Management

Instructure's products support centralized identity management and delegated authentication via integration with Central Authentication Service (CAS) and SAML 2.0. If authentication fails, the application looks up the credentials using its internal authentication service. If authentication fails again, the application will deny the user login.

Protocol and Session Security

Instructure's products use HTTPS (HTTP over TLS) for all communication. All inbound and outbound traffic is encrypted using TLS 1.2, ensuring that all personally-identifiable information, credentials exchange, page requests, and session data are secure. These products encrypt data at rest at the database layer. This includes all user information, performance, course information, and test in natively built courses.

Sessions are maintained and can be invalidated. An encrypted session cookie, signed with a hash message authentication code (HMAC), is used only identify a current session. The HMAC and cookie contents are encrypted with Advanced Encryption Standard (AES)-256 in cipher feedback (CFB) mode. The contents of the cookie cannot hijacked during transmission across the network, cannot be viewed or tampered with by the user, and cannot be accessed through javascript. Session IDs are compared and validated against the server-stored values. An invalidated session will require a user to login again.

Sessions are reset on each successful login to prevent access to session IDs by subsequent logins. To prevent cross-site request forgery (CSRF) vulnerabilities, all user actions that modify data require a session secret key to post data. All requests that modify data are done with HTTPS POST or PUT requests, never GETs.

Preventing Cross-Site Scripting (XSS) Attacks

Instructure employs a variety of strategies to prevent cross-site scripting (XSS) attacks. For example, when the application creates a form for user input, a one-time use token is embedded in the HTML form so that the application can identify the form and verify that it did not originate another site in a possible attack attempt.

The applications sanitize content to protect against intentional or unintentional vulnerabilities. When content is put into a form, such as content that a user enters with the Rich Content Editor, the application scrubs (both client-side and server-side) the content and removes any malicious content. Content sanitization prevents session jacking, form hacks, and other unauthorized data access and/or modifications.

All user-inputted content is sanitized before being saved to the database. The sanitization is done by explicit allow listing--not block listing--preventing the addition of JavaScript to HTML data and prevents the addition of unsafe HTML tags as well.

File Upload and Download Security

User-uploaded files are stored in Amazon S3 with unique names and folders. To prevent side-jacking from user uploaded files and preserve the integrity of the system, Instructure's products place uploaded files in the Files repository under a different subdomain to establish a separate security domain in order to take advantage of the browser's same-origin security measures. The browser will enforce security between the uploaded files and the user's session and prevent session jacking. If an uploaded file executes code using JavaScript, Java, Flash, or other technologies, that code will not be able to access the user's session nor be able to make requests to the application on the user's behalf. All file downloads require unique, short-lived authorization keys.

Data Security

Instructure has an established, documented, approved, and disseminated Data Classification, Handling and Encryption Policy . This policy outlines the processes for classifying and handling data during its lifetime. As part of this policy, data are classified as one of the following:

- Confidential
- Internal
- Public

Confidential

Confidential data are sensitive data elements that legally and contractually require security and privacy protection mechanisms. Examples of confidential data include customer data, authentication information, personally identifiable information (PII), payment information, and anything subject to attorney-client privilege. Confidential data are required to be encrypted at all times both in transit and at rest, shared with only appropriate and authorized personnel, and are securely destroyed.

Internal

Internal data are data for internal Instructure use only. These data elements are considered “insider information”, and are secured from the general public. Examples of Internal data are email correspondence, materials marked “Instructure Internal,” and other Instructure information not published or made available publicly. These data elements reside on Instructure systems and are only shared with external entities under a fully executed non-disclosure agreement (NDA).

Public

Public data is data from publicly accessible sources. Examples of public data include data from news articles, press releases, and internet searchable content. At Instructure, data classified as Public do not require any special data handling requirements.

Data Handling

Instructure has developed custom code to validate that all data models are protected against invalid assignment. For example, no user can change foreign keys arbitrarily and all lookups are scoped to the appropriate current user and context. All SQL is built using placeholders and a framework for escaping user input; strings are never directly interpolated or concatenated.

To protect against malicious or accidental data destruction, these applications store data redundantly and employs soft-deletions. Administrators and instructors can recover previous versions of the content pages and submissions.

Instructure maintains versions of all data elements and content by taking a series of periodic snapshots of databases.

Customer data are encrypted over public networks using TLS 1.2 (or higher encryption) protocols with known strong ciphers.

Customer data are encrypted at rest within Instructure's backend databases which reside on AES-256-encrypted AWS Elastic Block Store (EBS) volumes.

Customer objects uploaded to Instructure are stored in Amazon S3 where Instructure relies on AWS' robustly designed and operating physical and logical security controls in place to protect these objects. Instructure has also implemented strong security controls to help control access to these objects stored in S3.

Vulnerability Management and Security Audits

Internal Security Reviews and Vulnerability Management

Instructure's security team conducts vulnerability scans of the production environment and annual third-party code base and penetration testing. Members of Instructure's security team have many years of experience with security audits by major corporations and government agencies. Audit policies and procedures are reviewed on a regular basis and updated as needed by the security team.

The Instructure security team conducts thorough, comprehensive, prescriptive, internal security audits. In these audits, the security team:

- Scans the application externally, using both off-the-shelf and custom internally-built tools.
- Documents potential vulnerabilities, recommends fixes, and implements the most advantageous fix. The fixes are then retested, by both the original discoverer(s) and other, new-to-the-problem team members.
- Pushes fixes made in external libraries to the upstream development activities to be immediately applied and included in official packages instead of waiting for the next scheduled Canvas update release.

External Security Reviews

In addition to our frequent internal security audits conducted throughout the year, Instructure conducts annual, open, third-party security reviews. The open, external security audit is one way that Instructure can demonstrate not only the state of application security, but also our responsiveness to any vulnerabilities. Instructure issues security vulnerabilities to our customers, and because Instructure's products are multi-tenant applications, clients never experience the adverse effects due to unapplied updates or patches due to version differences or added costs or wait times for service packs.

This same level of responsiveness is applied when Instructure receives external input on security outside of the formal audit process. For customers who are interested in conducting their own security audit of Instructure's products, Instructure will, upon request, set up an environment where they can conduct automated and manual vulnerability scanning.

SOC 2 Compliance

Instructure produces, on an annual basis, a SOC2 Type II report covering the following principles: Security, Availability, Confidentiality, Processing Integrity, and Privacy.

Instructure's Response to Security Alerts

Unlike traditional LMS licensed products with service packs which often do not address security problems for weeks or months and which must be applied by the users themselves, Instructure's products are cloud services with a single version of the code base and production environment so that security updates are immediately and automatically applied for the entire client base as part of Instructure's hosting services.

Regular vulnerability scans of the applications and infrastructure are conducted using third-party tools, custom scripts, and open source tools. If any vulnerabilities are detected, Instructure's security and engineering teams work together to analyze, design, and develop the required patch. Security-related patches to the operating system, application software, and libraries are applied within one (1) week except in those cases which have been determined to be high severity. If a high-severity security vulnerability is detected, fixing the vulnerability is given the highest priority by Instructure's security and engineering teams. High-severity security patches will be applied within twenty-four (24) hours by best commercial efforts. In most cases, the vulnerability can be fixed using a hot patch without incurring any downtime to the production environments.

Instructure, in coordination with AWS, takes a proactive approach to enforcing SOC 2 controls. Postmortems are convened after any significant operational issue, regardless of external impact, and retrospective (root cause analysis) documents are drafted so the root cause is captured and preventative actions are taken in the future. Implementation of the preventative measures is tracked during Instructure's weekly operations meetings.

Incident Response Policy and Plan

Instructure has implemented a comprehensive set of security technologies, management and review policies, monitoring operations, and enforcement procedures to ensure that our system and data security meets or exceeds governmental statutes and regulations, industry standards, and institutional requirements. Instructure realizes that no organization is impenetrable and, accordingly, prepares plans to help most effectively facilitate a security incident.

Incident Response Policy

Backing up these preventative measures, Instructure has established a set of prescriptive responses to be executed in the event of unauthorized data exposure. Data exposure occurs when restricted or confidential information is disclosed, exposed, or reasonably believed to have been disclosed or exposed to an unauthorized person, process, or system.

Instructure's data exposure policy has been designed to ensure:

- Earliest possible detection of a system or data security breach;
- Rapid securing of the system and data to prevent further unauthorized exposure;
- Responsive notification to users and other affected parties that confidential or personal information has been or may have been exposed or compromised by a breach in system security.

Incident Response Plan

In the event of a breach of security and potential unauthorized data exposure, Instructure's VP of Security will oversee and execute a plan of action that conforms to the guidelines described in the subsections below. The exact plan of action to be executed and the sequence of the actions taken will depend on the type and scope of the breach in security.

Determine the Scope of the Security Breach

In all cases, Instructure's VP of Security and staff will quickly assess the status of the breach to determine whether the activity is ongoing. If the activity is ongoing, the security staff will take immediate requisite measures to stop the unauthorized activity in order to prevent any further data loss. Once the breach is isolated and stopped, Instructure's VP of Security and staff will begin to ascertain the extent of the breach, the source and type of data involved, the amount of data, and the affected persons and system resources.

Assemble the Incident Response Team

Instructure's VP of Security will assemble the incident response team. The composition and charge of the team will depend upon the type of breach and resulting data exposure. The team conducts a preliminary assessment to help develop a tailored response. Once the incident is contained, this team will also evaluate changes in processes, systems and/or policies to prevent a repeat event.

Control Dissemination of Information

In order to ensure that only accurate, timely information that will not interfere with the ongoing investigation is released, only Instructure's VP of Security will be authorized to provide information to any party outside of the incident response team.

Alert Executive Team

Instructure's VP of Security will alert the appropriate senior administrators including the Instructure executive team, client institution officials, system engineers, and other key players as warranted.

Identify Affected Persons

Instructure's VP of Security will work with institution officials, including Instructure's SVP of Engineering and Instructure's VP of Operations, and the incident response team to determine the identities of affected individuals and determine the extent of the data exposure.

Notify Impacted Organizations

Instructure's VP of Security will work with the SVP of Engineering, General Counsel, VP of Operations, and the incident response team to draft and execute a notification plan. The purpose of the plan is to provide full, accurate, and timely notification that meets or exceeds all statutory requirements. In the case of high severity security issues, affected parties will be alerted immediately while indirectly affected parties will be alerted within forty-eight (48) hours. These legal requirements will vary on a state-by-state basis. Working with the appropriate parties, Instructure's VP of Security and the incident response team notify all affected individuals and develop remediation strategies as appropriate and sufficient to the situation.

Manage the Incident Resolution and Aftermath

Instructure's VP of Security and the incident response team will continue to update and communicate response status, determine next steps, and develop a postmortem plan to review the efficiency and effectiveness of the response and develop future prevention and/or mitigation processes and procedures.

FERPA Compliance (Canvas)

FERPA Overview

FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools and institutions that receive funds under the applicable program of the U.S. Department of Education. FERPA provides students, and in some instances parents, the right to inspect their education records and some ability to control the disclosure of information contained in their education records.

FERPA requires educational agencies, which disclose personally identifiable information from a student's education record to other school officials, to use "reasonable methods" to insure school officials obtain access to only the education records they have legitimate educational interests in.

Canvas' Compliance with FERPA

Canvas was built to comply with the Family Educational Rights and Privacy Act (FERPA) by design, and Canvas readily integrates with other campus systems to prevent unauthorized access to FERPA-protected data. Whether implemented as a standalone system or as a fully integrated component of the campus IT/IS infrastructure, Canvas provides educational institutions and agencies with multiple mechanisms and technologies to manage, enforce, and comply with the provisions of FERPA and to fulfill their responsibilities under its requirements.

General Data Protection Regulation (GDPR)

GDPR stands for the General Data Protection Regulation. The GDPR is a European Union ("EU") law that regulates the personal data of individuals in the EU. It replaced the EU Data Protection Directive, the EU's current privacy law, which has been in place since 1995. The GDPR harmonizes data protection law across Europe and introduces sweeping changes that require companies to make significant updates to their privacy and security policies and practices. Instructure is committed to helping our customers comply with GDPR.

Instructure has complied with the European Commission's replacement law for the Data Protection Directive 95/46/EC, the General Data Protection Regulation ("GDPR"), since the enforcement date (25 May 2018).

To ensure ongoing compliance with the GDPR, Instructure does the following:

- Educates the organization about GDPR and its requirements.
- Has Conducted a GDPR gap analysis with the help of a reputable outside law firm experienced with GDPR, and has closed those gaps.
- Maintains an up-to-date listing if personal data Instructure holds, where it came from, and who Instructure may share it with.
- Maintains current privacy notices that comply with the GDPR.
- Ensures existing procedures cover all the rights individuals have under GDPR, including deleting personal data.
- Identifies our lawful basis for processing personal data, documenting it, and updating our privacy notice to explain it to individuals.
- Reviews how Instructure obtains, records, and manages consent.
- Reviews and updates contracts with third parties to ensure our privacy obligations are up to date.
- Ensures the right procedures are in place to detect, report, and investigate a personal data breach.
- Maintains processes for Data Protection Impact Assessments.
- Has appointed a Data Protection Officer.

Safeguards for Cross-Border Data Transfer

One of the GDPR's requirements is that any personal data transferred "cross-border", i.e., outside of the EU, can only be moved pursuant to a legal mechanism. The Privacy Shield Framework is one legal mechanism to make these cross-border data transfers to the United States legitimate. Instructure self-

certified under the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield in November 2017 and our certification remains in good standing, which helps us comply with this requirement of the GDPR.

Instructure also uses the European Commission's Standard Contractual Clauses (model clauses) as an alternative, lawful method to transfer personal data outside the EU. By incorporating these model clauses into Instructure's Data Processing Addendum ("DPA"), both data controllers (Instructure's EU-based customers) and data processors (Instructure) are contractually obligated to certain technical and organizational safeguards relating to individuals' (Instructure's EU-based customers' end users) privacy rights.

Instructure has always taken privacy seriously andhas a longstanding practice of undertaking internal privacy assessments of our products and of adopting a "privacy by design" approach to product development.