Driving innovation together

Data Protection Impact Assessment on Instructure's Canvas LMS

SURF Vendor Compliance

Authors: Valerija Kornilova, Julian Rill
Version: 1.0
Date: December 18th, 2025

Contact: vendorcompliance@surf.nl
DPIA by: https://vendorcompliance.surf.nl/en

Revision History

Version	Date	Author(s)	Changes
0.1	18-05-2025	Valerija Kornilova, Julian Rill	Initial version of part A.
0.2	28-05-2025	Valerija Kornilova, Julian Rill	Revised version of part A after review by Sandy Janssen.
0.3	14-07-2025	Valerija Kornilova, Julian Rill	Revised version of part A after review by Instructure. Chapters changed: A.3.1, A.4.4, A.5.2, A.5.3.3, A.5.5, A.5.7, A.5.11, A.5.12.1, A.5.12.2, A.5.12, A.6.3, A.6.3.3 A.6.4, A.6.5, A.6.7. Initial versions of parts B, C and D.
0.4	08-08-2025	Valerija Kornilova, Julian Rill	Revised version of parts B, C and D after review by Sandy Janssen.
0.5	24.10.2025	Valerija Kornilova, Julian Rill	Revised version after the meeting with Instructure on the 18th September.
0.6	26.11.2025	Valerija Kornilova, Julian Rill	Revised version after the meeting with Instructure on the 18th November about mitigating measures.
1.0	09-12-2025	Valerija Kornilova	Revised version after the feedback from Instructure for the version 0.6.

Review Record

Version	Date	Reviewer(s)	Notes
0.1	19-05-2025	Sandy Janssen	Review of part A.
0.2	19-06-2025	Instructure	Review of part A.
0.3	23-07-2025	Sandy Janssen	Review of parts B, C and D.
0.5	18-11-2025	Daisy Brugman, Jan Landsaat	Review of parts A, B, C and D.

Approval Record

Version	Date	Approver(s)	Notes
0.1	19-05-2025	Sandy Janssen	Approved with minor adjustments and clarifications to be made.
0.3	23-07-2025	Sandy Janssen	Approved with minor adjustments and clarifications to be made.

Table of contents

List of Tables and Figures

Glossary of Terms

Term	Abbreviation	Definition
Application Programming Interface	API	A set of rules and protocols that allows different software programs to communicate and exchange data or functionality with each other. It acts as a middleman, enabling applications to interact and perform actions in a structured way[1].
Customer	*N/A*	Means an organisation that purchases services from Instructure.
Customer managed Key	CMK	A customer-managed key is an encryption key that is generated, owned, and controlled by the customer rather than the service provider. The customer is responsible for managing the key's lifecycle.
Data Processing Agreement	DPA	An agreement between a data controller (such as an educational institution) and a data processor (such as a third-party service provider).[2]
Data Protection Impact Assessment	DPIA	Describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.[3]
Data Transfer Impact Assessment	DTIA/TIA	Assesses the risks that may arise when transferring personal data from one country to another, particularly outside the EU/EEA, if such third countries do not have an adequate decision.[4]
Dutch research and educational institution	Educational institution	All research and education institutions in the Netherlands—primarily SURF member institutions—including, but not limited to, university medical centres (UMCs), technical universities (TUs), research universities (WOs), universities of applied sciences (HBOs), and secondary vocational education institutions (MBOs).
European Economic Area	EEA	A single market that includes the 27 EU Member States and three EFTA (European Free Trade Association) countries: Iceland, Liechtenstein, and Norway.[5]

[1] IBM. "SDK vs. API: What's the difference?" IBM Think (blog), April 17, 2025. https://www.ibm.com/think/topics/api-vs-sdk.

[2] Autoriteit Persoonsgegevens. "Processing Agreement," April 9, 2025. https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/processing-agreement.

[3] Autoriteit Persoonsgegevens. "Data Protection Impact Assessment (DPIA)," April 9, 2025. https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia.

[4] European Data Protection Board. "International Data Transfers." Accessed May 28, 2025. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en.

[5] Eurostat. "Glossary:European Economic Area (EEA)." Accessed May 28, 2025. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European_Economic_Area_(EEA).

K-12	N/A	K-12 encompasses all the years of schooling from the very beginning of formal education through graduation from high school, before a student would typically move on to higher education (college or university) or the workforce. It refers to the publicly supported primary and secondary education system in these countries, though private K-12 schools also exist.[6]
Learning Tools Interoperability	LTI	A standard developed by IMS Global Learning Consortium that enables secure and seamless integration of external learning tools with learning management systems (LMS).[7]
Open source	*N/A*	Software whose source code is publicly available for anyone to use, view, modify, and redistribute. This contrasts with proprietary or closed-source software, where the source code is not accessible to the public.[8]
SURF Vendor Compliance	SVC	SURF's internal team conducting this DPIA. Undertakes compliance assessments on vendors where industry demand exists for in-depth discussions around privacy and security.[9]
Sharding	*N/A*	Horizontal partitioning such as design principle whereby rows of a database table are held separately, rather than splitting by columns.
Software Development Kit	SDK	A collection of software tools used by developers to create applications for specific platforms, operating systems, or programming languages. These kits typically include building blocks, debuggers, frameworks, and code libraries that help developers build software more efficiently and effectively[9].
Software as a Service	SaaS	A software distribution method in which a service provider gives customers access through the internet to applications, usually ones developed and owned by the provider[10], without the need for educational institutions to manage the underlying infrastructure themselves.

[6] Oxford Advanced Learner's Dictionary. "K-12 Adjective." Accessed May 28, 2025. https://www.oxfordlearnersdictionaries.com/definition/english/k-12.
[7] Instructure Community. "What Are External Apps (LTI Tools)?," May 27, 2025. https://community.canvaslms.com/t5/Canvas-Basics-Guide/What-are-External-Apps-LTI-Tools/ta-p/57.
[8] Opensource.com. "What Is Open Source?" Accessed May 28, 2025. https://opensource.com/resources/what-open-source.
[9] SURF. "About Compliance Services." SURF Vendor Compliance, June 3, 2024. https://vendorcompliance.surf.nl/en/about-compliance-services/.
[10] "SaaS Definition." In Dictionary.Com, August 7, 2023. https://www.dictionary.com/browse/saas.

Summary

This report is a data protection impact assessment (hereinafter: DPIA) on the use of the SaaS applications Canvas Learning Management System ('LMS') by Dutch educational and research institutions (hereinafter: educational institutions), offered by Instructure B.V. (hereinafter: Instructure). This DPIA is a central DPIA, carried out by sector organisation SURF, which provides institutions with a general framework for assessing data protection risks within Canvas LMS.

Scope: Canvas Learning Management System (LMS)

This DPIA focuses on the key functionalities and major features of Canvas LMS used by Dutch educational institutions. Canvas is a web-based educational platform developed by Instructure that supports schools, colleges, universities, and other organisations in managing digital learning. It is widely used across higher education (including universities of applied sciences and vocational colleges) and in K–12 settings to organise courses, distribute materials, communicate with students, and assess learning outcomes. Canvas LMS forms part of the broader Instructure Learning Platform.

Canvas LMS is largely open-source software. Instructure provides a hosted and fully managed Software-as-a-Service (SaaS) version, which is the focus of this DPIA. This corresponds to the deployment model used by most SURF member institutions, rather than institutions hosting Canvas on their own infrastructure.

Outside of the scope are the following services:

- Canvas Studio (video learning platform);
- Catalog (course catalogue system, branded marketplace);
- Canvas Credentials (professional learning for educators);
- The processing of children's data in Canvas LMS.

Outcome of the DPIA

This DPIA identified 3 high, 9 medium risks and 2 low risks associated with the use of Canvas LMS. Measures have been proposed for all these risks to reduce the risk level to low, both on the part of the institutions and on the part of Instructure.

During the DPIA process, Instructure demonstrated a high level of cooperation, supporting SURF at every stage and providing transparent insight into its processes. As the result of the mitigation measures negotiations, SURF and Instructure agreed on the following mitigating measures which are mentioned in Part D Description of Proposed Mitigation Measures.

Below, there is the summary of the risks SURF had identified thoughout the DPIA process. Additionally, mitigating measures were proposed to Instructure. After reviewing these measures, Instructure offered the measures to SURF that are feasible to mitigate the risk.

Nr.	Risk	Measures institutions	Measures Instructure
1	Insufficient information provided in the DSAR: Despite the DSAR's good structure and comprehensive format, the insufficient information provided poses a high risk due to opacity in data flows within Canvas LMS, which can lead to loss of control over personal data	Institutions will have an opportunity to file the service tickets through a standard operational procedure with a customer. Institutions will share their feedback directly with the vendor.	Add additional product data to the existing output format for DSAR in the areas of course content, assignment details, discussions, and assessment as referenced in the SURF analysis. Improve the format of the DSAR output to provide additional context, categories, and details alongside the raw data outputs. Include relevant customer service ticket data and communications in DSAR output along with product data.
2	Retention period misalignment with purpose: Instructure's current data retention practices, retaining backups for up to 4 months without clear purpose.	Establish a clear internal data retention and deletion policies and require Instructure to follow the retention periods. Monitor deletion requests and outcomes which are initiated by educational institutions.	Instructure provided the purpose for selecting the 4-month data retention period. The period was chosen for the reason of standardising retention period across all products, and to align with industry best practices. Instructure specified that '*We did not find any company who had a full restore greater than 4 months*'. SURF advised to include this purpose in the document 'Business and Continuity Disaster Recovery' from September 2025 and recurring updated documentations.
3	Leveraging feedback: The significant likelihood of users inadvertently uploading personal data and the use of Case IDs linking submissions to individuals.	Institutions can raise user awareness through internal guidance. For example, providing LMS usage guidelines.	The support team has added the following language in the submission box: "*Please do not include any personal, sensitive, or confidential information in this form. Submissions are intended solely for feedback purposes."*
4	The logging session and anonymisation features against data protection risks: Canvas LMS provides limited	Provide clear internal guidance on the purposes of the anonymisation such as explaining clearly to data	Instructure will update user help guides/documentation/descriptions to clarify the meaning of anonymization for this feature, explicitly stating that it is not

	anonymisation features focused on interface-level privacy during grading and feedback.	subjects that certain features marked as 'anonymisation' do not fully anonymise data. This falls within another purpose: pedagogical purpose.	designed as a data anonymization feature.
5	Nature of the data involved and excessive retention in the Inbox: Identifiable metadata and the potential processing of sensitive data through user-uploaded attachments, such as health information, which may be uploaded unintentionally	Attachments in an inbox is standard functionality which data subjects and institutions would normally navigate with intention. Therefore, institutions should develop training and procedures for data subjects to navigate the features of the Inbox.	Instructure customer implementation and support teams are informed and able to provide best practices guidance to institutions. Instructure will investigate additions to the user experience that add warnings/guidance when a user uploads content; with the goal of providing a follow up timeframe and specific improvements.
6	Analytics and Google Cloud Looker: International data transfers Analytics service provided by Instructure, which operates through Looker, a Google Cloud–based business intelligence platform using role-based access control (RBAC) to manage data access.	Disable Analytics features by default. If institutions would want to use the features, there will be separate options available. Educate teachers and administrators to not use these analytics features for profiling purposes. Raise awareness about the ethical contstraints of analytics features.	Instructure allows disabling of the Intelligent Insights add-on product, which would prevent all use of Looker for analytics. Instructure will update sub-processor statement for Intelligent Insights product as well as Course and Admin Analytics to clarify use of Looker is only for these specific analytic solutions in Canvas. Instructure allows the disabling of Admin Analytics and Course Analytics to ensure Looker is not used for data visualisation.
7	Analytics and Google Cloud Looker: purpose and data minimisation risk The use of Analytics and involvement of the third-party Looker may lead to the collection and processing of more personal data than necessary for the stated purpose of providing	Disable Analytics features by default. If institutions would want to use the features, there will be separate options available. Educate teachers and administrators to not use these analytics features for profiling purposes.	Instructure allows disabling of the Intelligent Insights add-on product, which would prevent all use of Looker for analytics. Instructure will update sub-processor statement for Intelligent Insights product as well as Course and Admin Analytics to clarify use of Looker is only for these specific analytic solutions in Canvas. Instructure allows the disabling of Admin Analytics and Course

	data visualization services.	Raise awareness about the ethical contstraints of analytics features	Analytics to ensure Looker is not used for data visualisation.
8	Lack of transparency: Masquarading Masquerading poses the risk of unauthorized access to personal data and undermines transparency, as users are not notified before or after such sessions.	Disable masquerading. Strict access controls in order to limit masquerading permissions only to essential personnel and roles, applying the principle of least privilege. Enhanced oversight and monitoring. This will allow to regularly review audit logs and establish automated alerts for suspicious or unauthorized masquerading activities. User notifications: Inform users promptly when their accounts have been accessed via masquerading, both before and after the session, to enhance transparency.	Instructure will add the ability, via site level setting, to notify an end user via existing notification services when an admin has used the masquerade feature to access their account. Instructure will update existing “Act As” (masquerade) feature to inform the admin user that the end user will be notified of their action. Instructure will update relevant help/guides based on feature changes for masquerade and best practices.
9	Instructure Community: lack of control over the data processing When users access the Canvas Community via single sign-on from their institutional Canvas LMS account, their profiles are automatically created and publicly display personal information such as full name, username, join date, and activity history.	Disable this feature	Instructure has already implemented new technology. The old Community platform was built in Khoros and the new Community platform is implemented in Higher Logic Vanilla and has gone live.
10	Lack of transparency and incomplete user information: Consent	Admin level setting to opt- out.	Conducting a cookie audit across our products and will update our cookie notice.

	Risks related to insufficient transparency and unclear consent regarding the collection and processing of personal data.		Implement an updated cookie consent tool that will allow for the needed information and control of cookies to users.
11	API Security and token management in Canvas LMS environment The risks remain, including token compromise. Where unauthorized parties gain access to tokens and token generation misuse, this allows malicious actors to exploit weaknesses in token issuance.	Monitor token usage and unusual access patterns.	Instructure requires user API tokens for API access to expire no longer than 180 days from creation. Admins are able to set shorter expiration timeframes on user API tokens. Admins can revoke user keys immediately. Instructure is planning to make additional improvements to API management and reporting throughout 2026 focused initially on 3rd party (partner) API usage. Exact timeframes are still pending technical discovery and planning. • Enhanced reporting on 3rd party partner API usage showing overall traffic and usage against endpoint domains or scopes. • Improved configuration over scopes and permissions for developer keys. • The ability to manage rate limiting for specific partners or developer keys.
12	Residual personal data in legacy backups No currently performing regular reconciliation or validation to ensure deleted data is scrubbed	Be specific regarding contractual requirements on backup deletion and verification.	Instructure defined the 4-month retention period to standardize retention period across all products, and to align with industry best practices. Back-ups are already encrypted and scrubbed.
13	Lack of effective encryption key management for education institutions	Education institutions can add specific encryption requirements in their DPAs. That the	Instructure should ensure that personal data is education institutions' tenant is encrypted before this data is uploaded.

	Instructure does not support the Customer managed keys (CMKs)	encryption should be stored in the EU. Education institutions should request key management controls where vendor describes how encryption keys are generated, stored, and rotated. Ask the vendor to limit personnel access to encrypted data.	
14	Unauthorised access to EU personal data Instructure's support staff can access the EU Customer data	Institutions can strengthen contractual and Governance controls such as the DPA explicitly stating that access to EU personal data by non-EU support staff is permitted only when necessary.	Instructure committed to develop a basic ability (likely globally on or off) to allow the customer to limit Instructure support staff access with additional improvements planned by November 2026. This capability will not be on by default as it can severely limit support response times for users and customers. Customers can request that it be enabled if required and with awareness of potential impacts to support.

Table 1 Overview of risks and mitigating measures as the result of the conducted legal and technical research of the DPIA

Conclusion

The DPIA identified 4 high risks, 8 medium risks and 2 low risk for data subjects. The risks arise from the transparency limitations, product's functionalities, and the use of subprocessors. If the proposed measures are implemented, all medium and some high risks will be reduced to low risks. It is important to note that high risks identified in this DPIA may be mitigated by educational institutions. For example, risks regarding the usage of the sub-processor Looker, using the functionality Masquarading and Canvas Community may be low or even remote for educational institutions if they disable these features for their internal use. Instructure has committed to several measures to reduce privacy risks. Once these features are implemented, SURF will review them and reassess the current high-risk classifications.

Throughout the DPIA process, Instructure has demonstrated a strong commitment to addressing the identified risks and has proactively begun implementing mitigation measures prior to the completion of the assessment. These measures are outlined in Part D under the section of the table titled 'Suggested Measures by the Vendor.' Instructure

specified the timelines that this vendor will require to mitigate the remaining risks. Educational institutions may review the timline in Part D.

The result of the DPIA is that educational institutions are advised to continue using Instructure's Canvas LMS given the support and commitments that Instructure proposes to educational institutions. In 2026, SURF will evaluate the new features and guidance for the users implemented by Instructure and reassess the risks identified in this DPIA.

Introduction

Canvas LMS is an application for planning, implementing and assessing specific learning processes, developed and maintained by Instructure, an educational technology company. This Data Protection Impact Assessment (DPIA), commissioned by the higher education sector and conducted by SURF, the Dutch IT cooperative of education and research, examines the personal data processing that occurs when Canvas LMS is used by Dutch higher-education and research institutions.

About SURF

SURF is the collaborative organisation for IT in Dutch education and research, owned by its member universities and research institutes. Through SURF, members jointly procure high-quality digital services, develop and share knowledge, and ensure compliance with data-protection regulations.[11] As part of its services, SURF conducts umbrella DPIAs for IT services widely used across the sector.[12]

What is a DPIA?

DPIA stands for Data Protection Impact Assessment and must be performed by data controllers when they process personal data in a way that may "result in a high risk to the rights and freedoms of natural persons", according to article 35 of the General Data Protection Regulation (GDPR). The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as freedom of expression. The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains:

"This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

Umbrella DPIAs versus Individual DPIAs

In GDPR terms, SURF is not the data controller for the processing of personal data via the use of

[11] SURF.nl. "About SURF," June 19, 2025. https://www.surf.nl/en/about.
[12] SURF.nl. "Suppliers Compliance Services," n.d. https://www.surf.nl/en/services/procurement-contracting/surf-vendor-compliance.

Canvas LMS. The data controller is the individual educational or research institution that uses this service. However, as the Dutch IT cooperative, SURF takes the responsibility to assess the data protection risks for the end users and to ensure the data processing complies with the GDPR. Therefore, SURF conducts umbrella DPIAs to assist its members to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only the organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and vulnerability of the data subjects. The Dutch DPA has endorsed this approach to improve the protection of personal data within the Education sector.[13] This umbrella DPIA is meant to help educational and research organisations with the DPIA they must conduct when they deploy Canvas LMS, but it cannot replace the specific risk assessments the organisations must make themselves.

Performing one umbrella DPIA on an IT service has benefits for SURF's members, as well as for the vendors of the products SURF assesses. For the members, it saves the cost of each of them having to do an entire DPIA individually. They are also able to incorporate their combined knowledge about a product and experiences with a vendor in the umbrella DPIA. Additionally, SURF can more effectively negotiate mitigating measures with the vendors, because it has the combined negotiating power of the entire sector as a representative. For the vendors, it saves time, effort and money as well to not have to assist every institution individually with DPIAs that will likely be very similar. It's also more efficient for them to be able to implement measures that benefit all members at once.

DPIA Criteria

The Dutch Data Protection Authority (DPA) has identified seventeen types of data processing for which a DPIA is always mandatory in the Netherlands. If a processing activity is not on this list, organizations must independently determine whether it is likely that the processing of personal data is to pose a high risk for data subjects.

The European national supervisory authorities (hereinafter referred to as the Data Protection Authorities or DPAs), united in the European Data Protection Board (EDPB) has published nine criteria to help assess risk. If a processing activity meets at least two of these criteria, a DPIA is required.

The circumstances of the data processing via Canvas LMS meet four out of the nine criteria defined by the EDPB: [7]

1. Sensitive data or data of a highly personal nature (criterion 4). The EDPB explains: *"some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected)."*
2. Data processed on a large scale (criteria 5). Working Party 29 recommends that the following factors should be considered when determining large scale processing:

[13] Dutch DPA (in Dutch only), Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6, URL: https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.
European Data Protection Board, 'Be compliant — SME Data Protection Guide' (EDPB, April 2023) https://www.edpb.europa.eu/sme-data-protection-guide/be-compliant_en accessed 24 October 2025.

a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population. Large-scale data from their entire Canvas instance via Canvas Data Service.[14]
b. the volume of data and/or the range of different data items being processed;
c. the duration, or permanence, of the data processing activity. The processing of personal data varies from normal categories of data to special categories of data.
d. the geographical extent of the processing activity. Since both the USA and Europe are in the geographical scope.

3. The processing involves data relating to vulnerable data subjects (criterion 7). Both employees and students whose personal data are processed through Canvas LMS are in an unequal relationship of power with the education and research organisations.

The Scope of this DPIA

In this DPIA we will look at Canvas Learning Management System (LMS). Canvas LMS is a web-based educational platform developed by Instructure that helps schools, colleges, universities, and organisations manage digital learning. It is widely used in higher education (including universities of applied science and vocational colleges) and K-12[15] to organise courses, distribute materials, communicate with students, and assess performance. It is part of the Instructure Learning Platform.

Canvas LMS is largely open-source software. Instructure offers Canvas LMS hosted and managed as a Software as a Service (SaaS) product, which is what we look at in this DPIA. Most of SURF's member institutions make use of this offering, rather than hosting the product themselves on their own infrastructure platform.

Within Canvas LMS, we looked at the key functionalities and major features that the education institutions in the Netherlands use.[16]

Moreover, some rarely or never used Canvas features are left out of scope as well: ePortfolios, Mastery Paths, Chat, Intelligent Insights, and the Course Import Tool. Other features, such as the Canvas App Center, are also left out of scope, as these facilitate LTI integrations with external parties. The in-scope features are described in A.1.1.

Within Canvas LMS, we determined the scope based on two questionnaires. One questionnaire was sent to the main Canvas stakeholders of SURF's member institutes, and the other questionnaire was sent to the Benelux (Belgium, Netherlands, Luxembourg) user group of Canvas. In these questionnaires, we asked, among other things, which Canvas products and features they use and what business processes they fulfil with the product. In

[14] Instructure Inc., "Institutions & Educators Privacy | FAQ" (Instructure) https://www.instructure.com/privacy-security/instututions-educators-faq accessed 24 October 2025.
[15] In Glossary of terms: K-12 encompasses all the years of schooling from the very beginning of formal education through graduation from high school, before a student would typically move on to higher education (college or university) or the workforce. It refers to the publicly supported primary and secondary education system in these countries, though private K-12 schools also exist.
[16] Instructure, 'Canvas Basics Guide – What is Canvas?' (Instructure Community) https://community.canvaslms.com/t5/Canvas-Basics-Guide/What-is-Canvas/ta-p/45 accessed 24 October 2025.

addition, the scope was further refined by having meetings with key Canvas stakeholders of our member institutes to discuss their process of using Canvas LMS in day-to-day activities.

Outside of the scope of this DPIA are the services of Instructure such as:

- Canvas Studio (video learning platform);
- Catalog (course catalogue system, branded marketplace);
- Canvas Credentials (professional learning for educators);
- The processing of children's data in Canvas LMS.

Methodology

This DPIA was developed through a multi-faceted approach combining desk research, technical research, and structured engagement with Instructure. The aim was to evaluate both the legal and technical dimensions of personal data processing within Canvas LMS.

Desk Research formed the foundation of the legal and policy analysis. This involved systematically reviewing documentation provided by Instructure, including data processing agreements, privacy policies, internal procedures, and relevant information security certifications. These documents were assessed against GDPR obligations, with particular attention to the legal basis for processing, data subject rights, international transfers, and roles of the parties involved. In cases where ambiguities or gaps were identified, SURF issued targeted follow-up questions to Instructure. Their responses were incorporated into our findings, and their opportunity to clarify positions contributed to the accuracy and fairness of the assessment. The outcomes of this documentation review are integrated throughout the DPIA.

Technical Research focused on understanding the data lifecycle within Canvas LMS from a systems and architecture perspective. This included evaluating how data is collected, processed, stored, shared, and secured. The investigation drew upon available technical documentation and system design descriptions, alongside real-world and live testing of the system, and interactive discussions with Instructure. Specific areas of analysis included data flows, storage methods, system logs, privacy-related settings, and the application of security controls. These findings were then cross-referenced with the legal review to assess alignment between stated policies and technical implementation, and to identify any areas of residual risk or non-compliance.

The DPIA used a grey box methodology, which blends aspects of black box and white box approaches. This allowed SURF to maintain an independent, external perspective while also engaging in focused, informed access to specific parts of the systems. It offered a pragmatic balance. It's sufficiently thorough to examine high-risk areas in depth, yet not so demanding as to resemble a full system inspection. In practical terms, we started with an external analysis based on observable behaviours and available documentation, then followed up by verifying key findings through direct collaboration with Instructure.

Outline of this DPIA

This DPIA is based on the structure of the Model Gegevensbeschermingseffectbeoordeling Rijksdienst (DPIA), and on the structure developed by SURF Vendor Compliance team. This combination helps to implement the technical investigation results with legal analysis.

This DPIA uses a structure of four main divisions, which are reflected here as “parts”.

A. Description of the factual data processing
B. Assessment of the lawfulness of the data processing
C. Assessment of the risks for data subjects
D. Description of mitigation measures

Part A explains the processing activities using Canvas LMS in detail in general terms, based on the tested setup.[17] This part describes the services within the scope of this DPIA, we will look at the purposes of the data processing from the perspective of the vendor as controller and processor, analyse project documentation such as privacy statements, security and privacy certifications. For this part, project documentation has been reviewed, as well as the contracts with Instructure. In addition, test scenarios were executed, and a data subject access request was submitted.

Part B provides an assessment by SURF of the lawfulness of these data processing activities through Instructure. This analysis starts with an analysis of the extent of the applicability of the GDPR and the ePrivacy Directive, in relation to the legal qualification of the role of Instructure’s Canvas LMS as provider. Subsequently, SURF has assessed conformity with the key principles of data processing, including transparency, data minimisation, purpose limitation, and the legal ground for the processing, as well as the necessity and proportionality of the processing.

Part C assesses the risks to the rights and freedoms of the data subjects created by the processing activities identified in Canvas LMS in Part A of this DPIA. It names specific risks that derive from these processing activities and aims to specifically determine both the likelihood that these risks may occur, and the severity of the impact on the rights and freedoms of the data subjects if the risks occur.

Finally, **Part D** contains concrete measures that can be taken by Instructure, the educational institutions to mitigate the risks identified in Part C. These measures might either reduce the chance of the risks to occur, or the impact they might have, or both. Part D also contains an assessment of any residual risk attached to the use of Canvas LMS that could not be mitigated by applying the suggested measures. If such unmitigated risks remain, the educational institution implementing Canvas LMS might be required to consult the supervisory authority prior to the processing.

[17] Find the test scenarios in Appendix 1.

Part A Description of Data Processing

Part A of this DPIA provides an overview of the relevant facts of the data processing operations. It describes the data processing operations, the processing purposes and the interests in the data processing operations. In addition, Part A provides an overview of the personal data processed, the parties involved, and the techniques and methods of data processing. Also covered are the legal and policy framework and retention periods.

A.1 Description of Services

In this section, we will describe the architecture of the Canvas LMS, provide an overview of its underlying system design, core components, data flows, and the technologies that support its scalability, security, and performance in delivering digital education at scale.

A.1.1 Canvas LMS

The SaaS-hosted offering of Canvas LMS is a cloud-based learning management system (LMS) provided by Instructure that supports educational institutions in managing, delivering, and monitoring online learning. This system is hosted on Amazon Web Services ('AWS') which is described in the Section A.1.2Architecture. This is described Canvas enables instructors (teachers and other educational staff) to create courses, grade assignments, track student progress, and facilitate communication between teachers and students.[18]

This platform includes a range of services and features designed for the online learning environment. To be more specific, these are the features that SURF analysed in this DPIA:

- **Assignments**: Instructors can create and share course content, including assignments, to assess student learning.
- **Discussions**: Facilitates interactive communication among students and instructors through discussion forums.
- **Modules**: Allows for the organisation of course content by weeks, units, or other structures, creating a linear flow of materials.
- **Quizzes**: Enables the creation of quizzes to assess student understanding and track progress.
- **Pages**: Instructors can create content pages to provide information and resources to students.
- **Collaborations**: Supports collaborative learning by allowing students and instructors to create and edit documents together.
- **Conferences**: Offers virtual classroom capabilities with real-time audio, video, and presentation tools.
- **Groups**: Facilitates group work by allowing students to collaborate in smaller subsets within a course.
- **Outcomes and Rubrics**: Instructors can add learning outcomes to rubrics to measure and track student skill development.
- **SpeedGrader**: A tool for providing comprehensive feedback on assignments and quizzes efficiently.
- **Gradebook**: Manages grade reporting and tracking within the course.

[18] Instructure in this sentence mean: End-Users such as faculty employees and account administrators.

- **Peer Reviews**: Encourages student-to-student feedback by allowing peer assessment of assignments.
- **Announcements**: Instructors can communicate course news and updates to students.
- **Calendar and Syllabus**: Helps in organising course schedules and outlines.
- **Inbox**: An internal messaging system for communication between course participants.
- **Analytics**: Provides data insights to inform instructional decisions and track student success.

A.1.2 Architecture

Canvas LMS, as offered by Instructure through its managed cloud service (referred to as "Canvas Cloud"), is architected primarily as a Software-as-a-Service (SaaS) solution hosted on Amazon Web Services (AWS). This includes conforming with AWS' framework, implementation of control plane hardening standards and benchmarks, and continuous workload monitoring.[19]

While the core Canvas LMS application is open source (written in Ruby on Rails and freely available on GitHub[20]) the production-grade version deployed for institutions is augmented with a variety of proprietary microservices, integrations, and infrastructure optimisations designed to meet the scale, reliability, and compliance requirements of educational institutions.

Instructure's 'Canvas LMS Architecture diagram' describes what AWS services are used for Canvas LMS as a SaaS (Software-as-a-service), and it includes: Elastic Compute Clouding (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), and Identity and Access Management (IAM). These features will be elaborated further in Part A.

Instructure points out that the use of AWS services allows it to grow and adapt based on education organisation's demands.

[19] Instructure, "Security | Trust Center" (Instructure) https://www.instructure.com/trust-center/security accessed 24 October 2025.
[20] Instructure, Inc., 'Canvas LMS – Open source repository (instructure/canvas-lms)' (GitHub, accessed 24 October 2025) https://github.com/instructure/canvas-lms.

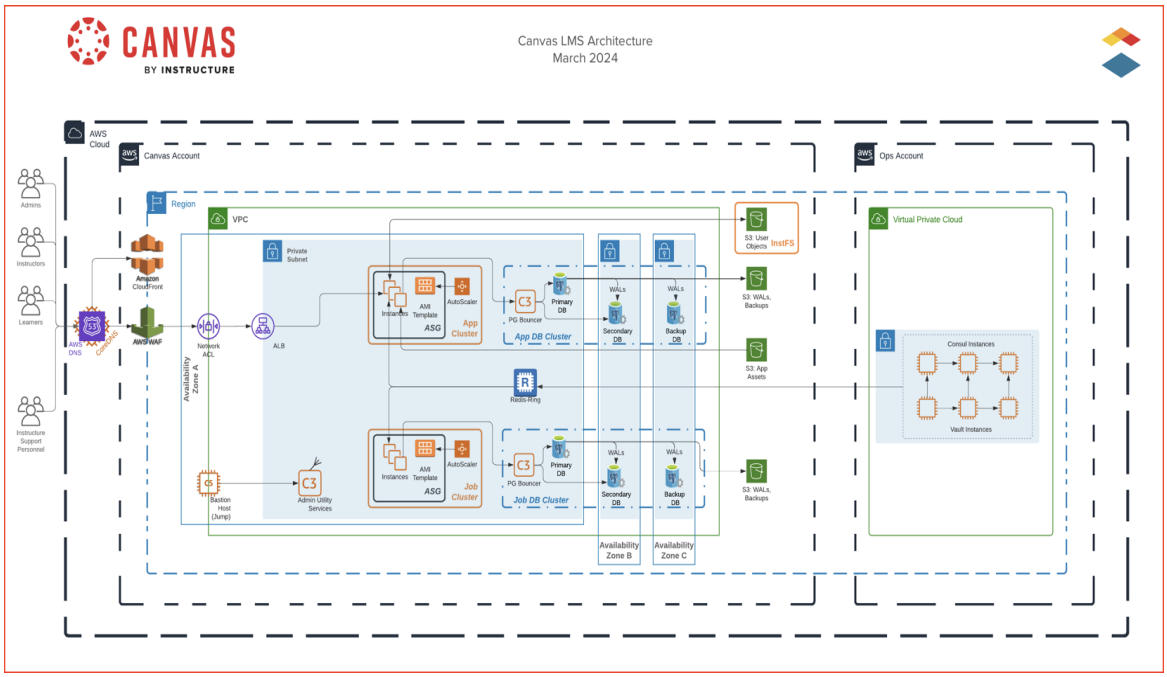

Figure 1 Canvas LMS Architecture diagram

A.1.2.1 Dependencies

At the heart of the system is the main LMS repository. This core application can, in theory, run on any infrastructure, including locally or on alternative cloud providers, and is open source. However, the SaaS production deployment utilised by Instructure's customers is heavily optimised for and dependent on AWS-native services. Several critical components, such as the event logging and analytics back-end, rely on AWS Kinesis, S3, and Lambda to process and store high-volume page view data. These services are not easily portable and reflect a deep coupling to AWS-specific tooling.

Instructure offers several integration options within Canvas LMS to alleviate some of these dependencies. For instance, storage within Canvas LMS is flexible. The platform supports multiple file storage backends, including traditional local storage with NFS (Network File System) mounts, S3-compatible APIs, and a proprietary service known as InstFS[21], which adds Canvas-specific functionality on top of AWS S3. However, while the base LMS could, theoretically, operate without these services, the cloud deployment model bundles them for scalability and performance.

A.1.2.2 Multi-Tenancy and Sharding

Multi-tenancy is central to Canvas Cloud's architecture. Each institution operates within what is termed a "root account," and these are logically segregated into database shards. Instructure explains in their documentation that sharding is when tenants are separated in AWS via logical separation in natively multi-tenant software.[22] It is a form of horizontal partitioning where data is divided by rows, typically by customer, rather than columns. This approach improves performance by reducing table size and index load. Each shard is isolated, preventing data leakage or cross-access between customers. Authentication

[21] Canvas LMS (GitHub, lib/inst_fs.rb) https://github.com/instructure/canvas-lms/blob/master/lib/inst_fs.rb accessed 24 October 2025.
[22] Instructure, Canvas LMS Architecture overview (2025), page 5.

occurs before shard assignment, and credentials are valid only for a specific shard. The integrity of this segregation is regularly verified through weekly disaster recovery tests.

The sharding itself is implemented via open-source extensions within the core Canvas code, making it possible to allocate different institutions to different database servers, with routing information stored centrally.

A web request is intercepted by the application, which determines the correct database shard and region using a domain-to-shard mapping configuration. From the customer's perspective, each instance appears as part of a single unified Canvas environment. Internally, however, routing is dynamic and region-specific.

A.1.2.3 Predictive Scaling

Scalability of the platform is handled through a mix of predictive and reactive mechanisms. Instructure has built custom predictive scaling tools (called HotTub) that anticipate usage spikes (particularly around known peak periods like semester starts) and scale up resources minutes before the anticipated surge. This system leverages historical data, projected growth, and class schedules to inform scaling actions. Post-peak, standard AWS autoscaling mechanisms take over, using a mix of CPU utilisation and custom metrics such as queued requests and background jobs to maintain optimal performance.

Instructure describes (the benefits of) HotTub as:[20]

"*HotTub is a reactive autoscaling mechanism specifically for Canvas that can scale up our application clusters in response to unexpected jumps in user activity up to 20 times faster than Amazon's own autoscaling service. Since we can look back to previous days or weeks and predict what resources will be needed ahead of time, our HotTub scaler can have a pool of pre-warmed application servers that are ready to be put into service at a moment's notice. Between both these services, Canvas provides unmatched stability and scalability regardless of user load.*"

A.2 Contractual Framework

This section will outline legal documentation between Instructure and educational institutions. SURF will further analyse general legal documents such as Instructure's Master Terms and Conditions, General Terms of Use, Privacy Policy, and Cookie Policy.

A.2.1 SURF and Instructure

At this moment, there is no contractual relationship between Instructure and SURF. According to the minutes of a meeting ('MOM') held with Instructure's representative for the Benelux region, all contractual agreements for the use of Instructure's services are established directly by individual educational institutions in the Netherlands through their own tendering processes.[23]

Furthermore, any previous framework agreements that may have existed have since expired, reinforcing the current decentralised procurement approach whereby institutions independently manage their contracts with Instructure. The purpose of this engagement is to facilitate the development of a centralised or umbrella DPIA that can be used by all institutions, supporting a consistent approach in privacy and DPAs towards Instructure within the education sector in the Netherlands.

A.2.1.1 Data Processing Agreement with the University and HBOs (Higher professional education)

Since Instructure does not have a contractual agreement with SURF, the first DPA analysed here and used as a reference is the document shared with SURF by one of our education institutions (higher education institutions such as universities and HBOs[24]).[25] This agreement was concluded directly between the Education institution as the Controller, and Instructure as the Processor.

The specifications for the processing of personal data are outlined in the Annex, which is organized into distinct categories. Certain details regarding the processing must be completed within the Annex, either by the Controller or the Processor, depending on their respective responsibilities. Here, it may be observed that Instructure as the processor fills in the details for the description of the processing. Since Instructure is the product owner of Canvas LMS system, the description that it provides describes in the most detailed way about the description of the processing that should be completed on behalf of the controller. According to the DPA, Instructure's processing are:

'*Processing the Controller's Personal Data on behalf of and in accordance with Controller's documented instructions for the following purposes:*

(i) Processing in accordance with the Agreement;
(ii) Processing initiated by Data Subjects as required under EU Data Protection Law; And
(iii) Processing to comply with other documented, reasonable instructions provided by Controller where such instructions are consistent with the terms of the Agreement.'

[23] MOM from the meeting with Instructure from the 26th June 2024.

[24] 'HBO' refers to higher professional education (Hoger Beroepsonderwijs), which is a type of university education focused on practical skills and career preparation through hands-on learning, internships, and projects.

[25] Data Processing Agreement with an educational institution (University).

The way the purposes are currently stated allows for a broad interpretation of data processing activities and provides a basis for conducting a compatibility assessment to determine whether future processing purposes align with the original ones.

According to the Agreement, the main purpose of the processing established by the Controller is 'support of education and education processes'.[26] The stated purpose is quite broad, as it allows virtually any activity related to processing to be interpreted as supporting education. As a result, this ambiguity makes it difficult to clearly distinguish the responsibilities and roles of the Data Controller and Processor, potentially leading to overlaps or confusion in accountability.

Regarding the categories of data subjects and the risk class estimation, special categories of personal data may be processed. The categories of data subjects are included: students and employees. The categories of personal data: 'Name and contact information, job title and institution (for employees) IP addresses, study materials and results, special examination arrangements (based on health), user data and telemetric.

Special examination arrangements, including health-related information, are not included in the Privacy Data Sheet. However, since they are regulated under this DPA, this suggests a gap in documentation that may lead to a lack of transparency or clarity regarding the handling of sensitive personal data.

Retention period of the personal data is determined by the Controller according to the institution's DPA. The period determined by the Controller is 12 months upon deletion by Controller data is permanently deleted from Instructure's backups as mentioned in Annex A.

Additionally, the DPA outlines the categories of employees acting on behalf of the processor who handle personal data, providing detailed information on those involved in processing the institutions' data. The list of the employees:

1) Customer support services;
2) Engineering services;
3) Customer success services;
4) Security services.

It is important to mention that in the description of the type of processing, customer support services processing is hosted in the USA. Specifically, Instructure's user support ticketing system and user helpdesk support and technical operations support. '*Any Customer Personal Data submitted through a support ticket is stored and processed in the USA'*.

[26] Data Processing Agreement with an educational institution (University), page 11.

A.2.1.2 Data Processing Agreement (DPA) with an MBO institution

For the comparison purposes, it will be a valuable addition to the DPIA to analyse the DPA that Instructure concluded with an MBO[27] institutions.[28] This agreement is an Annex and pertains to the Privacy Covenant for Digital Educational Resources ('the Privacy Covenant'). The provisions of the referenced DPA are consistent with the provisions of the Privacy Covenant.[29] This model agreement contains all legal requirements that apply to education institutions and suppliers according to the GDPR.[30] This DPA with an MBO institution was directly coordinated together with Instructure where the latter adjusted the deployment support in the USA.[31]

This Agreement shares the division between the roles of the subjects to this agreement. According to Articles 2 and 3 DPA, an Educational Institution acts as the Data Controller with respect to the processing of Personal Data carried out on its behalf. It retains full and independent authority over the determination of the purposes and means of such processing.[32] This role attribution corresponds to the responsibility of the controller mentioned in Article 24 GDPR.

Instructure, in the role of the Processor, ensures that the Education institution is adequately informed about the services provided by the Processor.[33] Additionally, Instructure shall provide a description of the specific products and/or services offered, along with details of the associated personal data processing, indicating whether such processing is necessary for the provision of the services or optional.[34]

Both parties shall ensure appropriate technical and organisational measures to secure and protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction or damage.[35]

The specific purposes that education institutions permits to process personal data are mentioned in Appendix 1 to the DPA and Privacy Covenant:[36]

1. Storing learning outcomes and test results;
2. Returning learning outcomes and test results to the Educational institutions;
3. Assessing learning outcomes and test results to be able to obtain course and test materials;
4. Analysing and interpreting learning outcomes and test results;
5. Exchanging learning outcomes and test results between Digital Educational Resources;

---

[27] MBO institution: secondary vocational training: Government of the Netherlands, 'Secondary vocational education (MBO)' (Government.nl) https://www.government.nl/topics/secondary-vocational-education-mbo-and-tertiary-higher-education/secondary-vocational-education-mbo accessed 24 October 2025.
[28] Data Processing Agreement ('MBO institute'- Canvas Learning Management Services) model 4.0, Privacy Covenant 2022.
[29] Ibid; Privacyconvenant Onderwijs, 'Convenant digitale onderwijsmiddelen en privacy' (Privacyconvenant.nl) https://www.privacyconvenant.nl/ accessed 24 October 2025.
[30] Privacyconvenant Onderwijs, 'Veelgestelde vragen' (Privacyconvenant.nl) https://www.privacyconvenant.nl/veelgestelde-vragen/ accessed on 24 October 2025.
[31] Ibid, page 1.
[32] ibid, Articles 2 and 3.
[33] Article 3 MBO DPA.
[34] Appendix 1 to the DPA.
[35] Article 7 Security and Control DPA.
[36] Appendix 1, Section E.

6. Supervising and supporting teachers and other staff within the Educational Institution;
7. Communicating with Education Participants and parents and with employees of the Education Institution;
8. Being provided with/able to use Digital Educational resources in accordance with the agreements made between the educational institution and the supplier;
9. Obtaining access to the Digital Educational Resources offered, and external information systems, including identification, authentication and authorisation;
10. the continuity, improvement, proper functioning of the Digital Teaching Device on the instruction of the Educational Institution in accordance with the agreements made between the Educational Institution and the Supplier, including having maintenance carried out, making a back-up, making improvements inter alia after errors or inaccuracies have been detected, and receiving support;
11. making Personal Data available to the extent necessary to comply with legal requirements for Digital Educational Resources;
12. handling of disputes;
13. financial management;
14. the implementation or application of a provision or regulation of Union or Member State law.

The purposes of personal data processing mentioned above are specifications by the Education Institution, as a controller, and Instructure, as a processor. Accordingly, this Education Institution acting as a Data Controller, clearly defined and limited purposes for which personal data may be processed. It corresponds to Instructure stating that the Customer is the controller and it chooses the type of the service and initiates the data processing and determines the purposes of using products and services such as Canvas LMS.[37]

To summarise this description about the MBO education institution's DPA, SURF observed that there is a clear delineation from the legal perspective. It ensures that the institution maintains control over how personal data is used within services of Canvas LMS and affirms the institution's authority over its data processing activities, content data, and metadata.

A.2.1.3 Data Processing Agreement (Instructure Vendor Data Processing Agreement)
This DPA regulates the relationship between Instructure and its Vendors. Vendors are subprocessors. They are third-party service providers or entities that process personal data on behalf of a primary data processor. They help perform specific tasks related to data processing under the instructions of the main processor (Instructure). In Clause 2.1 of this DPA, Instructure confirms the roles of the parties, where[38]:

- Instructure's Customer is the Controller;
- Instructure is a processor;
- Vendor is a processor.

Instructure recognises that '*Vendor shall only process Personal Data to the extent necessary to perform the services as specified in the agreement and this DPA and only in*

[37] Canvas LMS Privacy Data Sheet (2024).
[38] Instructure Vendor Data Processing Agreement (V.2024.09.01), page 3.

accordance with Instructure's or the Controller's (or as communicated by Instructure on behalf of the Controller) written instructions."[39]

Additionally, it is essential to emphasise that the obligations imposed on subprocessors arise directly from the provisions of this DPA. These obligations include the implementation of appropriate technical and organisational measures, which must be at least equivalent to those outlined in the Instructure's Security Specification.[40] This clause aligns with Article 28(4) of the GDPR, which mandates that subprocessors be subject to the same data protection obligations as those in the contract between the controller and processor. In Schedule 1 of the Instructure's Vendor DPA, the purposes are intentionally left blank because they will vary depending on the specific services performed by this subprocessor. As a result, detailing and distinguishing the roles precisely is challenging.

A.2.1.4 Data Processing Addendum (Global DPA)

This document is called Instructure Global Data Processing Addendum ('Global DPA'). It regulates the Data Processing Agreement between Customer and Instructure if the model of Instructure (as the vendor) is used for the agreement.[41]

Instructure acknowledges that Customer retains all ownership of Customer Personal Data. Same agreement applies here as was stated in the Education Institution's DPA: processing personal data only on behalf of the Customer and only according to the Customer's instructions.

Customer personal data such as SIS (Student Information System) identification number entails metadata. SIS ID might point to or uniquely identify a student's full record in the system such as student's profile, and a reference key to link different pieces of data (grades, attendance, schedules, and other). In this capacity, the SIS ID qualifies as metadata, as it provides contextual information about the underlying personal data without containing the data itself.

According to the Global DPA, the following data is processed presented in Table 1 Personal data processed by Canvas LMS according to the Global DPA below.

Service name	Personal Data Elements
Canvas Learning Management System (including mobile apps)	Application username/ID & hashed password Assessment results (e.g., 86%) Avatar URL (if enabled by the Customer, e.g., URL of Avatar image) Browser locale (e.g., en, browser language setting) Calendar events (e.g., event location) Comments (e.g., discussions, media comments, submissions) Country (e.g., CAN) Course content (e.g., Lesson #4, Syllabus) Course results (e.g., B+)

[39] Instructure Vendor Data Processing Agreement ((V.2024.09.01), page 3.
[40] Instructure Vendor Data Processing Agreement ((V.2024.09.01), page 5.
[41] https://www.instructure.com/policies/data-processing-addendum.

	Email address (e.g., John.Doe@awesomeu) Enrollment status (end-users association with a specific course or section, e.g., Student or Teacher) First and last name IP Address (e.g., 127.0.0.1) Locale (The end-user's locale. This is an optional field and may not be entered by the end-user, e.g., en - language selection) Messages (e.g., notifications and course conversations) Media content created by the user (e.g., images, voice recording, comments) Phone number (if enabled by the customer, for SMS messages) Pronouns (if enabled by the customer, preferred pronouns selected by the end-user, e.g., she/her) Session ID School Name School Position (e.g., Student) Short name (selected by the end-user, e.g., Sam) Student Information System (SIS) Identification Number SIS source ID (ID for the correlated record in the SIS if a SIS integration has been configured) Submitted content (e.g., research paper, assignments) Turnitin ID (unique identifier used by Turnitin) Webconference data (participant ID, particpant comments, user ID. If enabled by the Customer)

Table 2 Personal data processed by Canvas LMS according to the Global DPA

The Global DPA document defines the scope of processing in terms of the personal data involved and specifies the purposes. According to the Section 2 of the Global DPA, Instructure may process and transfer Customer Personal Data and Account Data outside of the Customer's home region as necessary. These are the purposes for which Instructure acts as the Controller:

1. Relationship and Contract Management: includes managing contracts and customer relationships;
2. Customer Support: encompasses end-user helpdesk assistance and technical operations;
3. Professional services: integration, implementation, and configuration based on the Customer's purchases;
4. Engineering and Security Support: involves authorized personnel to review Customer Personal Data contained in support tickets, logs, and security tools to maintain and secure the system.

Instructure takes an obligation to guarantee its Customers that personal data will be processed only according to these purposes. It is important to clearly document these purposes and map it with other Instructure's documentation.

Processing will be lawful if the purposes should be specified, explicit and legitimate to fall within Article 6 of the GDPR. All four Instructure's purposes will be analysed in A.3 and will be assessed whether they comply with the GDPR's legal bases for processing personal data

such as necessary for the performance of the contract; consent; necessary due to a legal obligation, and others.

In the Global DPA**,** prohibited purposes are mentioned.[42] According to the DPA with customers (educational institutions), Instructure:

1. shall not sell Customer Personal Data or share it for targeted advertising, except as expressly instructed by the Customer.
2. Instructure shall not combine Customer Personal Data with other Personal Data, except as permitted under applicable Data Protection Laws.
3. Instructure shall not collect, retain, use, or disclose Customer Personal Data outside of the direct business relationship with the Customer.
4. Instructure shall only process Customer Personal Data for limited and specified purposes that are consistent with this DPA and the Agreement.

The Global DPA purposes and prohibited purposes are not mentioned in the specific DPAs with Educational institutions such as universities and MBO discussed in this DPIA. The purposes mentioned in the institutional DPAs included the purposes according to which Instructure can process the personal data; however, the role was determined to be as a Processor, and not the Controller. The Global DPA mentions specifically the situations when Instructure acts as the Controller and Processor.

A.2.1.5 Instructure's General Legal Documentation

A.2.1.5.1 Master Terms and Conditions

Instructure's Master Terms and Conditions apply to the products or services identified in the Order Form of Instructure.[43] Order Form is defined as any order of products or services executed by the Customer, and it serves as the contractual basis for the provision of those products or services by the Instructure entity specified on the form.

Order Form is defined by the Customer, which is the list of the services that educational institutions order from the service provider. It is mentioned in the provision 1, that Instructure provides a software-as-a-service (SaaS) via a hosted URL, along with any other listed services. Updates and support are included as outlined in the Order Form. A User is anyone authorised by the Customer with a purchased subscription. Furthermore, it is specified in the Provision 3 that Customer shall have sole responsibility for the Customer Content (See Section A.4.2A.4.2and use of the Service in compliance with this Agreement and the Acceptable Use Policy (AUP).

According to this Policy, there are several requirements mentioned for Customers (educational institutions). This paragraph conveys the customer's liability: involves the responsibility for the services offered to the customers by Instructure. They must manage and secure User credentials, ensure user compliance with the Acceptable Use Policy

[42] Instructure, 'Data Processing Addendum' (Instructure) https://www.instructure.com/policies/data-processing-addendum accessed 24 October 2025.
[43] Instructure, 'Master Terms and Conditions' (Instructure) https://www.instructure.com/policies/mastertermsconditions accessed 24 October 2025.

(AUP)[44], prevent and report unauthorised access, provide cooperation for implementation, support, and maintenance, ensure User accounts have up-to-date email addresses, and obtain necessary consents from Users for service provision. Some of the practices are complex to implement since some processing techniques are not accessible to educational institutions. Correspondingly, according to the GDPR, the processor must assist the controller for the fulfilment of its obligation.[45] This will be discussed further in chapter A.6.3.

It is important to mention the term 'Usage Data' in provision 10. This Usage Data will be used only in aggregated form and will not contain any information that identifies, or could reasonably be used to identify, any individual:

'*Customer agrees that statistical and analytical data related to Instructure's provision of the Service or Customer's use and interactions with the Service (e.g., browsing history, inputs, outputs, feedback), and de-identified Customer Content (collectively, '**Usage Data**') is owned by Instructure, and may be used by Instructure for any lawful purpose not otherwise excluded by this Agreement.*'[46]

Instructure uses 'de-identified data', which is not directly a GDPR term. Instructure explained that the term 'de-identified' is used as the legal requirement according to the California's requirement to include information about the -de-identified data in Policy.[47] De-identified means *'information that cannot reasonably identify a particular consumer if the organization, implemented: technical safeguards and business processes that prohibit re-identification and processes to prevent inadvertent release of the de-identified information.'*[48] However, if it is still can be re-linked to an individual with additional information, it is considered personal data according to Article 4 (1) and (5) GDPR.

Therefore, Instructure owns and may use aggregated and de-identified data about how the Customer uses the Service for any lawful purpose, as long as it does not include personally identifiable information from Customers.

A.2.1.5.2 Instructure's General Terms of Use

Instructure's Terms of Use ('ToU') outline the conditions under which users may access and utilise its services, including services such as Canvas LMS.[49] Users (educational institutions) are granted a limited, non-transferable license for personal or educational purposes and are prohibited from selling, sublicensing, reverse engineering, or copying any part of the platform beyond what is explicitly allowed.

---

[44] Acceptable Use Policy (AUP) outlines the rules for using an organization's digital resources Instructure, 'Acceptable Use Policy' (Instructure, 12 August 2025) https://www.instructure.com/policies/acceptable-use accessed 24 October 2025.
[45] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (European Data Protection Board, 7 July 2021) https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf accessed 24 October 2025.
[46] Instructure, 'Master Terms and Conditions' (Instructure) https://www.instructure.com/policies/mastertermsconditions accessed 24 October 2025.
[47] Instructure's answer from the 16th of September 2025.
[48] Jacob Rubinstein, 'A Close-up on De-Identified Data Under the CCPA' (IAPP, 27 August 2019) https://iapp.org/news/a/a-close-up-on-de-identified-data-under-the-ccpa accessed 24 October 2025.
[49] Instructure, 'Terms of Use' (Instructure, 8 December 2015) https://www.instructure.com/policies/terms-of-use accessed 24 October 2025.

Users must provide accurate registration details and are responsible for maintaining the confidentiality of their accounts. Unauthorised account sharing, false identity creation, or failure to report breaches is prohibited. The terms also restrict commercial exploitation of the platform, automated data extraction, and any modification or removal of proprietary information. Instructure may update the Terms of Use at its discretion, with material changes communicated to users and taking effect 30 days after posting. Continued use of the services signifies acceptance of any such changes.

Section 5 of the ToU addresses the submission of Feedback. This includes ideas, suggestions, documents, or proposals to Instructure through their platforms such as suggestion boxes, forums, or wikis. It states that users submit such Feedback at their own risk and that Instructure has no obligations of confidentiality regarding this Feedback. More information about the Feedback functionality is discussed in the Section Feedback functionality.

A.3 Data Processing Purposes

This chapter is about the purposes that Instructure processes users' personal data for. Listing these purposes will give a general idea of what the product is used for.

A.3.1 HORA Purposes as determined by Institutions

In addition to these purposes as described by Instructure, the purposes described below are based on the questionnaires to SURF's member institutions as described in the scope, descriptions of the different Canvas LMS modules and the research into the actual processing operations. They are divided into purposes based on the functions described in the 'Higher education reference architecture' model (HORA)[50] and other purposes.

The HORA is a business function model for educational institutions. It describes the functions of an organisation, independently of how these functions are implemented in a specific organisation. Since the HORA describes the essential functions of educational institutions on a high level, it is a good model to derive the main purposes for data processing in applications like Canvas LMS from. Using the HORA as a reference also ensures that it will be easy for institutions to find the right place in their organisational structure to implement any measures or changes from this DPIA.

There is another reference architecture for the MBO sector that provides the insights into the processes, applications and information objects anf their mutual relationships. SURF used HORA instead of MORA because HORA is more broadly applicable in the education sector.

Table 2 shows the HORA business processes which are fulfilled with the Canvas LMS solution. Note that the HORA model is only available in Dutch. As such, the functions within the table are Dutch as well. We did translate the descriptions of the functions for your convenience.

[50] SURF, 'Bedrijfsfunctiemodel (detail)' (HORA2 wiki) https://hora.surf.nl/index.php/Bedrijfsfunctiemodel_(detail) accessed 24 October 2025. (in Dutch only).

Purpose	Function	Description
Communicatie-management	Interne communicatie	Providing information to participants and employees.
Deelnemer-begeleiding	Studieloopbaan-begeleiding	Helping participants in their development process and monitoring their study progress.
Human Resource Management	Medewerker-ontwikkeling	Explicitly developing employees' knowledge and skills, including related guidance.
Informatie-doorlevering	Ontsluiting digitaal materiaal	Making electronic books and journals available.
Onderwijs-ontwikkeling	Onderwijseenheid-ontwikkeling	The (re)development, adaptation and dissolution of an individual unit of study, including the work format(s) and associated learning and testing materials.
Onderwijs-ontwikkeling	Onderwijsmateriaal-ontsluiting	Making teaching materials available both inside and outside the institution.
Onderwijs-ontwikkeling	Opleidings-ontwikkeling	The (re)development, modification and discontinuation of a programme or minor, including the associated competence profile and examination programme.
Onderwijs-uitvoering	Onderwijsuitvoerings-begeleiding	Guiding the implementation of the work form.
Onderwijs-uitvoering	Toepassing didactische werkvorm	Applying and implementing the chosen didactic working form.
Onderwijs-uitvoering	Toepassing leermaterialen	Using, adding, modifying and publishing learning materials.
Onderwijs-uitvoering	Voorbereiding onderwijsuitvoering	Organising teaching implementation, such as putting together groups for the purpose of jointly carrying out learning activities, orienting participants/teacher, processing exceptions, implementing changes. Sharing overview, insight and composition of the teaching unit (consists of one or more work forms).
Onderwijs-uitvoering	Voortgangsbewaking	Monitoring progress of the participant during the performance of the unit of study.
Toetsing	Toetsbeoordeling	Determining the result of a summative test or work product prepared by a participant (e.g. in the context of a project, internship or graduation assignment), making a judgement on it and recording and establishing it.

Toetsing	Toetsuitvoering	The examination of the participant's knowledge, understanding and skills using the result to determine whether an examination programme has been met.
Toetsing	Toetsvoorbereiding	Preparing the test activities.
Toetsing	Vaststelling verworven competenties	Identifying the competences acquired by the participant at a given point in time.

Table 3 HORA business processes fulfilled with Canvas LMS

A.3.2 Supporting Purposes as determined by Institutions

In the agreements between Instructure and education institutions such as DPA with universities, MBO, Global DPA, Instructure confirms that their role is a Processor, and Controllers are educational institutions for the purposes that education institutions decide. In the section A.1.3.2., the purposes that were agreed between Dutch educational institutions[51] and Instructure were directly mentioned in the DPA. This allows to limit the scope and data processing accordingly.

Institutions use Canvas LMS for the purposes described in the previous Section 'Data Processing Agreement (DPA) with Education.' To ensure that Canvas LMS functions effectively, efficiently and safely, Canvas LMS processes personal data for the following purposes and acts as a controller. Processing activities for these purposes are common for IT services, and are referred in the section Instructure's Purposes as a Controller.

Additional to these purposes, Instructure acts as a Controller. They serve Instructure's own purposes where Instructure determines the means of processing.[52] The purposes are linked to Instructure's focus on providing the value to educators and students through:[53]

1) Core teaching and learning experiences;
2) Data and analytics solutions;
3) Lifelong learning opportunities;
4) To ensure a seamless experience for all with the Instructure learning platform.

A.3.3 Instructure's Purposes as a Controller

Purpose	Sub purpose
To manage Customer's business accounts	Marketing, billing, communications services
	To manage Customer correspondence (e.g. communications about updates to the Canvas LMS).

[51] From the DPA with an MBO institution.
[52] Instructure Inc - Privacy Data Sheet for Canvas Learning Management System – April 23, 2024, page 4.
[53] Instructure ESG FY2023 (page 38).

To request feedback from Customers and End-Users regarding Canvas LMS	Customer satisfaction surveys, surveys about support received, requests for product feedback.
Complying and resolving legal obligations	Such as responding to Data Subject requests for Personal Data processed by Instructure as a Controller.
	Fiscal requirements, agreements, and disputes.
Customer Support Services	To provide Customers and End-Users with support upon request.
	Includes the applied knowledge gained from individual Customer support requests.
	Instructure processes anonymised and aggregated data (to improve and optimise the performance and core functionality of accessibility, privacy, security, and the IT infrastructure efficiencies of Canvas LMS).
Abuse detection, prevention and protection	Virus scanning and scanning to detect violations of terms of services (such as copyright infringement, SPAM, and actions not permitted under Instructure's Acceptable Use Policy).

Table 4 Instructure's data processing purposes

A.4 Processed Personal Data

According to article 4(1)(a) of the GDPR,

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

To explain privacy risks of data processing operation, it is important to consider what types of data of which groups of data subjects are being processed.

A.4.1 Definitions of the parties' roles and responsibilities

For the clarification of the roles of both educational institutions and Instructure, it is important to clarify the terms mentioned in Article 4 of the GDPR. It contains definitions of the different roles of parties involved in the processing of data: controller, processor, join controllers and sub-processor.

Article 4(7) of the GDPR defines the (joint) controller as:

> *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*

Article 26 of the GDPR stipulates that where two or more data controllers jointly determine the purposes and means of a processing, they are joint controllers. Joint controllers must determine their respective responsibilities for compliance with obligations under the GDPR in a transparent manner, especially towards data subjects, in an arrangement between them. A key requirement is that the processing cannot occur without the involvement of both parties, meaning each party's role in the processing is so closely connected that it is inseparable.[54]

Article 4(8) of the GDPR defines a processor as:

> *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."*

A sub-processor is another processor engaged by a processor that assists in the processing of personal data on behalf of a data controller.

[54] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (European Data Protection Board, 7 July 2021) https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf accessed 24 October 2025 , page 3.

The GDPR stipulates in Article 4(8) that a processor may only process data on behalf of a data controller. *'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*.

Article 28 of the GDPR outlines several responsibilities that processors have toward the controllers on whose behalf they handle personal data. Specifically, Article 28(3) details obligations requiring processors to process personal data only according to the documented instructions of the controller and to cooperate with audits conducted by the controller. Furthermore, Article 28(4) permits processors to engage sub-processors to carry out certain tasks on behalf of the controller, but only with the controller's prior authorisation.

When data protection roles are assessed, the formal contractual division of roles is not leading nor decisive. The actual role of a party must primarily be determined on the basis of factual circumstances.

A.4.2 Categories of Personal Data

The information that Instructure collects from users depends on the used website, application, or service. In its DSAR response, Instructure details all the potential types of personal data that Canvas LMS collects and processes about its users.[55] This list is also available in Instructure's Privacy Policy and Cookie's statement.

Instructure uses several categories of personal data:[56]

- **Customer Data**: Customers and End-Users upload Customer Content in Canvas LMS to facilitate teaching and learning. Customer Content can include information such as lesson plans, course materials, assessments, teaching videos, rubrics, pictures, learning materials, surveys, audio files, video files, learning assignments, etc. Instructure claims that Customer data is retained as full ownership of all Customer Data.
- **User Data**: End user data. From the Privacy Data Sheet, the definition is the information provided by a Customer (End-User) through the use of Canvas LMS. The list of personal data that exactly falls under user data is mentioned in Table 4 List of Personal Data.[57]
- **Functional Data:** Functional data is processed temporarily to enable specific system functions and is immediately deleted or anonymised after transmission. Unlike diagnostic data, functional data is used solely for essential functions, such as enabling user interactions or specific features. Recital 22 and Article 6(1) of the ePrivacy Directive emphasise that this data, often collected without user consent, must be limited strictly to what is necessary and promptly removed or anonymized to maintain privacy and reduce unnecessary data retention.
- **Diagnostic Data**: Diagnostic data includes information gathered to troubleshoot, maintain, and optimize system performance. While this data may include usage patterns, error reports, and system health indicators, it should ideally avoid including personal data. If diagnostic data can identify individuals, it is subject to GDPR requirements. In these cases, data controllers must inform users about this

[55] For more information on the DSAR response see A.4.3Data Subject Access Requests.
[56] Email response from Instructure to SURF's questions (April 17th, 2025).
[57] Instructure Inc - Privacy Data Sheet for Canvas Learning Management System – April 23, 2024.

processing and ensure data security measures are in place to prevent unauthorised access, as per Articles 32 and 33 of the GDPR.

- **Support Data**: Support data is information collected during customer support interactions. This data may include communications between users and support teams, error descriptions, and other troubleshooting information. GDPR compliance for support data requires that users be informed about the types of data collected and how it will be used, aligning with transparency obligations under Articles 12–14. Additionally, Article 28 GDPR obliges data processors to follow strict confidentiality and data protection agreements when accessing support data.
- **Institutional Data**: Business information about the Customer and its settings within Canvas LMS
    - Name (e.g., Awesome University)
    - Institution address (e.g., 100 Awesome Drive, City, State, Country)
    - School Canvas LMS URL (e.g., canvas.awesome-university.com)
    - SIS integration types (e.g., Kimono, Clever)
    - Time zone (e.g., Mountain Time)
    - Canvas LMS settings (e.g., Allow Avatars)
    - Other settings (e.g., Institution-specific settings)
    - Courses (e.g., Programming in Java)
    - Assignments (e.g., Complete chapter 5 review questions for Math 103)
    - Assessments (e.g., Math 103 quiz questions)
    - Institution Wiki (e.g., Information Content on Programming in Java)
    - Institution administrator (e.g., Jane Doe the Admin)
    - Calendar (e.g., Course Events)
    - LTI tools (e.g., Awesome University's LTI tool)

Below you will find Table 4, where you can see the list of personal data that Instructure processes on behalf of the customers as a Processor for the purposes mentioned in the section Table 3 HORA business processes fulfilled with Canvas LMS Supporting Purposes as determined by Institutions, and Instructure acting as a Controller. The types of personal data are normal and sensitive data. Section A.4.3.1 explains the difference between different definitions of personal data.

Personal Data	Data Categories	Personal Data Category	Personal Data Sensitivity	Purposes
Full name (e.g. John Doe)	End-user data (students)	Directly Identifiable Data	Normal	**Controller**: With respect to processing personal data for customer or end-user support.
	End-user data (observers)	Directly Identifiable Data	Normal	
	End-user data (faculty)	Directly Identifiable Data	Normal	**Controller:** Processing account data – performing the

	End-user data (account administrators)	Directly Identifiable Data	Normal	contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations.
User account (username and password)	End-user data (students)	Directly Identifiable Data	Normal	**Controller**: With respect to processing personal data for customer or end-user support.
	End-user data (observers)	Directly Identifiable Data	Normal	
	End-user data (faculty)	Directly Identifiable Data	Normal	**Controller:** Processing account data – performing the contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations.
	End-user data (account administrators)	Directly Identifiable Data	Normal	
Biographical information	End-user data (students)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
	End-user data (faculty)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
	End-user data (account administrators)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
Canvas User ID	End-user data (students)	Directly Identifiable Data	Normal	**Controller**: With respect to processing personal data for customer or end-user support.
	End-user data (observers)	Directly Identifiable Data	Normal	

	End-user data (faculty)	Directly Identifiable Data	Normal	**Controller:** Processing account data – performing the contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations. Processing for customer or end-user support.
	End-user data (account administrators)	Directly Identifiable Data	Normal	
Short Name	End-user data (students)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
	End-user data (observers)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
	End-user data (faculty)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
	End-user data (account administrators)	Directly Identifiable Data	Normal	Processor: To perform instruction explicitly authorised by the Customer in the customer agreement.
Email address	End-user data (students)	Directly Identifiable Data	Normal	**Controller**: With respect to processing personal data for customer or end-user support.
	End-user data (observers)	Directly Identifiable Data	Normal	
	End-user data (faculty)	Directly Identifiable Data	Normal	**Controller:** Processing account data – performing the contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations.
	End-user data (account administrators)	Directly Identifiable Data	Normal	

				With respect to processing personal data for customer or end-user support.
School position (e.g. student)	End-user data (students)	Organisational Data	Normal	**Controller:** Processing account data – performing the contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations. With respect to processing personal data for customer or end-user support.
	End-user data (faculty)	Organisational Data	Normal	
	End-user data (account administrators)	Organisational Data	Normal	
Avatar URL (e.g. URL of Avatar image) Instructure mentioned that this field is optional. It can be turned off. Avatar can fall into a special category if it reveals protected characteristics such as ethnicity, gender, and others.	End-user data (students)	Normal/Racial/Ethnic Data	Normal/Special	**Controller:** Processing account data – performing the contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations. With respect to processing personal data for customer or end-user support.
	End-user data (observers)	Normal/Racial and Ethnic Data	Normal/Special	
	End-user data (faculty)	Normal/Racial and/or Ethnic Data	Normal/Special	
	End-user data (account administrators)	Normal/Racial and/or Ethnic Data	Normal/Special	
Pronouns	End-user data (students)	Indirectly identifiable	Special	Only for the purpose of processing personal data for customer or end-user support.
Country code (if linked to IP address)	End-user data (students)	Location dta	Normal	**Controller:** Processing account data – performing the

	End-user data (faculty)	Location Data	Normal	contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations. With respect to processing personal data for customer or end-user support.
	Administrator	Location Data	Normal	
Submitted content (research paper, assignments)	Students	Indirectly Identifiable Data	Sensitive	Processor: To perform instructions explicitly authorised by the Customer in the customer agreement.
	Faculty and account administrators	Indirectly Identifiable Data	Sensitive	
Analytics information (e.g. click patterns, logging information)	Students	Behavioural Data	Sensitive	
	Observers	Behavioural Data	Sensitive	
	Faculty and account administrators	Behavioural Data	Sensitive	
Associated learner account	Observers	Directly Identifiable Data	Normal	
Assessment, course, and assignment results	Students	Indirectly Identifiable Data	Sensitive	
Student specific assessment, course, and assignment results	Faculty and account administrators	Indirectly Identifiable Data	sensitive	
Discussion comments	Students	Indirectly identifiable data	Normal	
	Faculty and account administrators	Indirectly identifiable data	Normal	

IP Address	Students	Location Data, indirectly identifiable data	Normal	**Controller:** Processing account data – performing the contract such as billing and communication with customers. And, for internal bookkeeping and fulfilling other legal obligations. With respect to processing personal data for customer or end-user support.
	Faculty and account administrators	Location Data, indirectly identifiable	Normal	
Course enrolments	Students	Organisational Data	Normal	
Course taught	Faculty and account administrators	Organisational Data	Normal	
Messages (e.g. notifications and course conversations)	*Students*	Behavioural Data	Normal	
	Faculty and account administrators	Behavioural Data	Normal	
Video Content created by the end-user (images, voice recording, comments)	Students	Directly Identifiable Data	Normal/Special	
	Faculty and account administrators	Directly Identifiable Data	Normal/Special	
Institution administrator (e.g. Jane Doe the Admin)	Institutional Data	Directly Identifiable Data	Normal	
Assignments (e.g. Complete chapter 5 review questions for Math 103)	Institutional Data	Directly Identifiable Data	Normal	
Assessments (e.g. Math 103 quiz questions)	Institutional Data	Directly Identifiable Data	Normal	
Name	Support Data	Directly Identifiable Data	Normal	Constroller: Processing of personal data for

Email address	Support Data	Directly Identifiable Data	Normal	customer or end-user support.
Customer contact instructions (e.g. 'Also contact)	Support Data	Organisational Data	Normal	
Billing instructions (e.g. accounting@university)	Support Data	Organisational Data	Normal	
Support chat messages (please rest my passwords)	Support Data	Indirectly identifiable data	Normal	
Support phone call voice recording	Support Data	Directly identifiable data	Special	
Files exchanged during a support chat session	Support Data	Communication Data	Normal	
Log, Diagnostic, and analytic data	Log, Diagnostic, and Analytic Data	Technical Data	Normal	**Controller**: Product improvement, engineering operations, and data security (the respective personal data is de-identified before the product improvmenet analysis).
Customer and end-user content	Customer Content Data	Directly Identifiable Data	Special	Processor: to provide and update the Canvas LMS as purchased, configured, and used by customers and end-users.
Full name	Feedback Data	Directly Identifiable Data	Normal	Controller: To request feedback from Customers and end-users regarding Canvas LMS.
Email address	Feedback Data	Directly Identifiable Data	Normal	
Survey responses	Feedback Data	Communication Data	Normal *(If no special categories of personal data are provided*	

			in the survey responses)	
Canvas LMS role	Feedback Data	Contact Information	Normal	
Job title	Feedback Data	Organisational Data	Normal	

Table 5 List of Personal Data

A.4.2.1 Data definitions

Special categories of personal data are especially protected by the GDPR. According to Article 9 (1) of the GDPR, personal information falling into special categories of data is any:

> "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*"

Instructure in LMS can process several types of special category data through user generated content. As was mentioned in the Table 4 List of Personal Data, it has been marked yellow, Instructure may process student's content, voice recordings, video recordings, which can show racial or ethnic origin, political opinions, religious or philosophical beliefs, and others.

In the Table 5 List of Personal Data, SURF mentions 'sensitive' data in addition to special categories of data. It is not formally defined term in the GDPR, but it is often used to describe data that poses higher privacy risks. It can include special category data, but it might also refer to: financial data; location data; communication metadata, and children's data.[58]

The Privacy Data Sheet states that Instructure processes biographic data from end users; however, this information is not reflected in the Global Data Processing Agreement (DPA).[59] In the meeting with Instructure, they explained that biographic information includes the phone numbers, etc, and not special categories of data.[60] Furthermore, Instructure will review the documentation and no longer use the biographic data in the next versions of privacy and security documentations. This analysis will be further provided in next sections.

A.4.3 Data Subject Access Requests

This section is divided into 3 sections: the importance of the DSAR, how it is incorporated in Instructure's documentation and the results of the DSARs we conducted.

[58] Information Commissioner's Office, 'Examples of processing "likely to result in high risk"' (ICO) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/ accessed 24 October 2025.
[59] Instructure, Inc. – Privacy Data Sheet for Canvas Learning Management System, April 23, 2024.
[60] MOM dated 23rd June 'Canvas LMS Part A review with Instructure'.

A.4.3.1 The importance of the Data Subject Access Rights (DSAR)

In accordance with the rights afforded to individuals under the GDPR, data subjects have the right to request access to their personal data. According to Articles 12–22, with Article 15 GDPR specifically covering data subject access requests, organisations must be prepared to handle these requests lawfully, promptly, and transparently.

This includes the right to obtain confirmation as to whether their data is being processed, access to the data itself, and information regarding the purposes of processing, categories of data concerned, recipients, and retention periods. To assess the organisation's procedures for fulfilling these obligations, a Data Subject Access Request (DSAR) was submitted as part of this DPIA. The following section outlines the findings from that request and evaluates the adequacy and responsiveness of the organisation's current practices in relation to data subject rights.

A.4.3.2 Incorporation of Data Subjects' Rights in Instructure's documentation

Access Rights are incorporated in the various legal documents.

Instructure's DPA includes a provision stating that, to the extent the Customer is unable to take certain actions required under applicable Data Protection Laws, such as (a) fulfilling Data Subject Requests or (b) implementing appropriate security measures to protect Customer Personal Data, Instructure will make commercially reasonable efforts to assist. This assistance will be provided in response to reasonable Customer requests, to the extent required by Data Protection Laws, legally permissible for Instructure, and taking into account the nature of the processing and the information available to Instructure.[61]

The Product Privacy policy mentions a reference to the right to access the personal data that Instructure maintains, and in some cases, have choices to limit the use and disclosure of personal data.[62]

It is worth mentioning that Instructure continues to develop the DSAR mechanisms which will create a self-service for end-users data exports in Canvas in accordance with GDPR regulations. It means that Instructure develops more tools for the controllers to fulfil their obligations. This will be taken into account when reviewing the results to the DSR requests submitted by SURF.[63]

A.4.3.3 DSAR Responses

SURF executes DSARs as part of technical testing on vendor's systems to evaluate the quality and speed of their responses. For instance, we check whether the DSARs contain all the information we put into the system, including logs and any other information that Instructure might hold about our data subjects. DSARs are executed after completing the testing scenarios. Please also refer to Appendix 1 for more information about these testing scenarios.

---

[61] Instructure, 'Data Processing Addendum' (Instructure) https://www.instructure.com/policies/data-processing-addendum accessed 24 October 2025.
[62] Instructure, 'Product Privacy Policy' (Instructure) https://www.instructure.com/policies/product-privacy-policy accessed 24 October 2025.
[63] As was presented to SURF in the Instructure's confidential release: Data Privacy upcoming releases (presentation).

The fictional data subjects, including an instructor and two students, as well as an IT Administrator, requested access to their personal data held by Instructure within our Canvas demo environment. The formal DSAR requests were emailed to Instructure on May 12th, 2025. We received Instructure's responses within 17 days on May 29th, 2025.

The requests aimed to obtain:

- A copy of all data traceable to the individual, including data stored in Canvas, log files, audit logs, user interactions, and technical error reports.
- The purposes for which their data is being processed.
- The categories of personal data concerned.
- The recipients or categories of recipients to whom the personal data has been or will be disclosed, particularly those in third countries or international organisations.
- If possible, the period for which personal data is expected to be stored or the criteria for determining that period.
- Information about the source of the data (if not collected directly from them).
- Options available to rectify or erase personal data, to object to its processing, and the procedures to follow.
- The existence of automated decision-making, including profiling (referred to in Article 22(1) and (4) GDPR), along with useful information on the underlying logic, significance, and expected consequences for the data subject.

A.4.3.3.1 Included data from DSAR responses

The DSAR responses provided a comprehensive overview of various data types, such as user interactions, enrolments, logins, and file attachments/exports, presented in a tabular format, with each table appearing in its own sheet. The system successfully captures that certain actions (e.g., submissions, quiz attempts, discussion replies, conference participation) occurred, and often links them to specific assignments, quizzes, or discussion topics. For each data subject, the report included:

- **Communication Channels**: This table outlines the methods used to communicate with the data subject, such as email.
- **Page Views**: This section lists Canvas pages accessed by the subject and related metadata about the interactions.
- **Asset User Accesses**: This provides aggregated information about resources accessed by the subject, including Pages, Assignments, and Quizzes.
- **Pseudonyms**: This table outlines the subject's methods for logging into Canvas and associated metadata.
- **Attachments**: This section lists files uploaded by the subject to Canvas. Accompanying the document was a folder containing these uploaded files, with a structure attempting to match the Canvas view.
- **Submissions**: This table includes submissions to assignments, including legacy graded quizzes, by the subject.
- **Discussion Entries**: This table lists the subject's discussion entries. For example, the instructor made entries like "Excited!" and "Desk chair" in discussions.
- **Enrolments**: This table details the subject's course and section enrolments.
- **User Metadata**: This provides metadata about the subject, such as name, email, and time zone preferences.

A.4.3.3.2 Missing data from DSAR responses

A notable gap in the DSAR responses is the lack of direct access to the specific textual content of submissions (e.g., the text entered for an assignment or quiz answers), announcements created by instructors, syllabus content, and page content. While the action of creating or modifying this content is recorded in page views (URLs), the content itself is not easily retrievable in a comprehensive, human-readable format directly from the DSAR. Similarly, specific comments made within peer reviews are not detailed.

In particular, the following types of data are not comprehensively available via the DSAR:

- **Textual content entered by users**: This includes assignment submissions, quiz answers, announcements, syllabus entries, and static page content. Although the creation or modification of such content is traceable through system logs or URL references, the content itself is not presented within any dedicated DSAR table or field.
- **Peer review and comment content**: Comments made by students during peer review activities, such as short evaluative remarks, are not surfaced in the structured DSAR data, even when the corresponding participation is logged.
- **Rubric and grading metadata**: Descriptive elements created as part of assignment rubrics are not consistently reflected in the DSARs.
- **Engagement with embedded content**: Interactions such as viewing media files attached to instructor feedback are not clearly itemised, with only broader navigation activity captured (e.g. grades or dashboard views).
- **Support interactions**: Actions such as the creation of help tickets or user support requests are not represented in the DSAR, nor is their content retrievable via any of the standard tables.

Additionally, despite our explicit requests for various other types of information, the following information was not found in their DSAR responses:

- **Purposes for data processing**: The reports did not specify the purposes for which the personal data is being processed.
- **Categories of personal data concerned**: While various data types were provided, a clear, consolidated list of the categories of personal data concerned (e.g., identity data, academic data, usage data) was not explicitly presented.
- **Recipients of data disclosure**: Information regarding the recipients or categories of recipients to whom the personal data have been or will be disclosed, especially concerning third countries or international organisations, was not included.
- **Data storage period/criteria**: The reports did not indicate the period for which the personal data is expected to be stored, nor did they provide the criteria used to determine such storage periods.
- **Source of data (if not collected directly)**: There was no explicit information about the source of the data if it was not collected directly from the data subject.
- **Rectification, Erasure, Objection Options and Procedures**: The reports did not outline the options available to rectify or erase personal data, nor did they provide the necessary procedures to object to its processing.
- **Automated Decision-Making and Profiling**: Information about the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the GDPR, was absent. This also means no details were provided on the underlying logic, significance, or expected consequences of such processing for the

data subject. Instructure does not carry out any form of automated decision-making or profiling.[64]

- **Comprehensive Log Files and Technical Error Reports**: Although 'Page Views' and 'Asset User Accesses' provide detailed user interaction logs, more detailed log files and technical error reports, including system-level logs or specific error logs, were not explicitly provided in the current format.

The gaps in the DSAR response do not provide the same details and specific information that is mentioned in Article 13 and 14 GDPR for purposes, categories of personal data, data storage, and source of data. For example, purposes of the processing should be provided at the time of data collections (if collected from the data subject) or within a reasonable period after obtaining the data.[65]

A.4.3.3.3 Ease of DSARs

An administrator of Canvas LMS has the ability to easily execute DSARs from the admin panel within the user interface of Canvas LMS. They can do this by simply clicking on 'Creating DSR Request for <user>' next to the person's name within the 'People' tab, as seen in Figure 2. From a usability standpoint, this is a commendable implementation that empowers educational institutions to quickly respond to access requests without requiring manual extraction, intervention or human support from Instructure. An export is generated within minutes.

Figure 2 Creating DSAR Request for user

Interestingly, utilising this feature nets the exact same results as the DSAR requests SURF sent by email on May 12th, 2025, and discussed above. If the DSARs SURF received from

[64] Instructure's comment from the 16th of September 2025.
[65] 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 (General Data Protection Regulation) [2016] OJ L119/1., Article 13 (1) (C) and Article 14 (1) C).

Instructure are identical to what can be exported by a Canvas admin with a few clicks, it still took Instructure 17 days to deliver the responses. The technical capability suggests a much shorter response time should have been possible. Second, the contents of the reports align exactly with what is produced by this automated export tool, which seems to indicate that Instructure relied solely on this feature without addressing the broader scope of our DSAR requests. Instructure explained that exporting a DSAR response is a manual process, which is currently being streamlined.[66]

[66] Instructure's feedback from the 16th of September 2025.

A.5 Data Processing Activities

This chapter outlines the types of processing activities that may occur within Canvas LMS. In accordance with Article 4, Paragraph 2 of the GDPR, "processing" is defined as follows:

> "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

The processing activities are described in the DPA between Instructure and Education Institutions in the section A.1.3.2. In the Global DPA that Instructure uses with it customers, additional purposes according to which Instructure acts a controller are mentioned. It is important to bear in mind that the controllers determine the purposes and means. Therefore, the scope of the processing may vary based on the specific requirements of the institutions. The descriptions below go into more detail and are based on the actual processing operations as found in the research for this DPIA.

A.5.1 Customer Support Access

Customer support access to institutional environments within Canvas LMS is facilitated through a centralised internal administrative interface known as Site Admin. This interface is available at *siteadmin.instructure.com*, and is used by Instructure employees to locate and enter any customer environment, referred to as a root account. Each institution typically corresponds to one root account, although for large institutions or performance reasons, an institution may span multiple root accounts or database shards. These shards are logically partitioned but centrally discoverable within the Site Admin tool.

When a support agent or other authorised Instructure employee needs to access an institution's instance, they can browse through a list of all available root accounts. Upon selecting a particular institution, the system resolves the corresponding shard and its associated database configuration (including its geographical region) and routes the request accordingly. From the employee's perspective, this routing process is seamless.

Although there are several internal role-based permissions that gate what level of access a given employee has, ranging from read-only support roles to high-privilege "super admin" roles (of which only a few exist in Instructure), the actual act of entering a customer environment does not include a real-time verification step. Once logged into Site Admin, an employee can directly enter a customer's environment, provided their role grants them the necessary permissions. There is no secondary approval, dual-authentication, or validation by the institution before access is granted.

Instructure has implemented an internal justification prompt that appears when an employee initiates access to an institution's environment. This prompt requests that the employee provide a reason for access, typically a reference to a support case, internal issue ID, or engineering task. This justification is logged for audit purposes, and access is time-limited (generally to 48 hours). However, during our discussions with Instructure it was acknowledged that, at present, this process may be auto approved with no human review

step prior to granting access. The justification mechanism is handled by a separate service that integrates lightly with Canvas, performing logging and time-based access management, but it does not prevent the initial access.

Importantly, this access is not geographically constrained. Support personnel based in the United States are technically able to access environments hosted in the EEA. While encryption keys and customer data remain within the designated AWS region (e.g., Dublin or Frankfurt), the application-layer access is not restricted based on geography. In practical terms, this means that a US-based employee, if authorised, can navigate into an EU-hosted Canvas instance and view or act on personal data, provided they enter a justification (which may be automatically accepted). While this facilitates flexible global support, it raises questions under the GDPR regarding cross-border access to personal data and the adequacy of safeguards.

In the updated risk register, Instructure stated that access to personal data within Canvas by non-EU personnel is strictly limited.[67]

'*Access to Canvas personal data by non-EU personnel is strictly limited. EU Account are assigned to a Customer Experience team based in the EU, ensuring localized oversight and responsiveness.*

We have expanded our operations in Hungary by 144% since 2022, further enhancing our overall presence and capabilities within the EU region.

Where engineering access is necessary, it is tightly controlled, requiring formal approval and documented authorization, in line with our internal security and compliance protocols.

In addition, Instructure has certified to and complies with the EU-U.S. Data Privacy Framework, which remains fully effective. We continue to actively monitor developments that could impact the DPF, and stand ready to implement alternative measures, as we have done in the past, should any changes to the DPF occur.'[68]

A.5.2 Feedback functionality

To gain a clearer understanding of how Instructure handles feedback, additional information was requested regarding the processes Instructure follows for managing user feedback and the confidentiality obligations it observes in this context. To our information request, Instructure provided the following information about the feedback functioning:

'We ask the following questions such as the ones below with a "Yes" or "No" response option.
Was your experience with the product good?
How was your experience with customer service good?
We then have a comment box to elaborate.'[69]

[67] Risk Register Updates, shared with SURF on the 3rd of July.
[68] Risk Register Updates, shared with SURF on the 3rd of July.
[69] From the Instructure answer to SURF on the 11th of July 2025.

Instructure specifies that the survey is delivered through a Salesforce notification containing a case ID in the link, which allows the response to be matched to the appropriate case. The survey provider does not receive or store any personal data as part of this process.[70]

The answers themselves ('Yes' or 'No') are not considered personal data. The GDPR does not apply to these responses unless they are linked to an identifiable person according to Article 4 GDPR (name, email, account ID). Case ID is included in the link: if that ID can be traced back to an individual (through internal systems, for example), then it is personal data under GDPR. Additionally, the comment box introduces risk, since it can contain personal data. The controller of the feedback data needs to clearly inform users how it's handled and encourage them to avoid unnecessary personal data. In the screenshot below, it is demonstrated that in the screenshot below that Instructure does not warn the users not to include personal data in the responses to the feedback.

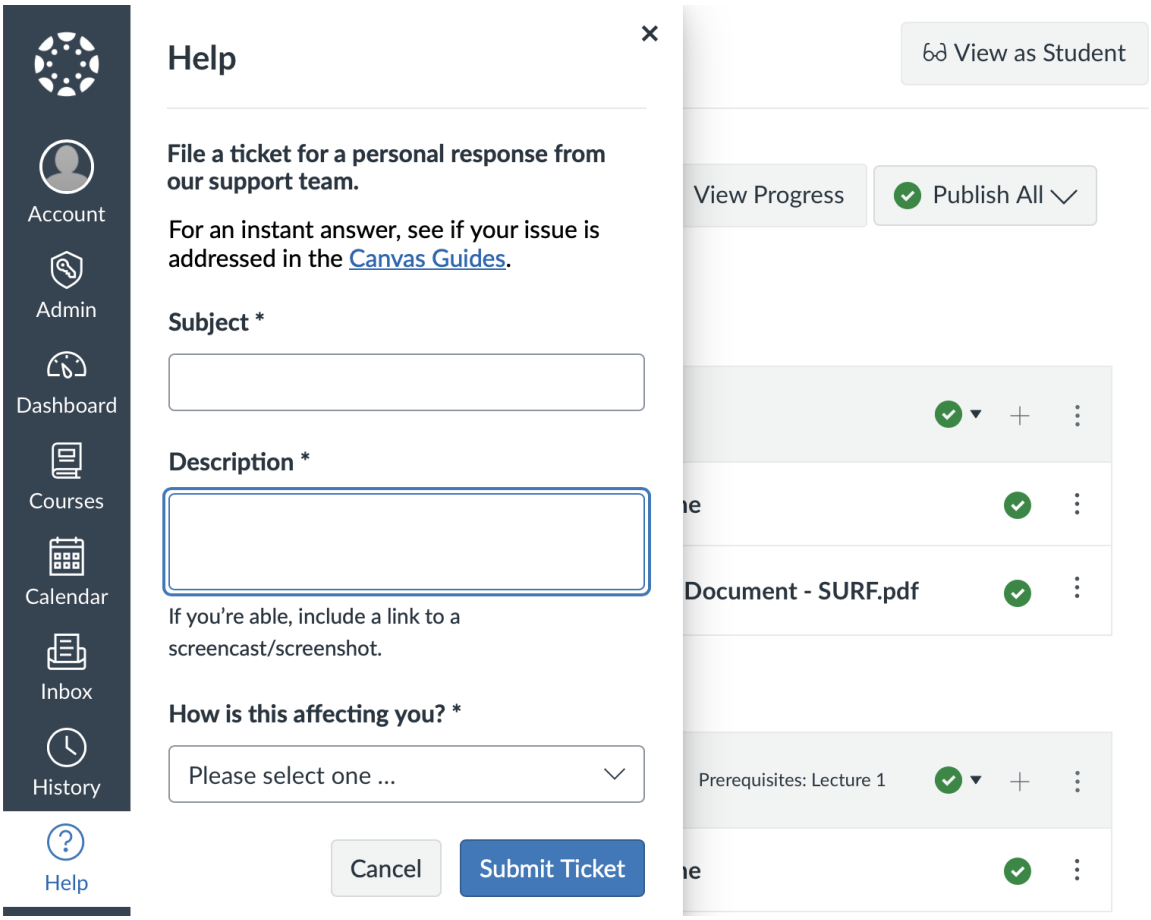

Figure 3 Canvas LMS support ticket

The risk associated with the Feedback processing may lead to risks. Since Instructure explicitly disclaims confidentiality obligations, any personal data included within submitted Feedback may be processed, stored, or shared. This increases the risk of unauthorized use or disclosure of personal information.

[70] From the Instructure answer to SURF on the 11th of July 2025.

A.5.3 Masquerading Functionality

Canvas LMS includes a masquerading feature, also known as “act as”, designed to allow administrators, whether from Instructure or from within an educational institution itself, to assume the identity of another user within the platform. This feature is intended primarily for troubleshooting, support, and configuration validation purposes.

Masquerading is available to two primary groups:

- **Instructure Support Staff**: Support agents, when handling customer requests, may use the masquerade function to simulate a student's or instructor's experience. This is particularly useful when trying to reproduce issues or provide contextual assistance.
- **Institutional IT Administrators**: Within an institution’s Canvas environment, any user assigned an administrator role with sufficient privileges can initiate a masquerade session. This includes IT staff, platform administrators, or others with administrative capabilities granted via the institution's internal role configuration.

In both cases, the process to begin masquerading is straightforward. An administrator selects the target user and clicks a “Masquerade” button. A continuous warning is displayed, informing the administrator that they are about to assume another user’s identity. If they confirm, they are immediately transitioned into the environment as that user. From that moment on, all actions taken are performed as if by the masqueraded user.

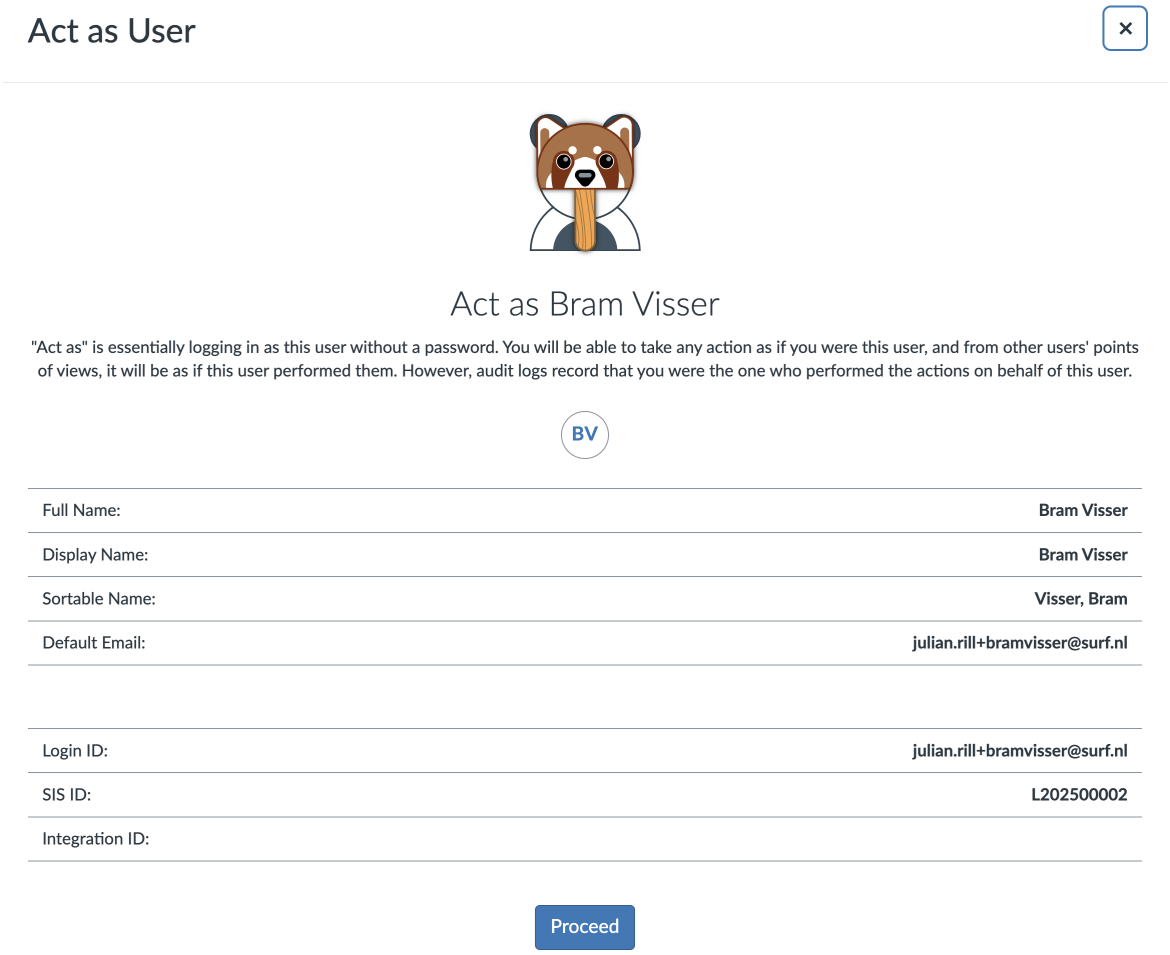

Figure 4 Masquerading disclaimer

The masquerade function operates entirely within the role-based permissions model of Canvas LMS. There is no approval workflow, either within Instructure's own support structure or within the institution's hierarchy, for initiating a masquerade session. That means, for example:

- A support agent at Instructure can masquerade as a user at an EU-based institution, assuming their permissions allow it, and provided they enter a support ticket justification. No one within the institution is notified, and no real-time approval is required. This functionality operates entirely within Canvas's role-based permissions model.
- An IT administrator at a university can impersonate any student or staff member without needing permission from a data protection officer, risk manager, or department head. There is no built-in mechanism to implement a supervisory approval step.

To enhance transparency, Canvas records all actions taken during a masquerade session in the audit log. These logs show when the session began, who initiated it, which user was impersonated, and the sequence of actions taken, each with a corresponding date and time stamp. Although the user interface does not notify the impersonated individual,

administrators are visually reminded of their status by a bright border around the screen during the session.

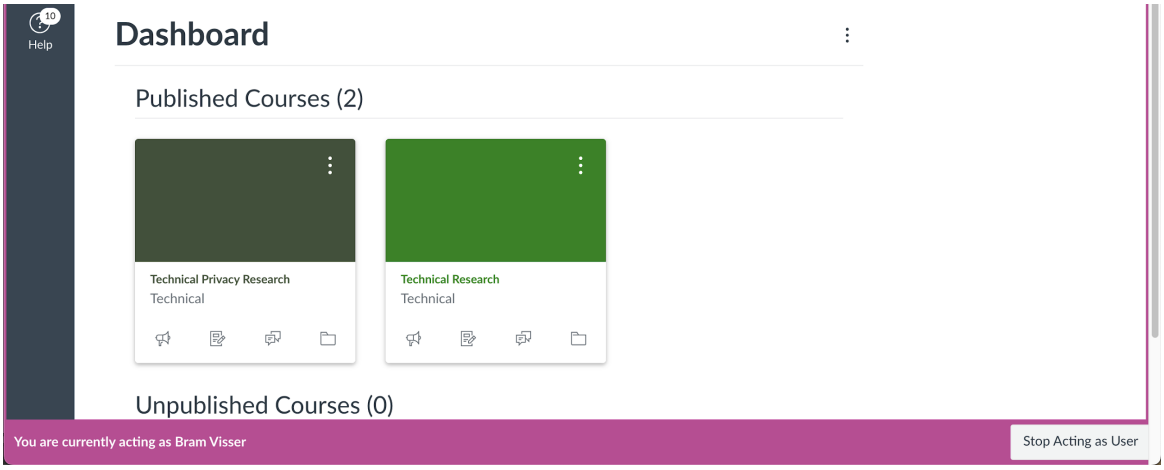

Figure 5 Visual Reminder of Masquerading

A.5.4 Identity and Access Management

Canvas LMS provides a flexible and granular identity and access management (IAM) model, primarily structured around roles. These roles are divided into two categories: course-level roles and account-level roles, each of which governs permissions and access scope in different parts of the platform.

A.5.4.1 Course-Level Roles

Canvas includes a set of predefined course roles, namely:

- Student
- Teacher *(used by instructors)*
- Teaching Assistant
- Designer
- Observer

These roles can be modified or extended. Institutions may create custom roles derived from the defaults, allowing for tailored permission sets that align with local governance policies or pedagogical needs. For instance, it is possible to create a variant of the Teacher role that has restricted grading capabilities or limited access to student analytics.

The permission model at the course level is highly granular. Roles can be configured to allow or restrict access to individual capabilities such as:

- Viewing course analytics
- Creating or moderating discussions
- Editing or posting grades
- Managing assignments
- Accessing and configuring LTI (Learning Tools Interoperability) tools
- Viewing or editing groups and student group data
- Reading SIS (Student Information System) data

Each user is assigned a role per course, rather than globally. A single user may, for example, hold a Teacher role in one course and simultaneously be a Student in another. This

contextual assignment of roles ensures that access is restricted to what is appropriate for a specific learning environment.

A.5.4.2 Account-Level Roles

Beyond the course level, Canvas supports account-level roles, which govern administrative functions across the entire institution's Canvas instance. By default, there is a single Account Admin role, which can be used as a template for creating additional administrative roles with varying privileges.

Account admins have access to advanced configuration and oversight capabilities, including:

- Managing global course templates via blueprints
- Modifying account-level settings
- Generating reports
- Viewing student analytics
- Creating and managing user groups
- Accessing global LTI tools
- Viewing and managing SIS integration

Like course roles, account roles can be customised; however, not all permissions are mutable. For example, the ability to add or remove other admins or alter core account-level permissions is strictly reserved for users already designated as account admins. Only an existing account admin can assign or elevate another user to that level.

A.5.4.3 Authentication and Role Provisioning

Canvas supports a wide range of third-party authentication providers (like SAML, LDAP, CAS, OIDC) and offers Just-in-Time (JIT) provisioning capabilities that allow user accounts to be created dynamically during login events.[71] Our research confirms that this JIT functionality, when combined with federated attributes, enables the assignment of user roles (including administrative privileges) at the time of authentication. Specifically, Canvas accepts a field called admin_roles as part of the federated attribute payload, which allows external identity providers (IdPs) to specify which users should receive which administrative roles within the root account.[72]

This mechanism supports basic access governance when Canvas is integrated with a well-managed IdP such as Azure AD, Okta, or similar platforms. Canvas will not only assign roles dynamically based on incoming assertions but also remove roles that are no longer present, unless otherwise configured. As such, federated attribute mapping can serve as a lightweight, login-triggered access control system that externalises role decisions to the institution's identity infrastructure.

However, this model has limitations. Role assignment via federated attributes only applies to the root account level. Sub-account roles or context-specific permissions must be managed manually or via the Canvas API. Furthermore, Canvas's access control changes are event-driven and occur only at the time of login. This means that if a user's role changes

[71] Instructure Community. "How Do I Configure Third-party Authentication Providers for a Canvas Account?," June 24, 2025. https://community.canvaslms.com/t5/Admin-Guide/How-do-I-configure-third-party-authentication-providers-for-a/ta-p/225.
[72] Instructure. "Authentication Providers - Canvas LMS REST API Documentation." Canvas LMS - REST API and Extensions Documentation. Accessed July 3, 2025. https://canvas.instructure.com/doc/api/authentication_providers.html.

(e.g., they leave the organisation or change departments), that change will not be reflected in Canvas until the next login event. There is no out-of-band mechanism for revoking or modifying roles independently of authentication events.

Given these limitations, institutions with higher access governance requirements may find federated SSO insufficient on its own. In such cases, integration with a full-featured Identity and Access Management (IAM) platform (e.g., SailPoint, Saviynt, or One Identity) can provide better lifecycle management control, segregation of duties enforcement, attestation workflows, and real-time deprovisioning. These platforms can interface with Canvas via its API to manage user access beyond what is possible with federated login alone.

A.5.5 AWS Databases

From a database architecture standpoint, Canvas uses PostgreSQL with streaming replication for high availability. Each database shard has a primary and one or more secondaries. Transactions are replicated in near real-time via WAL (Write-Ahead Log) shipping. In the event of a failover, some transaction loss is theoretically possible, but replication lag is minimal due to the tight synchronisation of replicas within the same AWS region. In cases where read-after-write consistency is required, background job queues carry transaction log pointers to ensure that secondaries have received the necessary data before executing tasks. Additionally, a tertiary "reports database" is maintained for heavy, less latency-sensitive operations, relying on slower log-based replication mechanisms and used for generating pre-defined institutional reports.

A.5.6 Logging

Canvas LMS demonstrates a high level of logging coverage across its application layers. Through our own investigations, we observed that the platform captures extensive telemetry related to user activity, administrative operations, and system-level events. This includes, but is not limited to: web access logs, authentication events, user impersonation (“masquerading”) actions, and GraphQL mutation traces. The system also records high-value events such as grade changes and course interactions to provide institutional administrators with detailed visibility into user behaviour.

Some logs are made available via Canvas APIs, to enable limited self-service audit capabilities for institutions. Other logs are ingested into backend storage systems, including long-term retention buckets such as AWS S3, presumably for internal analysis, compliance, or forensic purposes. Notably, Canvas appears to support traceability even in complex support scenarios: when a support agent impersonates a user, logs capture both the effective (impersonated) and actual (impersonating) user IDs. This contributes meaningfully to accountability and operational transparency.

Despite these positive aspects, there are transparency gaps regarding Canvas’s overall logging policy. In response to a formal request for documentation on log types, retention, access governance, and personal data handling, Instructure provided a high-level statement: logs are retained for one year and are subject to SOC 2 and ISO/IEC 27001 controls. However, no detailed breakdown was offered regarding which subsystems produce which types of logs, the specific purposes they serve, or how they relate to data protection principles.

A.5.6.1 Logs from Data Subject Access Requests

Trying to gain more insights into Canvas' logging activities, we conducted several Data Subject Access Requests (DSARs) based on our technical testing scenarios. Please refer to A.5.13 for more information. This research indicated that Canvas LMS logs a wide array of activities and interactions. This logging captures granular details of how a user navigates and interacts with the platform's features.

Key things logged from a user perspective include:

- **Page Navigation and Interactions (Page Views):**
  Captures user actions within the Canvas platform, such as viewing content, navigating features like courses or assignments, and interacting with tools like SpeedGrader. It includes metadata about the context of these interactions, the type of content accessed, technical details of the session, and timing of each event.
- **Resource Accesses (Asset User Accesses):**
  Provides information on the user's interaction with different types of course materials, including assignments, quizzes, files, and discussions. It also reflects the user's level of engagement, contextual roles, and when resources were accessed or interacted with.
- **Login and Authentication (Pseudonyms):**
  Details user login activity, including timestamps, login frequency, and IP addresses used. It also captures session timing and information about unsuccessful login attempts.
- **Content Creation and Submission:**
  Covers materials uploaded or submitted by the user, including assignments, quiz attempts, and discussion contributions. This section includes both the content types and the timing of submissions, which reflects participation in course activities.

Essentially, Canvas LMS maintains logs that record user activity across the platform and provides a digital footprint of how individuals engage with courses, assignments, discussions, and other features. These logs typically capture metadata (such as timestamps, accessed resources, navigation paths, and login history) which can include personal data like user IDs, roles, and associated course enrolments. However, the logs generally do not include the actual content that users actively input, such as assignment text, quiz responses, or discussion posts. It is important to note that while the logs do contain personal data, they do not reflect the full substance of user-generated content.

A.5.7 Authentication Processing

In Authentication Settings, you can manage SSO, Canvas self-registration, control Multi-Factor Authentication (MFA) requirements. You may also be able to customise password requirements and manage login attempt details.

By default, users can login in directly to Canvas using Canvas authentication. However, all Canvas users must have a Canvas account before they can log in to Canvas.

Canvas authentication includes an option called self-registration, which displays a registration banner on your account login page that allows users to create their own Canvas

accounts. You can also require users to complete a Captcha form before completing the registration process.

Canvas authentication can be used without self-registration. For instance, some institutions want to create user accounts with a student information system (SIS) and import SIS data into Canvas but allow users to log in using the default Canvas login page. Canvas authentication also supports Single Sign On (SSO) authentication, which allows you to customise your login information, and can be used in addition to third-party authentication providers.[73] SURFconext is one of the supported providers.

A.5.8 Instructure Community

Instructure Community is an online platform provided by Instructure to support collaboration, peer-to-peer assistance, and shared learning across institutions using Instructure products, including Canvas. It is not part of the core LMS but is operated by Instructure as an auxiliary service designed to empower educators, students, and administrators with resources and discussions outside the boundaries of their educational organisation's LMS environment[74].

Users can access the Canvas Community through single sign-on (SSO) from their education organisation's Canvas LMS account. When logged in to their Canvas environment, both students and instructors can navigate to the Canvas Community site without creating a separate account. This integration facilitates seamless access to Community content.

The Canvas Community offers:

- Product guides and release notes
- User forums for asking and answering questions
- Topical groups for specialised interests
- Live and on-demand webinars

Once logged in, the user's Community profile by default shows the following publicly available information[75]:

- Username as predefined during the first login in Instructure Community
- Full name (only visible to admins of the Community space)[76]
- Joined date
- Community activity
- Number of posts

According to Instructure, there is currently no technical method to disable access to the Canvas Community at the educational organisational or admin level[77]. This means educational institutions cannot prevent users from accessing the Community site via technical controls but can manage expectations or communicate use limitations through internal guidance.

---

[73] Instructure, 'How do I configure Canvas authentication details for an account?' (Instructure Community) https://community.canvaslms.com/t5/Admin-Guide/How-do-I-configure-Canvas-authentication-details-for-an-account/ta-p/257 accessed 24 October 2025.
[74] Instructure. "Instructure Community." Accessed June 4, 2025. https://community.canvaslms.com/.
[75] Instructure Community. "JulianRillSURF." Accessed June 4, 2025. https://community.canvaslms.com/t5/user/viewprofilepage/user-id/3720928.

[76] Instructure's feedback to the version 0.6 of this DPIA from December 4th 2025.
[77] Email response from Instructure to SURF's questions (May 19th, 2025).

A.5.9 Conferences

Canvas LMS includes a built-in virtual conferencing feature designed to support real-time interaction between instructors, students, and guests. Conferences are primarily used for virtual lectures, office hours, group collaboration, and live events. By default, Canvas integrates with BigBlueButton, which provides the conferencing infrastructure, including video, audio, screen sharing, and presentation tools.

When a user with the appropriate permissions (such as an instructor or student in a group) creates a conference, recording is enabled by default. This means that unless the setting is manually disabled at creation, the session will be recorded automatically. These recordings are stored temporarily and are automatically deleted after 7 days. The recording feature allows students who are unable to attend live sessions to view the content later; however, it also introduces a processing step where audio, video, and potentially participant names or avatars may be captured.[78]

Conferences are accessible to all course participants depending on the role-based permissions configured by the institution. While students can initiate conferences within their assigned groups, they cannot create course-wide conferences unless explicitly permitted. Conferences can host multiple participants.

A.5.10 Discussions

Canvas LMS includes a built-in discussion feature that facilitates asynchronous interaction among instructors, students, and teaching assistants. Discussions can be used for informal dialogue, topical engagement, or as graded assignments integrated with the Canvas Gradebook. They may take the form of focused discussions (limited to a single level of replies) or threaded discussions, which allow for nested responses and more complex, long-running exchanges.

By default, the setting that allows participants to comment is enabled, meaning students can respond to a discussion topic and to each other's posts without requiring any additional instructor action. Students can also view the names of others participating in the discussion unless group privacy settings are used. Instructors can choose to modify these defaults by restricting student permissions, enabling anonymous grading, or requiring students to post before viewing others' responses. Discussions can include rich media and attachments, and participation data may later be used for grading or analytics purposes.

A.5.11 Peer Reviews

Canvas LMS provides an optional peer review feature that allows students to review and comment on each other's assignment submissions. The peer review process involves collecting student submissions, assigning them to peers (either manually or automatically), and enabling reviewers to leave feedback either through free-text comments or structured rubrics. Peer review assignments become accessible to students only after they submit their own work.

By default, peer reviews are not anonymous, meaning students can see the names of those they are reviewing and who reviewed them. Although Canvas offers an anonymous mode, it

[78] Instructure Community. "What Are Conferences?," June 17, 2025. https://community.canvaslms.com/t5/Canvas-Basics-Guide/What-are-Conferences/ta-p/53.

must be explicitly enabled at the time of peer review assignment creation. If enabled, names are hidden from both the reviewer and the reviewed student; however, anonymity is not retroactive and cannot be changed once peer reviews have been assigned. Even in anonymous mode, instructors and teaching assistants retain visibility into reviewer identities.

A.5.12 Messaging and Communication

Canvas includes a built-in messaging system known as the Inbox, which provides an internal communication channel for users enrolled in the same course. This system facilitates asynchronous communication between students, instructors, teaching assistants, and administrators.

The Inbox supports individual and group messaging. Users can initiate a message to one or more recipients within the same course context. If the recipient list exceeds 100 users, the system automatically sends individualised messages to each recipient to ensure that recipients do not see the other addressees. Users may also message themselves, though such messages are only visible in the “Sent” folder.

Messages can only be exchanged between users with active enrolment in a course, and only while the course is published and ongoing. Messaging functionality is disabled once the course has concluded. Additionally, users cannot message across multiple courses simultaneously, nor can they contact users from unpublished or inactive course instances.

When permitted by institutional settings, the Inbox also supports differentiation tags, allowing messages to be targeted based on user roles or subgroups within a course (e.g., specific sections or assignment groups).

Messages sent through the Inbox can include file attachments. While the messaging system itself does not enforce file size limitations, any files uploaded during the exchange are counted against the sender’s personal file storage quota within Canvas. This creates a linkage between messaging and the personal files subsystem, implicating both in the processing of any user-submitted content. Attachments may therefore persist in user storage even if the corresponding message is deleted from the Inbox view. This has implications for both data retention and deletion requests.

The Canvas Inbox processes and stores the following personal data:

- **User Identifiers**: Sender and recipient names, roles, and Canvas user IDs.
- **Course Metadata**: Course ID, name, and role context, used to determine message eligibility and scope.
- **Message Content**: Subject lines, body text, and timestamped message threads.
- **Attachments**: Uploaded files, which may contain structured or unstructured personal data depending on user input.
- **Activity Metadata**: Read/unread status, timestamps of sending and receiving, and interaction logs.

Depending on institutional configuration, Canvas may also store delivery context metadata, such as whether a message was sent using differentiation tags or sent as part of a batch.[79]

A.5.13 Collaborations

The Collaborations feature within Canvas enables multiple users to work simultaneously on the same digital document. Changes to the document are saved in real time and immediately visible to all participants. This functionality is especially useful for group assignments, shared note-taking, and collaborative planning during course activities. Data processing within Collaborations hinges on integrations with third-party cloud platforms, which handle the underlying document creation, sharing, and editing infrastructure.

Collaborations in Canvas rely on specific third-party services made available through the Learning Tools Interoperability (LTI) standard. Institutions and course administrators can configure these integrations via the Canvas admin interface, selecting from a limited set of supported tools. At present, Canvas supports the following platforms for collaboration purposes:

- Google Docs (default)
- Google Drive and Google Workspace Apps (via Google Apps LTI)
- Google Assignments (LTI 1.3)
- Microsoft Office 365 (Word, Excel, PowerPoint via Office 365 LTI)

It is important to note that Canvas does not support any other integrations for Collaborations outside of these explicitly listed options. Alternatives such as Nextcloud or other third-party document collaboration services cannot be used within this feature.

A.5.14 Technical Investigation of Data Flows and Endpoints

We conducted a network-level technical investigation based on scripted scenarios, which in turn are based on real-world usage of educational institutions (see Appendix 1). One of our investigations is to map out the endpoints that handle user data during platform use. Our investigation revealed several important observations that diverge from the documented data processing arrangements, particularly concerning data residency and third-party services. All mapped endpoints can be consulted in Appendix 3.

A.5.14.1 Blindside Networks (BigBlueButton Conference Hosting)

Blindside Networks Inc. provides the virtual classroom functionality within Canvas LMS through its BigBlueButton service. Although the provider's documentation and regional support materials list Ireland as one of the available processing locations for EU-based institutions, our technical investigation revealed that traffic during test sessions was instead routed to infrastructure in Canada, specifically to the endpoint: *mxoa230004.rna1.blindsidenetworks.com*

This finding is significant, as BigBlueButton handles particularly sensitive categories of personal data in the context of virtual classroom delivery. The data types collected and processed during a session include:

- **Identification Data**: Username, ID, profile photo, and IP address. Captured when users join sessions.

[79] Instructure Community. "Differentiation Tags • FAQ," August 4, 2025. https://community.canvaslms.com/t5/Differentiation-Tags/Differentiation-Tags-FAQ/ta-p/639336.

- **Attendance Metadata**: Meeting ID, content shared, and login times. Used for generating attendance reports.
- **Analytic Signals**: Session interaction data, browser, operating system. Used for moderator insights and session engagement analysis.
- **Audio Recordings**: Live speech content is processed to support real-time captioning and later transcription.
- **Session Recordings**: Captures visual likeness, spoken content, and shared materials. Stored for later review, quality assurance, and troubleshooting.
- **Technical Diagnostics**: Interaction metadata and audio quality metrics, collected during sessions for debugging.

Given the nature of this data, much of it linked to identifiable individuals and involving real-time interaction, the expectation from a data protection standpoint is that such processing be handled within the EEA, particularly where the provider already advertises support for hosting in Ireland.

Following this finding, Instructure confirmed that this routing occurred because the sandbox environment provided to SURF had not been correctly configured to direct BBB traffic to the EMEA region. This configuration step is normally implemented for customer environments but was omitted in our test setup. According to the vendor, this behaviour would not occur in properly configured customer instances.

A.5.14.2 Canvas LMS' Single Sign-On (SSO) Endpoint Hosted in the United States
During our investigation of network traffic related to user authentication, we initially identified that while most Canvas-related services (e.g., *canvaslmsreview.instructure.com* and *canvaslmsreview.quiz-lti-fra-prod.instructure.com*) are hosted on Amazon Web Services infrastructure in Germany (eu-central-1) as expected, the domain *sso.canvaslms.com* stands out as an exception.

Captured requests during live authentication included traffic to:
https://sso.canvaslms.com/post_message_forwarding?rev=59677caad5...
https://sso.canvaslms.com/delegated_auth_pass_through?target=https...

The payloads and headers in these requests suggest that the following categories of data are processed:

- **User Identifiers**: Includes a persistent user ID and potentially obfuscated or encrypted session tokens associated with the user identity (e.g. cluster59).
- **Session Metadata**: Tokens or hash-based references to user session state are transmitted to facilitate login continuity across services.
- **Origin Information**: Request headers such as referrer, origin, and user-agent reveal the user's browser type, Canvas instance URL, and device details (e.g., x-canvas-meta).
- **IP Address**: Captured as part of standard request metadata and likely logged at the server level for security and routing.
- **Cross-Origin Authentication Artifacts**: The request and response headers include CORS-related metadata, token forwarding, and security context used in federated login flows.

This endpoint does not appear to process user profile data (like names, emails, roles or course affiliations) directly in the observed payloads. However, the session tokens it handles are tightly coupled to such data and would grant access to it once resolved by downstream services.

Instructure's own Transfer Impact Assessment (TIA) on AWS states[80]:

> *"Instructure Global Limited hosts its application and data servers at AWS on servers physically located in the EU. The only exception is Canvas Commons, which is out of scope of this TIA. A very limited subset of this data, which is non-personal except for the IP address, may be transferred to edge servers located outside of the EU based on the physical location of the user, solely for content delivery purposes."*

At first glance, this suggested that user authentication traffic (including session tokens and associated identifiers) might be routed through U.S.-based infrastructure. However, further analysis revealed that sso.canvaslms.com uses AWS Global Accelerator. This service routes requests to the nearest AWS edge location based on the user's physical location. In our case, authentication requests made from within the EU (Netherlands) included a response header indicating that traffic was handled by infrastructure in eu-central-1c — an AWS availability zone in Frankfurt, Germany: *x-canvas-meta: … z=eu-central-1c; …* This header provides strong evidence that the authentication traffic, despite being directed at a global endpoint, is in fact being handled within the EU region when initiated by EU-based users.

While this setup reduces the likelihood of cross-border data transfers during authentication, it relies on AWS infrastructure and routing logic that is not visible or configurable by the end user. The endpoint itself (sso.canvaslms.com) does not offer any assurance, from a domain or certificate standpoint, that EU residency is preserved. It implicitly trusts AWS's regional routing guarantees, without exposing sufficient architectural detail to verify where session tokens are ultimately resolved or whether any replication or logging occurs outside the EU.

[80] Instructure Inc. – TIA on Amazon Web Services – 2023.10.

A.6 Processing Techniques and Methods

A.6.1 Canvas LMS Cookie Notice

The Canvas LMS Cookie Notice outlines the types of cookies Instructure uses within the Canvas LMS detailing their purposes, durations, and classifications.[81] In this document, Instructure provides detailed information about the cookies used within its services. All cookies are first party, set either by Instructure or its authorised partners, and are categorised into three types: strictly necessary, functionality, and analytics.

Users manage their cookie preferences through their browser settings or in accordance with their institution's policies. Users can find the list of individual cookies with corresponding purposes and data processed explained in detail and in Table 6 Relevant Cookies as described in the Cookie Notice of Instructure below. Additionally, the cookie notice includes contact information for users who may have questions, comments, or concerns regarding the use of cookies or the content of the notice itself.

It is important to note that analytics cookies are configured for use exclusively within the United States and are not actively deployed in other regions. While they are not intended to operate outside the U.S., our technical research was conducted to confirm that no analytics cookies are placed in other regions. The cookies as shown in Table 6 below are the relevant cookies for educational institutions within the EEA.

Cookie	Purpose	Data Processed	Duration	Type	Type
canvas_otp_remember_me	Used for persistence of a one-time password.	None	Session - Expires at end of the user's session.	First-party Instructure	Functionality
_legacy_normandy_session	Used to work around iOS12 samesite=none issues.	None	Session - Expires at end of the user's session.	First-party Instructure	Functionality
_csrf_token	Used for cross-site request forgery protection updates with ajax requests.	None	Session - Expires at end of the user's session.	First-party Instructure	Strictly Necessary
canvas_session	The cookie is the authenticated session ID for the user for the session in Canvas LMS. It is initiated upon	String value of a unique session token instantiated upon successful	24 hours	First-party Instructure	Strictly Necessary

[81] Instructure, 'Canvas Learning Management System Cookie Notice' (Instructure) https://www.instructure.com/policies/canvas-lms-cookie-notice accessed 24 October 2025.

	successful authentication to Canvas LMS and is used to maintain an authenticated session for the user for the duration of this session token. This session token is used with all requests during the session. When this cookie expires—either by logging out or by reaching the session token max time —the user is required to re-authenticate to initiate a new session token.	authentication to the Canvas LMS.			
deleted_page_title	This cookie is used to store the value of a previously existent and recently deleted page. When a user tries to access the previously deleted page, a "page deleted" message with the deleted page title to a user when that page is loaded. Having this value persist in a cookie helps make an intuitive user experience when attempting to access a previously deleted page.	Title of the previous existent page title prior to deletion.	Session - Expires at end of the user's session.	First-party Instructure	Functionality
last_known_canvas_host	This cookie stores the value of the Canvas hosts last visited by the user. The purpose of this cookie is to provide a smooth user experience when the user is in a logged-out state and Canvas LMS. When the user clicks on "Login" on a Canvas / Instructure website, this cookie is used to redirect the user to the user's expected Canvas authentication URL for login.	String value containing the most recently visited Canvas hostname.	24 hours	First-party Instructure	Functionality

last_page_view	This cookie is a unique identifier that is included as part of each request during an active session. The purpose of this identifier is to allow for Instructure's operations and engineering teams track session requests for the entirety of a user session, making the ability to troubleshoot in-session request errors or other user interface errors contrained to this ID.	String value of a unique log session token identifier instantiated upon successful authentication to the Canvas web application.	24 hours	First-party Instructure	Functionality
ui-tabs-*	This cookie is used to remember the focus of a tab within the web user interface (where tabbed content is displayed to the user). These cookies are used by jquery-ui. The purpose of this cookie is to provide a smooth user experience to the user—allowing the user, upon return to the originally in-focus tab when returning to the user interface showing multiple tabs.	String value of the in-focus tab prior to leaving the interface displaying multiple tabs.	Session - Expires at end of the user's session.	First-party Instructure	Functionality
unsupported_browser_dismissed	This cookie is used to save the users response to a prompt displayed to a user via the web user interface to dismiss the notification. This cookie is used only for users using an unsupported browser and is stored only when the user clicks "Dismiss" on the notification. This cookie tells the application to not show this notification for every loaded page.	Exists if the user has click "Dismiss" on the unsupported browser notification.	Session - Expires at end of the user's session.	First-party Instructure	Functionality

Table 6 Relevant Cookies as described in the Cookie Notice of Instructure

In addition to the cookies in Table 6 (the cookies as described in the Cookie Notice), the execution of scenarios as part of technical testing (see Appendix 1) revealed that additional cookies were placed not described in the Cookie Notice. These cookies and their purposes are described in Table 7 Found Cookies during Technical Research.

Cookie	Purpose	Data Processed	Duration	Type	Type
inst-fs-session	These cookies are currently used to authenticate the session in Canvas to validate that the user downloading a file is the same as the one logged into Canvas. Instructure noted that they are removing session authentication from Inst-FS by July 2025, and consequently, these cookies will also disappear.	Uploaded files by end-users, presenting files hosted on Canvas Cloud.	Session - Expires at end of the user's session.	First-party Instructure	Functionality
inst-fs-session.sig		Uploaded files by end-users, presenting files hosted on Canvas Cloud.	Session - Expires at end of the user's session.	First-party Instructure	Functionality
log_session_id	A unique identifier that is included as part of each request during an active session. The purpose of this identifier is to allow for Instructure's operations and engineering teams to track session requests for the entirety of a user's session, making the ability to troubleshoot in-session request errors or other user interface errors constrained to this ID.	String value of a unique log session token identifier instantiated upon successful authentication to the Canvas web application.	Session - Expires at end of the user's session.	First-party Instructure	Functionality
pseudonym_credentials	A value (database identifier for a remember-me token, a random-but-persisted-value from their credentials, and a random-but-persisted value from the remember-me token) that is stored in a persistent cookie, allowing the user to automatically be logged back in with a fresh session when they next open the browser.	The user's unique_id, password and whether 'remember me' is turned on.	2 weeks - the corresponding token on the backend is expired after 1 month.	First-party Instructure	Functionality

Table 7 Found Cookies during Technical Research

A.6.2 ISO/IEC 27001

Instructure's Canvas LMS holds valid third-party assurance certifications: ISO 27001 and SOC 2. They provide reasonable assurance that their security controls align with the requirements of the GDPR, and on the security of processing. The vendor has also committed to providing their next SOC 2 report and updates on open risks in their risk register, reflecting a proactive approach to maintaining transparency and ongoing compliance.

A.6.3 Analytics

Canvas LMS provides built-in analytics capabilities that allow instructors, students, and administrators to gain insight into user engagement, course performance, and participation trends. These analytics tools are implemented through two main interfaces: the legacy **Analytics** feature and the evolving **New Analytics** interface. In addition, administrative-level insights are accessible via the **Analytics Hub**, a centralised portal that aggregates data across Canvas and other Instructure products. Notably, Intelligent Insights (a separate AI-driven product) is out of scope for this DPIA as described in the scope. Analytics are enabled by default and cannot be disabled.

A.6.3.1 New Analytics

New Analytics is a modernised data visualisation and monitoring tool designed for instructors and students at the course level. It offers interactive charts and tables that track key metrics such as:

- Course grades and assignment submissions
- Weekly online activity and student participation
- Inbox communication (messaging activity between users)

This tool enhances visibility into learner engagement and course performance. For instructors, it includes options to message students based on performance or submission status directly from within the analytics interface. For students, it provides downloadable views of their academic activity, such as grades and participation metrics.

New Analytics only operates in published courses and requires that users have the appropriate course-level permissions to view analytics content.

While mobile usage data is captured, it is subject to limitations. Because mobile page views depend on the specific device settings and network latency, time stamps for activity may not align precisely with actual usage. As such, Canvas explicitly notes that New Analytics data should not be used to assess academic integrity.

Unposted assignments are excluded from course grade calculations within the New Analytics interface, and users may need to enable third-party cookies in their browsers for full functionality.

A.6.3.2 Analytics Hub

At the administrative level, Canvas offers the Analytics Hub, a centralised interface designed to provide Canvas admins with consolidated access to analytics tools across the Instructure ecosystem. The scope of available tools is determined by a combination of user role permissions, account-level feature settings, and institutional purchases.

The Analytics Hub includes a variety of data domains, such as:

- **Usage & Adoption**: Monitors use of Canvas and integrated LTI tools.
- **Student Success**: Provides dashboards like "Students in Need of Attention" to support proactive interventions.
- **Course Effectiveness**: Reports on how course content is structured and utilised.
- **Data Access**: Offers interfaces such as Canvas Data 2, the DAP CLI, and the DAP Query API for institutions needing direct access to raw datasets for research, mining, or third-party analysis.

Importantly, analytics data within both New Analytics and Analytics Hub is subject to role-based access control (see) to ensure users can only view data relevant to their assigned permissions.

Analytics runs on Looker, a business intelligence platform. It provides a data exploration and dashboarding interface for users, an IDE for data modelers, and embedding and API features for developers. Please also refer to A.7.3.1.

A.6.3.3 Crash Analytics

The Canvas mobile applications integrate Firebase Crashlytics for real-time crash reporting and diagnostics. This service, provided by Google, collects and processes technical crash data to support application stability and performance monitoring. Crashlytics data collection is enabled by default in the SDK and begins automatically once the app initialises the service. Unless explicitly disabled in the app's configuration, this processing takes place without requiring active user opt-in.

Firebase Crashlytics enables developers to monitor application reliability through automatic collection of crash reports, exception traces, and related contextual metadata. Instructure uses this for identifying app failures, understanding failure trends, and prioritizing bug fixes.

Our technical analysis of the source code[82] revealed that exceptions are logged, but the user ID is forcibly set to an empty value, except during masquerading. Custom log messages (e.g., non-fatal errors) are also logged. No evidence was found of explicit collection or logging of names, email addresses, or other personally identifiable information. Logging is limited to exception traces, debug messages and context metadata.

Firebase Crashlytics operates in conjunction with Google Analytics for Firebase (GA4) to augment crash reports with demographic and device-level data that is inferred or derived from the client environment and Firebase's backend systems. These data points include[83]:

User Dimension	Type	Description
Age	Text	Age bracket: 18–24, 25–34, etc.

[82] Rill, Julian Calvin. "Google Firebase Crashlytics Crash Simulation · RillJ/Canvas-android@E915a2c." GitHub, June 4, 2025. https://github.com/RillJ/canvas-android/commit/e915a2c30e3a3606ff2f9bc5bca01f0aff6a66c5.
[83] Google. "[GA4] Predefined User Dimensions - Analytics Help." Accessed June 3, 2025. https://support.google.com/analytics/answer/9268042?sjid=14191604911736132664-EU.

App store	Text	The source from which the app was installed.
App version	Text	App version (versionName or bundle version).
City	Text	City from which user activity originated.
Continent	Text	Continent of origin.
Country	Text	Country of origin.
Device brand	Text	Manufacturer (e.g., Samsung, Apple).
Device category	Text	Type of device (e.g., mobile, tablet).
Device model	Text	Device model (e.g., iPhone 13, SM-J500M).
Gender	Text	User gender (male or female), if inferred.
Interests	Text	Inferred interests (e.g., Arts, Sports).
Language	Text	Device OS language setting (e.g., en-US).
New/Established	N/A	Classification as a new or returning user.
Operating system	Text	OS type (e.g., Android, iOS).
OS version	Text	Version of the OS (e.g., 14.4, 13).
Platform	Text	The platform (e.g., iOS, Android).
Region	Text	Sub-national region (e.g., California, Bavaria).
Subcontinent	Text	Geographical subcontinent (e.g., Northern Europe).
App-instance ID	Text	Pseudonymous identifier generated automatically by Firebase Analytics.

Table 8 Google Firebase Crashlytics Data Points

The app-instance ID is a randomly generated identifier assigned to each installation of the app. It is used to group crash and analytics data without directly identifying users. The ID format is either a 32-character hexadecimal string or a UUIDv4 (without dashes).

A.6.3.4 Admin Access to User Activity

In Canvas LMS, administrators can access detailed user activity information by navigating to Admin > People and selecting an individual user's profile. By default, this view displays a full log of the user's actions within the platform, including which pages they visited and the exact timestamps of those visits. This activity data is presented immediately upon opening the user profile without requiring any additional steps or confirmation.

A.6.4 Encryption

Encryption practices follow AWS's envelope encryption model. All data volumes are encrypted at rest using AWS-managed keys (via KMS). These keys are never visible to Instructure employees and are region-specific to ensure they are never transferred across jurisdictions.[84] Access to encrypted data is mediated by IAM (Identity and Access Management) policies, which strictly limit what roles or services can decrypt or read sensitive data. Thus, data remains confined to its originating region, and even in scenarios involving cross-regional support, encryption keys are never transported.[85]

Instructure's current architecture does not support customer-managed keys (CMKs)[86]. Educational institutions do not have the option to generate or control their own encryption keys via AWS KMS or otherwise get access to them[65]. While AWS supports such a model, whereby customers provision and manage their own KMS keys and grant service providers scoped access to decrypt specific resources, Instructure has opted not to implement this model. Their justification is that they operate as a SaaS provider, and key management is centrally handled as part of the platform architecture.[66]

This means:

- Educational institutions cannot unilaterally revoke Instructure's access to encrypted data via key controls.
- Educational institutions cannot directly audit key usage events or decryptions.
- All key generation, access, and revocation are performed within the AWS-managed KMS under configurations controlled by Instructure.

Institutions are therefore dependent on Instructure's access policies, AWS KMS configurations, and associated audit and compliance frameworks (such as SOC 2 and ISO/IEC 27001 certifications) for the protection of cryptographic assets.

A.6.4.1 Encryption from the legal perspective

When processing personal data, the Controller decides both the purpose and the method: essentially answering the 'why' and 'how' of the data processing. It means that the following is determined: why the data is being processed (what goal it is meant to achieve) and how that goal will be reached (what tools or strategies will be used). Education institutions hold

[84] Online meeting between Instructure and SURF to discuss SURF's questions (May 8th, 2025).
[85] Email from Instructure answering SURF's questions (May 19th, 2025).
[86] Canvas Instructure CAIQ assessment.

this level of influence over data processing plays a role in shaping its purpose and methods, as defined in Article 4(7) of the GDPR.[87]

Applying this rule to the encryption keys managed by Instructure, if the controller is responsible for determining the purpose and essential means of processing, then holding encryption keys is a crucial factor in assessing whether a processor has control over the data. If an education institution (as the controller) defines both the purpose and the means, but a processor retains exclusive control over encryption keys, this could challenge the controller's ability to truly govern the processing operation.

In such a case, the processor, rather than merely executing controller's instructions, might hold a degree of influence over the 'how' of data processing, raising questions about whether they are effectively acting as a joint controller or assuming more responsibility than a typical processor under GDPR.

GDPR compliance in this setup depends on the degree of control the processor has over the encrypted data. A legally binding contract acts a safeguard and defines the processor's responsibilities and outline processing measures that align with the Controller's objectives: both the 'why' and 'how'. In the situation of SURF, there is no direct agreement with Instructure, however SURF Education Institutions regulate this aspect in the direct DPA between Instructure and themselves. The clause mentioned in the Institution's (MBA's) DPA:

'*For data transferred to countries outside the EEA, it will be encrypted with key in Europe or fully annotated. For this, the TTP (Thrusted Third Party) protocol of European commission applies'*.[88]

The data should be encrypted before the transfer of data, and the encryption key will be stored in Europe. This means that the recipient cannot decrypt the data unless authorised by an entity within Europe.

From the DPA with the universities, encryption key is not regulated, however it is mentioned that usernames and passwords are never transmitted in plain text. They are always encrypted (via HTTPS) to protect against interception or misuse during login or communication.[89] Additionally, it is stated that the basic principle is that use is made of SURFconext (which provides a Single Sign On (SSO) environment), which allows users to log in once and access multiple services securely.

According to the EDPB, for encryption to be effective, the encryption keys must be reliably managed and retained solely under the control of the data exporter.[90] Data exporter is a

[87] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (European Data Protection Board, 7 July 2021) https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf accessed 24 October 2025' ; 'Case C-25/17, ECLI:EU:C:2018:551, para 68.
[88] MBO DPA, page 17.
[89] University DPA, page 16.
[90] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (European Data Protection Board, 18 June 2021) https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 24 October 2025' ; 'European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (European

controller, and so far, the keys are legally under the control of education institutions because of the DPA.

However, GDPR recognizes that security risks, data misuse, and emerging technologies evolve over time. Vendors (not only Instructure) should continuously enhance privacy measures, not just meet the minimum legal standards but anticipate potential risks and integrate robust safeguards at every stage of development. Article 25 of GDPR explicitly states that controllers and processors must implement appropriate technical and organizational measures before processing begins, ensuring that personal data remains secure throughout its lifecycle.
Despite encryption keys stored in the EU as regulated by the contract, Instructure is obligated to continuously improve security and ensure they stay aligned with evolving best practices. This means that if Educational Institutions will be continuously dependent on Instructure's access policies, AWS KMS configurations, and associated audit and compliance frameworks (such as SOC 2 and ISO/IEC 27001 certifications) for the protection of cryptographic assets, their role as controllers will be challenged by not having access in a timely manner to Institution's data.

A.6.5 AI Processing Features

Canvas LMS includes a set of artificial intelligence (AI)-powered functionalities designed to enhance usability and pedagogical scalability. These features rely on third-party large language models and machine translation technologies, but are implemented with attention to data minimisation and compliance considerations. The three primary AI features currently available are Canvas Discussion Summaries,[91] Canvas Smart Search,[92] and Canvas Course Translation.[93] Each feature involves different data inputs and processing methods.

A.6.5.1 Canvas Discussion Summaries

The Discussion Summaries feature uses Anthropic's Claude 3 Haiku large language model to generate high-level overviews of course discussion threads. Its primary goal is to support instructors in large-scale courses by providing a recap of key points, questions, and insights from discussion forums that may otherwise be impractical to monitor manually.

- **Data Inputs**: The model processes the course's discussion prompts and replies, which may contain personal data (e.g., names, student reflections).
- **Data Retention**: The model does not retain or reuse input data. Once processed, summaries are stored in the Canvas database for future review and reuse.
- **Data Logging**: Summaries are logged within Canvas; however, the AI model provider does not retain logs of the data.
- **PII Handling**: No personally identifiable information (PII) is intentionally shared with the model, but incidental exposure may occur via student replies.

Data Protection Board, 11 November 2020) https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en accessed 24 October 2025' page 30. Schrems 2 ruling.

[91] Instructure Community. "AI Nutrition Facts: Canvas Discussion Summaries," October 29, 2024. https://community.canvaslms.com/t5/Artificial-Intelligence-in/AI-Nutrition-Facts-Canvas-Discussion-Summaries/ta-p/608252.

[92] Instructure Community. "AI Nutrition Facts: Canvas Smart Search," October 29, 2024 https://community.canvaslms.com/t5/Artificial-Intelligence-in/AI-Nutrition-Facts-Canvas-Smart-Search/ta-p/608254.

[93] Instructure Community. "AI Nutrition Facts: Canvas Inbox and Course AI Translation," October 30, 2024. https://community.canvaslms.com/t5/Artificial-Intelligence-in/AI-Nutrition-Facts-Canvas-Inbox-and-Course-AI-Translation/ta-p/608256.

- **Controls and Oversight**: Instructors can review, regenerate, or refine summaries, ensuring a human-in-the-loop model. AI settings are configurable.

A.6.5.2 Canvas Smart Search

The Smart Search feature utilises Cohere Embed Multilingual, a multilingual embedding model, to index course content and enable natural language search capabilities for both students and educators.

- **Data Inputs**: The model indexes course materials (e.g., syllabus, modules, pages) for use in search. This content may include incidental personal data.
- **Data Retention**: Inputs are used only for generating embeddings and are not stored or reused by the model.
- **Data Logging**: No logging occurs at the model provider level. Indexed data is stored in the Canvas database for serving search queries.
- **PII Handling**: While PII may exist in course content, it is not specifically targeted or extracted.
- **Controls and Oversight**: Human review is enabled, and AI settings can be adjusted institutionally.

A.6.5.3 Canvas Course Translation

This feature enables automatic translation of discussion threads and inbox messages into over 100 languages, using Meta's M2M-100 translation model. The aim is to promote inclusion by supporting multilingual communication, particularly for non-native speakers.

- **Data Inputs**: The translation system processes content from inbox messages, discussion prompts, and replies.
- **Data Retention**: No input data is stored or reused by the model.
- **Data Logging**: There is no data logging at the model provider level.
- **PII Handling**: Although PII may appear in messages or discussions, no identifying information is deliberately submitted to the model.
- **Controls and Oversight**: Human review of translations is possible; untranslated content remains accessible for comparison.

Across all three features, Instructure states that AI processing is stateless and does not train on user data.[71, 72, 73] In all cases, model outputs are either stored locally in the Canvas database or used transiently to serve functionality. Institutions have access to configuration settings and review mechanisms. Nevertheless, incidental PII exposure in input content, particularly in discussions or messaging, should be considered inevitable.

All AI models run on Instructure's AWS instance of the institution. No other sub-processors are involved.[94]

A.6.6 Application Programming Interfaces (APIs)

Canvas LMS provides two primary APIs to facilitate programmatic interaction with the platform: a RESTful API and a GraphQL API. These interfaces are used by institutions, third-party tools, and integrators to access and manipulate data within Canvas LMS outside the core user interface.

[94] Email from Instructure answering SURF's questions (May 19th, 2025).

A.6.6.1 REST API

The REST API is the more mature and comprehensive interface. It is designed to expose resources and operations over HTTP in a structured manner. It supports typical CRUD (Create, Read, Update, Delete) operations across key entities such as courses, assignments, users, enrolments, grades, and messages. Each resource is accessed via defined endpoints, and all responses are returned in JSON format.

REST APIs are widely used in LTI contexts, custom scripts, institutional integrations, and administrative automation. Canvas's REST API also forms the backend of many internal platform components.

A.6.6.2 GraphQL API

The GraphQL API is a newer, more flexible alternative to REST. It allows clients to request only the specific fields they need and to bundle multiple queries into a single request. This results in reduced payload sizes, faster response times, and more efficient network usage, especially for mobile applications or complex UI components.

Canvas's GraphQL API adheres to the Relay specification, meaning it uses globally unique object IDs and supports features like connection-based pagination. Developers can request either the global ID or the legacy-style _ID used in REST. The API also supports introspection and offers a browser-based tool (GraphiQL) for testing and crafting queries within the institution's Canvas LMS environment.

However, the GraphQL API does not yet cover the full surface area of the REST API. New functionality is gradually being added based on demand and community contributions.

A.6.6.3 Authentication and Authorisation

Both the REST and GraphQL APIs in Canvas use OAuth 2.0 for authentication and authorisation. This protocol allows external applications to act on behalf of users without exposing their passwords.

To access the API, client applications must first register with Canvas to obtain a client ID and client secret. Once registered, applications initiate the OAuth 2.0 flow, which includes:

- User redirection to Canvas for consent and authorisation.
- Canvas redirects back to the application with a one-time authorisation code.
- The application exchanges this code for an access token via a server-to-server request.
- The access token is then used in the JWT authorisation header of subsequent API requests (Bearer <token>).

Tokens are short-lived (typically 1 hour) and may be refreshed using a refresh token to maintain session continuity without user re-authentication. Canvas also supports manual token generation for testing purposes, but production use mandates the OAuth flow for multi-user applications.

All API communications are encrypted using HTTPS. HTTP connections are automatically redirected, but as any credentials sent via HTTP are already exposed, they should be avoided entirely.

Canvas enforces role-based access control on API interactions. API access mirrors the permissions of the authenticated user as described in A.5.3

- A student using an access token will only be able to view their own data and actions permitted within their role.
- An instructor can view and modify content and grades within their assigned courses.
- Admins with broader roles can access institutional-level data, subject to their configured privileges.

GraphQL queries are similarly constrained: the backend applies the same permission model to ensure that users cannot use the API to circumvent UI-based access controls.

Canvas also uses OAuth2 for LTI Advantage services, enabling third-party tools to access line items, assignment scores, and enrolment data using the client credentials grant type. These services are commonly integrated into institutional learning environments and are governed by the IMS Global Learning Consortium's security framework.

A.6.7 Anonymisation and Pseudonymisation

Canvas LMS includes a limited range of anonymisation features that aim to reduce the visibility of personal data during teaching and assessment workflows. These features are mostly interface-level configurations and are primarily designed to support impartial grading and privacy-conscious feedback. They do not provide systematic anonymisation of user data at rest or in backend systems.

A.6.7.1 Anonymous Grading

Canvas provides an anonymous grading feature that, when enabled, hides student names from instructors or graders during the assessment process in SpeedGrader.[95] This helps reduce potential bias during evaluation. The feature is applied on a per-assignment basis and is opt-in at the course level. Once activated, anonymous grading can make sure that student identities are masked until grades are manually posted. Posting grades removes anonymity from the assignment, thereby restoring the association between submissions and student identities.

This form of anonymisation is effective only within the grading interface. It does not extend to backend data, audit logs, or instructor access elsewhere in the course environment. Additionally, anonymous grading is not supported for all assignment types. Most notably, it is not available for graded discussions, which may carry identifiable content submitted by students.

The feature also integrates with moderated grading which allows additional privacy between graders if configured, but its application remains confined to the interface and workflow in SpeedGrader.

[95] Instructure Community. "How Do I Add an Assignment That Includes Anonymous Grading?," August 4, 2025. https://community.canvaslms.com/t5/Instructor-Guide/How-do-I-add-an-assignment-that-includes-anonymous-grading/ta-p/769.

A.6.7.2 Anonymous Instructor Annotations

Instructors can choose to anonymise their own annotations made via DocViewer, the Canvas tool used for in-line feedback on student submissions.[96] When this setting is enabled before any annotations are made, comments added through DocViewer do not display the instructor's name to the student. However, this anonymity only applies to annotations within the submission window. Comments entered in the SpeedGrader sidebar (outside of DocViewer) are not anonymised and will include instructor attribution.

It is important to note that the setting for anonymous annotations is assignment-specific and must be enabled before any student submissions are received. Annotations made before enabling this option will remain identifiable. The feature is not retroactive.

A.6.7.3 Implications

These features are not intended for data protection purposes in the broader legal or technical sense. They are not designed to render data irreversible or de-identified under data protection law, nor do they provide persistent anonymisation at the database or storage level. All original identifiers remain accessible to administrators and can be restored or revealed through standard workflows (like posting grades or viewing submissions outside the grading interface).

In terms of effectiveness, the anonymisation in Canvas LMS should be understood as interface-level obscuring rather than full data anonymisation. It supports fair assessment practices and role-based privacy in teaching workflows, but it does not prevent re-identification or provide safeguards against linkage through other available data in the system.

[96] Instructure Community. "How Do I Enable Anonymous Instructor Annotations in Student Submissions?," August 4, 2025. https://community.canvaslms.com/t5/Instructor-Guide/How-do-I-enable-anonymous-instructor-annotations-in-student/ta-p/665.

A.7 Involved Parties

A.7.1 The Role of Education Institutions

This DPIA examines the data processing in the context education institutions. Different from consumer users, public sector organisations are data controllers in relation to the data they process about their students and employees, including disclosure of personal data to third parties.

According to Instructure's documentation, Education institutions act as controllers for the personal data that processed by Instructure.

A.7.2 The Role of Instructure

Under the Instructure's Canvas LMS Privacy Data Sheet (April 2024), Customer is the data controller of personal data inputted into Canvas LMS by their End-Users. Instructure explains that educational institutions determine the purpose of using the products and services, and for which Canvas LMS is used. Instructure, on the other hand, acts as a processor and on behalf of the Customer. Instructure provides the software and technical infrastructure for Canvas LMS.

The Data controller and contracting party is Instructure Global Limited.[97] It is the controller according to the purposes mentioned in the Table 3 Instructure's data processing purposes. However, for the purposes outlined in the DPA and Global DPA, the customer acts as a controller with respect to the purposes and means it has determined.

A.7.3 Third Parties Involved in the Processing

Instructure conducts third-party security risk management program which include robust practices for backup, disaster recovery, and business continuity plans.[98] Additionally, when Instructure engages a third party (Sub-processor), substantially the same data protection obligations as set out in this DPA shall be imposed on that Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures, including measures substantially similar to the Instructure Security Specifications, in such a manner that the Processing will meet the Data Protection Laws and the requirements of this DPA.[99]

From the Privacy Notice, Instructure may share Customer's personal information with authorised third-party service providers for the sole purpose of providing you with their Products. It is stated that Instructure does not permit third-part service providers to use personal information shared with third parties service providers for advertising or marketing purposes, or for any other purpose other than in connection with the services they provide to Instructure. Additionally, Instructure does not sell or rent Customer's personal information to third parties.[100]

---

[97] Instructure, European Union Region Product Privacy Addendum, dated 28 June 2022, URL: https://www.instructure.com/policies/privacy/EU accessed 24 October 2025.
[98] Business Continuity & Disaster Recovery, page 6.
[99] Instructure Vendor Data Processing Agreement, page 5.
[100] Instructure, 'Product Privacy Policy' (Instructure) https://www.instructure.com/policies/product-privacy-policy accessed 24 October 2025.

Instructure's sub-processors are described in Section A.6.4.1.,

A.7.3.1 Sub-processors of Instructure's Canvas LMS

From the listed sub-processors in 'Instructure Third Party service provider guide' who support delivery of Instructure products and services included in the sub-processor list, the following sub-processors are relevant for this DPIA[101]:

Vendor	Description of the processing	Services	Data processed	Processing
Cloudflare, Inc. 101 Townsend St., San Francisco, CA 94107	Used for translations in Canvas LMS if enabled by Customer in their instance.	Canvas LMS	Any information in the web UI that is translated	Germany Netherlands USA
Amazon QuickSight EU: 38 Avenue John F. Kennedy, L-185 Luxembourg USA: 410 Terry Avenue North, Seattle, WA 98109-5210	Add-on service for Customers that purchase custom development processional services. With QuickSight, admin users can perform analytics from Canvas DAP through interactive dashboards, pixel-perfect reports, natural language queries and embedded analytics.	Canvas LMS (Professional Services)	All Customer Data stored in Data Access Platform.	Australia Canada Germany Ireland Singapore USA
Amazon CloudFront EU: 38 Avenue John F. Kennedy, L-185 Luxembourg USA: 410 T erry Avenue North, Seattle, WA 98109-5210	Content Delivery Network service which routes static and dynamic content to end-users of the Services.	Canvas Services	Services end-user encrypted IP address, static and dynamic content from the Services.	Global - Nearest edge server to the end-user.

[101] Instructure Third-party Service Provider Guide (last updated December 2024).

Looker (Google Cloud) 101 Church Street, 4th Floor, Santa Cruz, CA 95060, USA	This Vendor provides data visualisation services for in-application analytics (New Analytics & Admin Analytics). These analytic tools are used by Customers to analyse certain activities by their end-users. Primarily used for data caching for visualisation.	Canvas LMS	Canvas LMS username, short name, email address, SIS identification number, and Avatar URL, hierarchy data (i.e., account, sub account, course, section, students), dimensions and their columns (i.e., assignments, calendar events, collaborations), and, facts and their measures (i.e., Canvas activity log including page view and participation count).	Australia Canada Germany Ireland Singapore USA
Drieam BV Don Boscostraat 4, 5611KW Eindhoven the Netherlands	This Vendor provides certain services that are resold by Instructure.	Eduframe StudyCoach Portflow	Drieam may also retain certain information on your behalf, such as files and messages stored within the end-users Canvas LMS account.	Ireland
Visiarc AB PO Box 244, S-581-02 LINKÖPING, Sweden	This Vendor provides Smartsearch LTI as a product that is resold by Instructure. When a Canvas LMS user does a search the Smartsearch server relays the search results from	Smartsearch	When an end-user does a search the Smartsearch server relays the search results from Canvas LMS to the end-user's web browser using the LTI standard and OAuth2.	Europe USA

	Canvas LMS to the users web browser using the LTI standard and OAuth2.			
Blindside Networks Inc. 116 Albert Street, Suite 901, Ottawa, Ontario, K1P 563, Canada	Hosting provider for Canvas Conferencing services (Big Blue Button). This Vendor is only applicable if the Customer uses Big Blue Button or Canvas Conferences.	Canvas Conferences (BigBlueButton)	Identification data: name, user id, profile photo, IP Address. Collected when a user joins a virtual class. Attendance information: name, user ID, meeting ID, profile photo, content shared during session, IP address. Collected to provide attendance reports for session moderators. Analytics data: Name, Session content, Session interactions, browser, operating system. Collected to provide Session moderators with insights regarding your Session participation and attendance Audio recordings: Speech, Session content. Collected during sessions to offer live speech-to-text subtitles and transcriptions. Session recordings: likeness, speech, session content. Collected to store and index sessions for	Australia Canada Ireland USA

			later view. Used by session moderators for session insights. Used to improve the quality of the services and troubleshoot issues. Technical data: Name, User ID, Session interactions, IP address, browser, operating system, and audio quality score. Collected during a session for debugging purposes.	

Table 9 Sub-processors of Instructure's Canvas LMS

A.7.3.2 Joint controllership

According to three judgments of the European Court of Justice[102] parties can factually become joint controllers, even if the roles are unevenly distributed, and also if the party that is the customer does not have access to the personal data processed by the party that supplies a service.[103]

Joint controllership needs to be established on a factual basis and cannot be excluded if there is no contractual arrangement. Instructure cannot unilaterally determine its role as a data controller or processor simply by including such classifications in its contract terms. For example, Instructure may not legally assert that it is an independent data controller for all processing activities described in the agreement, nor claim to act as a data processor for specific categories of personal data if, in practice, it determines the purposes and means of processing, thus acting as a data controller. The actual role must be assessed based on the factual circumstances of the data processing activities, not solely on contractual labels.

According to the EDPB guidelines on joint controllership, parties may be considered ”joint controllers” when they take a common decision or when they take converging decisions about the purposes and essential means of the processing. The term ”converging decisions” is defined as decisions that ”*complement each other and are necessary for the*

[102] European Court of Justice, C-40/17, 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, C210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein versus Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388. See in particular par. 38-43. Also see: C-25/17, 10 July 2018, Tietosuojavaltuutettu versus Jehovah’s Witnesses — Religious Community, ECLI:EU:C:2018:551, par. 66-69.
[103] See par. 39 of the Schleswig Holstein Fan Page case and par. 69 of the Jehova’s Witnesses case: it is not necessary that the community had access to the personal data, or to establish that the community had given its members written guidelines or instructions in relation to the data processing.

processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing".[104] According to the EDPB, an important factor in determining whether there are converging decisions is whether the two entities' processing activities are "inextricably linked", in the sense that the processing in question "*would not have been possible without both parties' participation" in the processing operations*."[105]

Instructure follows the commands of the Education Institutions which retain independent control over the purpose and means of the processing of personal data such as metadata.[106]

With regard to the processing of Account Data, Customer and Instructure are both independent Controllers (and not joint Controllers).[107] An independent controller is an entity that alone determines the purposes and means of processing personal data. The ECJ has clarified that a controller is not defined by formal designation (such as a contract), but by the factual influence over the purposes and means of processing.[108]

A.8 Interests in Data Processing

This section outlines the (potential) interests of Instructure and the educational institutions. However, it does not address the fundamental data protection rights and interests of the data subjects. An analysis of how these rights interact with and relate to the interests of Instructure and the educational institutions is provided in Part B of this DPIA.

A.8.1 Interests of Educational institutions

Educational institutions have several legitimate interests in adopting Instructure's Canvas Learning Management System (LMS) as part of their digital infrastructure. Educational institutions in the Netherlands are increasingly exploring the use of Software-as-a-Service (SaaS) platforms such as Canvas LMS, with its user base steadily expanding. This growing interest underscores the institutions' motivation to adopt the system while also prioritising the completion of a DPIA to ensure responsible and compliant implementation. Additionally, it provides the ability for students to use the platform in which the enrolment, engagement, and progress of the students is provided and can be followed.

Canvas includes analytics and reporting tools that allow institutions to monitor student engagement and performance, identify at-risk students early, and make data-informed decisions to improve educational outcomes.[109]

[104] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0, Adopted on 2 September 2020, p. 3, URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.
[105] Idem.
[106] Data Processing Agreement (College Agreement), page 4.
[107] https://www.instructure.com/policies/data-processing-addendum.
[108] European Court of Justice, Case C-683/21, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija, ECLI:EU:C:2023:949 https://curia.europa.eu/juris/document/document.jsf?text=&docid=280324&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7438261.
[109] Instructure, 'Canvas LMS for Higher Education' (Instructure) https://www.instructure.com/higher-education accessed 24 October 2025.

The platform also plays a role in supporting regulatory and institutional compliance, including data retention and accessibility requirements. Canvas integrates with existing identity and access management systems, helping institutions safeguard access and ensure secure user authentication. Furthermore, its ability to integrate with a wide range of educational technologies, student information systems (SIS), and third-party tools adds scalability and flexibility across different educational environments. By leveraging such a comprehensive system, institutions can also enhance their digital readiness and reputation, appealing to both students and faculty in an increasingly competitive educational landscape. Finally, the use of a cloud-based LMS like Canvas can lead to cost efficiencies by consolidating disparate systems and reducing infrastructure maintenance needs. These combined interests reflect the strategic value of adopting Canvas to fulfill both pedagogical and operational objectives within educational institutions.

A.8.2 Interests of Instructure

Instructure, as the provider of the Canvas LMS, has a strategic interest in expanding its footprint within the European education sector. Demonstrating compliance with the General Data Protection Regulation (GDPR) is critical to supporting this objective. Canvas LMS is widely used to facilitate digital teaching, learning, and administrative processes in schools and universities, which inherently involves the processing of personal data, including student identifiers, academic performance, and communication records. Instructure's ability to clearly evidence GDPR compliance, including transparency in data flows, robust contractual safeguards (such as a Data Processing Agreement), and appropriate technical and organisational security measures, is essential for gaining and maintaining the trust of European educational institutions. Compliance strengthens Instructure's eligibility to enter into agreements with public sector institutions that are subject to stringent data protection requirements and procurement rules. Furthermore, by aligning Canvas LMS with GDPR obligations, such as data minimisation, purpose limitation, and support for data subject rights, Instructure not only mitigates legal and reputational risks but also positions itself as a privacy-conscious and reliable EdTech partner in the European market.

A.9 Processing Locations

The GDPR restricts transfers of personal data to countries outside the EEA unless adequate protection is ensured. This can be achieved through an adequacy decision by the European Commission or, in its absence, by using safeguards such as Standard Contractual Clauses (SCCs). Multinational organisations may also use Binding Corporate Rules (BCRs) for intra-group data transfers. Instructure does not have BCRs, but intracompany SCCs between Instructure Inc and Instructure Global.

Intracompany SCCs are legitimate to transfer personal data based on Instructure's self-assessment, and without obtaining the EDPB's approval decision as needed for the BCR to have a long-term compliance framework.[110]

A.9.1 Data Residency

To support data residency and compliance requirements such as the GDPR, institutions can choose the AWS region where their root account, and therefore their data, will be hosted. There are multiple geographically separate sites and Availability Zones. Instructure explains that they help to make Canvas application be fully redundant and having capacity capabilities offered by AWS.[111]

Regions are paired for resilience, meaning that data hosted in, for example, Dublin, is backed up in Frankfurt. This approach ensures that data never leaves its designated geographical boundary without explicit intent. Moreover, disaster recovery is achieved by maintaining region-paired backups. These backups are not only stored, but are also replicated using region-specific AWS infrastructure, which avoids trans-regional data movement that might raise compliance concerns.

For international clients including the EU clients, Instructure uses EU Central AWS region. It is located in Germany.[112] Instructure explained:

'European customers can choose to can choose to have Canvas hosted either at the AWS hosting center in Dublin or Frankfurt/Main (EU Central, Germany). However, most of our German Canvas customers decide to go with Frankfurt/Main as their server location. This allows clients in Germany to reassure their users (students, parents, staff) that their data is being saved and managed within Europe. Specific customer names are not listed in the provided context, but the majority of German customers opt for the Frankfurt/Main region for hosting.'[113]

A.9.2 Data Privacy Framework (DPF)

An adequacy decision means that the country in question has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay. With the

[110] European Data Protection Board, 'Approved Binding Corporate Rules' (European Data Protection Board) https://www.edpb.europa.eu/our-work-tools/accountability-tools/bcr_en accessed 24 October 2025.
[111] Canvas LMS Architecture overview.
[112] Canvas LMS Architecture Overview, page 4.
[113] Instructure's feedback from the 16th of September 2025.

exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).

On 10 July 2023, the European Commission issued a renewed adequacy decision for the US. As a result, the US is considered to have an adequate level of data protection, and European organisations are allowed to transfer personal data to US based cloud service providers without any additional protective measures, provided that the importing organisations have registered themselves for these specific services, as a participant in the Data Privacy Framework.

As mentioned in Privacy Data Sheet, Instructure is self-certified under the EU-US Data Privacy Framework.[114]

The new EU-U.S. data transfer framework does not limit the authority of U.S. law enforcement agencies to compel disclosure of personal data belonging to Dutch customers under the U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data). This legislation was specifically designed to enable access to data stored in data centers located outside the United States, including within the EU. The CLOUD Act extends the jurisdiction of U.S. courts to all data controlled by U.S.-based companies, regardless of where that data is physically stored.

As the European Parliament notes in its opinion on the Data Privacy Framework:

"the EO [Executive Order from the President, added by Privacy Company] does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements.". [115]

A.9.3 Standard Contractual Clauses

For educational institutions whose use of Instructure's Canvas LMS involves the transfer of personal data from the European Economic Area (EEA), the United Kingdom, or Switzerland to countries outside these jurisdictions, Instructure relies on established legal mechanisms to ensure adequate protection of personal data. Instructure primarily uses the Standard Contractual Clauses (SCCs). These clauses are approved by the European Commission as the legal basis for such transfers. These clauses are incorporated into its DPA and serve to safeguard data when it is transferred to Instructure, Inc. in the United States or other non-EEA affiliates. Instructure has implemented internal policies and security controls to support the lawful and secure processing of personal data in compliance with the GDPR.[116]

According to the EDPB (European Data Protection Board) guidelines, *'the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined. The data exporter and importer need to ensure that additional clauses cannot be construed*

[114] U.S. Department of Commerce, 'Data Privacy Framework Participant List' (U.S. Department of Commerce) https://www.dataprivacyframework.gov/list accessed 24 October 2025.
[115] European Parliament, 'Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-U.S. Data Privacy Framework' (European Parliament, 11 May 2023) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023IP0204 accessed 24 October 2025.
[116] Instructure, 'Data Processing Addendum' (Instructure) https://www.instructure.com/policies/data-processing-addendum accessed 24 October 2025.

in any way to restrict the rights and obligations in the SCCs or in any other way to lower the level of data protection.'[117]

Instructure also regularly assesses the legal landscape in destination countries and, where required, implements supplementary measures to ensure an equivalent level of protection as required by the GDPR and the Schrems II decision.

A.9.4 Data Transfer Impact Assessment

Instructure states that a primary method of data transfer for education institution customers is the DPF.[118] In addition to the DPF, customers can also choose SCC as was discussed in the previous section.

Instructure has conducted TIA's (Transfer Impact Assessments) for the following countries: Egypt, Jordan, Philippines, United States. It is a mechanism to assess the level of protection in third countries of destination and the need for additional safeguards. By doing the assessments on the mentioned countries, Instructure ensured that the following points are considered:[119]

1. Is there a transfer of personal data?
2. Is it necessary to carry out a TIA?
3. Who is responsible for the TIA?
4. What is the scope of the TIA, in particular considering onward transfers?
5. Is the transfer compliant with the principles of the GDPR?

[117] European Data Protection Board, 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data' (European Data Protection Board, 18 June 2021) https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf accessed 10 October 2025, page 23.

[118] From the Instructure's response to SURF questions on the 28th May 2025.

[119] Commission Nationale de l'Informatique et des Libertés, 'Practical Guide – Transfer Impact Assessment (TIA)' (CNIL, January 2025) https://www.cnil.fr/sites/cnil/files/2025-01/guide_tia.pdf accessed 24 October 2025. - Transfer Impact Assessment (TIA): the CNIL publishes the final version of its guide 31 January 2025.

A.10 Legal and Policy Framework

ePrivacy Directive significantly affects how organizations process personal data in the context of electronic communications. It complements the GDPR providing more specific rules around privacy in the digital environment. This section elaborates in more details.

A.10.1 ePrivacy Directive

Certain rules from the current ePrivacy Directive apply to the storage of information on, and retrieval of that stored information from, browsers with pixels and cookies and similar technologies such as tracking pixels. Consent is required prior to the retrieval or storage of information on the devices or browsers of end users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or the necessity for the technical transmission of information.

The current ePrivacy Directive also includes rules on the confidentiality of data from the content and on communication behaviour. Article 5(1) obliges Member States to guarantee the confidentiality of communications and related traffic data via public communications networks and publicly available electronic communications services. Article 6(1) obliges providers of publicly available telecommunications services to erase or make the traffic data anonymous as soon as they are no longer needed for the purpose of the transmission of the communication.
Although the confidentiality rules in the ePrivacy Directive originally only covered classic telephony and internet providers, the scope was expanded significantly. Since the European Electronic Communications Code (EECC) became applicable law (21 December 2020)[120], the confidentiality rules apply to all over-the-top communications services.

The Regulation (EU) 2021/1232 (“Interim Regulation”) lays down temporary and strictly limited rules derogating from the confidentiality obligations in Article 5(1) and 6(1) of the Directive, with the sole objective of enabling providers of online communications services (like webmail and messaging platforms) to use specific technologies for the processing of personal and other data to the extent strictly necessary to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services. These derogations were initially in effect until 3 August 2024. [121]

A.10.2 Transparency report

Instructure publicly publishes a yearly transparency report to provide information regarding requests submitted by law enforcement, judicial authorities, and government agencies from around the world. It is stated in the report that for Instructure, transparency is a foundational principle of our Privacy Program, and it is ensured that any requesting agency has the legal authority and follows the appropriate process before any data is disclosed.[122]

---

[120] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, L 321/36, 17 December 2018, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN.
[121] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC for the purpose of combating online child sexual abuse, COM/2023/777 final, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A777%3AFIN.
[122] Instructure, ‘Transparency Report – 01/01/24 – 06/30/2024’ (Instructure Community, 12 August 2024) https://community.canvaslms.com/t5/Privacy-Articles/Transparency-Report-01-01-24-06-30-2024/ta-p/611632 accessed 24 October 2025.

Instructure's Transparency Report for the first half of 2024, published on August 12, 2024, provides insights into government requests for customer data received during this period. The report underscores Instructure's commitment to data protection and transparency. Instructure received four subpoenas or equivalent legal orders, impacting 122 users. No search warrants, international requests, or national security requests were reported.

Instructure informed SURF that none of the received requests in 2024 were for EU countries.[123] Instructure works to update this information for 2025.

Under the GDPR, any transfer of EU personal data to non-EU countries must ensure an 'essentially equivalent' level of protection. The CLOUD Act allows the United Stated (U.S.) authorities to compel access to data held by the U.S. companies, even if that data is stored in the EU. While Instructure's transparency and limited number of requests are positive indicators, there is a possibility of the risk: if U.S. authorities can access EU customers' data under U.S. law, this may still pose compliance challenges under the GDPR.

[123] Comments to the DPIA Part A by Instructure.

A.11 Retention Periods

A controller may retain personal data as long as it is necessary for the purpose for which it was collected, the GDPR states (Article 5(1)(e) GDPR). After that, the controller must destroy the data, unless the controller is obliged to keep it longer, for example because it is provided for in a law. The latter should be set out in the processor agreement or otherwise similar agreement. This section describes the retention periods Instructure applies in its role as data processor and data controller.

Instructure lists its retention periods in the Business Continuity & Recovery Plan.[124] This is a response plan that used as a guide during incidents. Additionally, SURF was informed that the Canvas LMS system regularly creates full database snapshots, which are encrypted and stored in Amazon.[125] You will find further explanation of the Amazon storage in the next section.

A.11.1 Amazon S3 storage

Canvas uses Amazon S3 storage for the data backups.[126] All backup data stored in Amazon S3 is encrypted at rest and in transit, and AWS data centers adhere to stringent security standards, including ISO 27001, SOC 2. Access to backup data is restricted to authorised personnel under controlled, audited conditions. The use of Amazon S3 enables Canvas to offer reliable disaster recovery capabilities while maintaining compliance with data protection obligations.

Canvas backups include the following types of data[127]:

- **Database Data**: Instructure updated the backup retention policy in September 2025.[128] Full database backups (snapshots) are retained now for up to 4 months, with daily, weekly, and monthly snapshots. Point-In-Time Recovery (PITR) is available for up to 4 months of rolling backup data. In Instructure's previous policy 12 months were a retention period.
- **Object Data**: Files, documents, uploaded media, and other static assets are recoverable for a period of 4 months.
- **Media and Metadata**: Canvas Studio backups include media, metadata, and analytics, which can be extracted via API.
- **Student Pathways / ePortfolios**: Retained for 35 days.
- **Grade Exports and Learner Artifacts**: Grade exports and individual learner artifacts with teacher annotations and feedback in PDF format.
- **Standards-Based Content Exports**: IMS Global certified Common Cartridge packages (.imscc).
- **Course Data and Content**: All past and current course data and content are maintained and accessible online.
- **Source Data for Analytics**: Canvas data 2 provides bulk access to source data for data warehousing and learning analytics.

[124] Business Continuity and Disaster Recovery Plan, September 2025.
[125] Instructure communication to SURF (question about retention periods) from the 17th April 2025.
[126] LMS Architecture document #76, page 3.
[127] As communicated in Instructure's response to SURF's questions from the 17th April 2025.
[128] Business Continuity and Disaster Recovery Plan, September 2025, Page 24.

In Instructure's documentation, there were no disctinction made between the storage of database data and object data. However, Instructure explained the difference between the storage of database data and object in Amazon S3 storage very clearly:

'In S3 (file objects), every file is essentially versioned. So if you upload a file, thats version 1, if you later re-upload that file, that's version 2. If you delete it, that's actually version 3. What we do is hold on to those non-active versions for 1 year, but unlike a database backup, at no point is a "copy" ever made, meaning there is only one file object reference, these references is what we're referring to. Which essentially represent a soft delete. If we get a request to say, delete all of a users documents, that's considered a hard delete and those are gone forever, no backups, no recovery, literally gone forever.

Files are only discoverable with the accompanying metadata present in the database. Without that data, not only is there no identifying data but the file itself becomes undiscoverable without previously having had access.'[129]

[129] Instructure's answer to SURF questions from the 16th November 2025.

A.11.2 Backup Retention

Canvas LMS implements a robust data backup and recovery strategy to ensure data durability and business continuity.

In a previous Business continuity and Disaster recovery documentation, it was mentioned that in addition to real-time replication across multiple geographic locations within the customer's designated region, to ensure a very low Recovery Point Objective (RPO), Instructure retains comprehensive database backups (snapshots) for a rolling period of 12 months. Specifically, this includes 7 daily snapshots, 4 weekly snapshots, and 12 monthly snapshots. This backup structure enables Point-In-Time Recovery (PITR) of data up to 4 months old and allows for monthly data restores for data aged between 5 to 12 months. Additionally, object data, such as user-uploaded files, documents, and multimedia content, is recoverable for up to one year following deletion or modification. This layered backup strategy supports data integrity and aligns with best practices for disaster recovery and compliance with applicable data protection regulations.[130]

In the meeting with SURF, Instructure mentioned that their policy was updated in September 2025.[131] The maximum retention period became 4 months.

A.11.3 Back-up and Deletion Policies

Canvas LMS implements multiple backup strategies as part of its business continuity and disaster recovery planning. These backups are performed regularly across infrastructure levels, such as database snapshots, transaction logs, and S3-based file backups, and are retained for fixed durations, which are addressed separately in A.11 Retention Periods. This guarantees data durability in the face of failures and enables both full and partial restoration in the event of data loss or operational errors.

When a data subject exercises their right to erasure under GDPR (for instance, a student requesting the permanent deletion of a discussion post they made), Canvas performs a deletion from the active production database. This deletion process typically begins as a soft delete, where data is marked as deleted and hidden from user view, and is later finalised via hard delete routines that permanently remove the data from the live environment. In cases specifically tied to GDPR compliance, Instructure stated that support agents can trigger these more thorough deletions using internal tooling.

However, our technical assessment identified significant limitations in how these erasure requests are handled in relation to backup data. Standard deletion processes do not automatically propagate to historical backups. Previously captured versions of deleted data remain within backups for the duration of the defined retention window, with no automated mechanism to selectively purge specific personal data from these backups following erasure requests.

Instructure has confirmed one limited technical control for backup remediation: when a production shard requires restoration from backup (for example, following catastrophic database failure), their runbook includes re-running the *user_scrubber* utility. This process

[130] Business Continuity & Disaster recovery, page 16.
[131] Business Continuity and Disaster Recovery Plan, September 2025.

reapplies user account deletions to the restored data to ensure that previously deleted user accounts do not reappear following restoration.

This mitigation only addresses complete user account deletions and does not extend to granular erasure requests for specific categories of personal data. Under GDPR Article 17, data subjects have the right to request erasure not only of their entire account, but also of specific personal data relating to them (such as particular submissions, communications, or profile attributes). The current technical implementation does not support selective purging of such data from backups.

Part B Assessment of Lawfulness of Data Processing

The second part of the DPIA assesses the lawfulness of the data processing. This part contains an assessment of the legal grounds of both the educational institutions and Instructure the processing of special personal data, the application of purpose limitation, the necessity of the processing and the application of data subject's rights.

B.1 Legal Basis from the contractual perspective

To comply with the GDPR, the processing of personal data must be based on one of the legal bases outlined in Article 6(1) of the Regulation.

Before addressing the applicable legal bases for the processing, it is first necessary to outline the context in which the processing occurs. This includes not only defining the roles of the parties involved but also examining the contractual framework that governs their relationship.

B.1.1 Contractual context and role determination

According to the DPA between Instructure and education institutions, and Global DPA, the Customer (education institutions) is the controller for Customer personal data. The controller determines both the purposes and the means of the processing.

Instructure acknowledges that the Customer retains full ownership of all Customer Personal Data. Instructure, on the other side, is the controller for the personal data for the purposes mentioned in the Section Data Processing Addendum (Global DPA).

The same terms outlined in the Educational Institution's DPA apply in this context: Instructure will process personal data solely on behalf of the Customer and strictly in accordance with the Customer's instructions. From the contractual perspective presented in the DPA with educational institutions and Global DPA, there is a clear separation of the roles' responsibilities according to the purposes that were determined by the controller and/or processor.

In the Table 4 Instructure's data processing purposes, it is observed that Instructure processes personal data primarily to manage customer accounts and communications, provide support services, collect user feedback, fulfil legal obligations, and ensure the security and proper functioning of the Canvas LMS. This includes activities such as billing, responding to user requests, improving system performance using anonymized data, and preventing abuse or policy violations. For these specified purposes, Instructure acts in the capacity of a data controller and determined the means and purposes of the processing independently from the Customers (education institutions). The analysis of the DPAs and other agreements for the processing according to these purposes are assessed in section .

Additionally, the sufficient clarity is provided from the Global DPA. The section about the 'Customer for the consents for the processing of customer personal data' underscores that the responsibility for obtaining all necessary consents and complying with data protection

laws lies with the Customer.[132] Instructure relies on the Customer's assurance that such compliance has been met. If the Customer fails to meet these obligations, they must inform Instructure without delay and may be held liable for any resulting claims or damages. Such a failure constitutes a serious breach of the DPA.

From a legal perspective, the actual allocation of roles must be assessed based on the specific facts and circumstances. During this DPIA, SURF submitted the DSARs to Instructure. In the section , SURF observed a comprehensive overview where for every data subject, the report included communication channels, page views, asset user accesses, pseudonyms, attachments, submissions, discussion entries, enrolments, user metadata.

Even though the personal data was received for every data subject, the report lacked purposes for data processing, categories of personal data concerned, recipients of data disclosure, and others mentioned in section 40. Additionally, the DSAR responses lack direct access to the actual content entered by users such as assignment submissions, quiz answers, announcements, syllabus details, and page content. Although actions related to this content are logged via page views, the content itself is not presented in a clear, readable format. Additionally, specific peer review comments are also not included in detail.

The missed metadata can qualify as personal data if it can be linked (directly or indirectly) to an identifiable individual.[133]

Overall, Instructure defines roles and responsibilities; however, further clarification is needed on the specific types of data it processes in its capacity as either a processor or a controller for various purposes.

B.2 Legal grounds

In this section, before addressing the specific examples applicable to Canvas LMS, it is important to note that all available options and approaches in a broader context are examined. The following references are provided to illustrate possible scenarios and not directly applicable to actual processing activities of Canvas LMS yet.

The institutions are responsible for the processing operations that fall under educational planning, providing materials, organising the education environment and supporting processing activities that are necessary to enable these purposes.

Article 6, paragraph 1(e) of the GDPR (Task carried out in the public interest).

Institutions have a legal obligation to perform a public task, namely the organisation of education.

In order to perform this task, institutions must draw up plans and schedules, and the processing of personal data is necessary to do so. To invoke this basis, institutions must

[132] Instructure, 'Data Processing Addendum' (Instructure) https://www.instructure.com/policies/data-processing-addendum accessed 24 October 2025.
[133] Meta Platforms Inc. v Bundeskartellamt (Case C-252/21) [2023] ECLI:EU:C:2023:537.

carry out a necessity test to demonstrate that the processing is necessary for the proper performance of their public task. For the processing of data that is not necessary for their public task, institutions may be able to apply one of the following bases. [134]

Article 6, paragraph 1(a) of the GDPR (Consent)
To process users' personal data such as page views where it the information may be accessed by the subject and related metadata about the interactions. The institution requests consent from the user via the platform. Among other things, this consent must be freely given to be valid as a basis under the GDPR. This means that the user must not suffer any adverse consequences from refusing consent. Institutions must therefore offer users who do not wish to share their detailed information about the interactions in Canvas LMS if they wish to use this basis.

Article 6(1)(b) of the GDPR (Performance of a contract)
Processing that is not necessary for the performance of a public task may be necessary to perform a contract with students (e.g. an education contract) and/or employees (e.g. an employment contract). Here too, institutions must carry out a necessity test to demonstrate that the purpose of the contract cannot be achieved without the processing of personal data in question.[135]

Article 6(1)(f) of the GDPR (Legitimate interest)
Processing that is not necessary for the performance of a task carried out in the public interest may be necessary for the purposes of the legitimate interests pursued by the institution. In order to use this basis, it must be assessed whether institutions (1) have a legitimate interest, (2) the processing is necessary to pursue this interest, and (3) whether the interests of the institution outweigh those of the data subjects.[136]

B.2.1 Legal ground from the Instructure perspective

This section will look at the legal grounds of data processing from the Instructure perspective. When acting as a processor, Instructure is instructed by the educational institution and operates on behalf of that organization. The legal basis for processing used by the institution also applies to Instructure in its role as a processor, and an educational institution

Under the agreement with educational institutions, Instructure is permitted to process Customer Data for purposes where it acts as a data controller. The purposes that Instructure is allowed to process personal data as a controller are mentioned in Table 3 Instructure's data processing purposes. However, it was not determinable which types of personal data are processed for which specific purposes.

[134] Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW), as amended on 1 January 2025 https://wetten.overheid.nl/BWBR0005682/2025-01-01 accessed 24 October 2025.
[135] *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) of the GDPR in the context of the provision of online services to data subjects*, EDPB
[136] Autoriteit Persoonsgegevens, *'Grondslagen AVG uitgelegd'* (Autoriteit Persoonsgegevens) https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-gerechtvaardigd-belang accessed 24 October 2025.

B.2.1.1 Consent

Consent can make processing of personal data lawful, if and to the extent the purposes are specific (Article 6 (1) (a) GDPR). When processing has multiple purposes, consent should be asked for all of them separately. Article 4 (11) GDPR, defines 'consent' as meaning 'any freely given, specific, informed and unambiguous indication of the data subject's wishes y which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Educational institutions should refrain from asking for consent from students and employees for the processing of their personal data. In view of the imbalance of power between students and educational institutions, consent should seldom be given freely.[137] Employees and students may not be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences.

According to the Instructure's privacy notice from Section 2, it processes personal information and personal data which was identified in the Table 5 List of Personal Data for the purposes identified in the agreement with education institutions. For the purposes other than the purpose for which this information was collected, Instructure provides the notice in advance of the new processing and obtain consent if required.[138] From the information presented to SURF and public documentation, it is difficult to derive whether the consent is obtained from the admin of the educational institution or on behalf of the users.

For end users affiliated with an educational institution or company that utilizes Instructure's products, the institution is responsible for determining how personal information is managed. Accordingly, the use of personal information (as written in privacy policy, but applicable to personal data according to the GDPR) is governed by the organization's privacy notice. Instructure's privacy notice provides transparency regarding Instructure's own privacy practices.[139] This is the information that should be provided to admins and end users to enable the users to give the informed consent.

The fact that education and research institutions are public sector organisations also makes it difficult to rely on consent for processing. In the context of Recital 43 of the GDPR, the EDPB explains: "*whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities*."[140]

---

[137] 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 (General Data Protection Regulation) [2016] OJ L119/1, recital 49.
[138] Instructure, 'Product Privacy Policy' (Instructure) https://www.instructure.com/policies/product-privacy-policy accessed 24 October 2025.
[139] Instructure, 'Product Privacy Policy' (Instructure) https://www.instructure.com/policies/product-privacy-policy accessed 24 October 2025.
[140] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (EDPB, 4 May 2020) para 3.1.1 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en accessed 24 October 2025.

The consent from educational institutions is needed when it comes to requesting Customer's consent for choosing third parties. '*With your consent or at your direction. As noted, we may share information other than as described in this Privacy Notice with your consent, or at your specific direction, for example, if you choose to use the Products with social networking platforms (Facebook, YouTube, Twitter, etc.).*'[141] There is the shortage of the information regarding which type of personal data is being processed according to the legal ground as consent. Consent must be freely given, specific, informed, and unambiguous. the original consent does not cover additional processing activities.

In addition, according to Privacy notice, obtaining the Customer's (educational institution's) consent is necessary prior to soliciting feedback regarding Instructure's products, including through requests to participate in surveys or questionnaires. Instructure feedback system will be further analyzed in the next session in the Part C.

Cookies

Instructure provides clear information about the cookies used in its services. As was described in the Canvas LMS Cookie Notice, all cookies are first-party, and they are set either by Instructure or its authorized partners. Cookies fall into three categories: strictly necessary, functionality, and analytics. Users can manage cookie preferences through their browser settings. They may also follow their institution's policies. The cookie notice also includes contact details for users with questions or concerns.

Additionally, cookie notice mentions that customed can change your browser settings to control how cookies are handled.[142] For example, there are options:

- Block all cookies.
- Choose to be asked (prompted) before accepting cookies from any website.

However, Instructure informs that if customers block all cookies (including essential ones that are needed for the website to work properly) some parts of the website may stop working correctly or may not work at all. So, while there is a control over cookies, completely disabling them could affect the site's functionality. If the site becomes unusable or significantly degraded when cookies are refused (especially non-essential ones), the user's ability to freely choose is compromised.

Instructure uses the cookies which are mentioned in Table 5 Relevant Cookies as described in the Cookie Notice of Instructure, however particular cookies found by SURF such as inst-fs-session; inst-fs-session.sig ; log_session_id ;pseudonym_credentials are not mentioned in the Cookie notice.[143] Therefore, the legal ground for data processing as consent cannot be exercised by Instructure, since this information was not received by educational institutions.

[141] Instructure, 'Product Privacy Policy' (Instructure) https://www.instructure.com/policies/product-privacy-policy accessed 24 October 2025.
[142] Instructure, 'Canvas Learning Management System Cookie Notice' (Instructure). https://www.instructure.com/policies/canvas-lms-cookie-notice accessed 24 October 2025.
[143] *See* Table 7 Found Cookies during Technical Research.

B.2.1.2 Necessity for the performance of the contract

The legal ground of necessity for the performance of a contract (Article 6(1)(b) GDPR) is limited to situations where organisations have a contract with specific data subjects, and the processing is strictly necessary to perform the contract with these individuals.

The legal basis 'necessity for the performance of a contract' is therefore not applicable in this context, as the contract is not concluded with the data subject (the individual user), but rather with the educational institution. Since the data processing is not necessary for the performance of a contract with the data subject, this legal basis cannot be relied upon to justify the processing of their personal data.

B.2.1.3 Necessity to comply with a legal obligation

Article 6 (1) (c) GDPR reads: *"processing is necessary for compliance with a legal obligation to which the controller is subject"*. There are four conditions that need to be met for this legal basis to be relied on:[144]

- the legal obligation must be defined by EU or national law to which the controller is subject;
- these legal provisions must establish a clear and specific obligation to process that personal data;
- these provisions must at least define the purposes of the processing;
- this obligation should be imposed on the controller and not on the data subject.

If these criteria are not fulfilled, the processing operation cannot rely on the legal ground 'to comply with a legal obligation'.

B.2.2 Legal grounds for educational institutions

This section assesses the potential legal bases for educational institutions for using Canvas LMS.

When educational institutions use Canvas LMS to deliver education, the processing of personal data can be justified under several legal bases according to the GDPR, including:

- The necessity for performing a task carried out in the public interest (Article 6(1)(e)), such as providing publicly funded education.
- The necessity of performing a contract (Article 6(1)(b)), such as agreements with enrolled students or employment contracts.
- In certain limited cases, legitimate interests (Article 6(1)(f)) of the organisation, where such interests are not overridden by the rights and freedoms of the data subjects.

These organisations do not rely on the legal bases of protecting vital interests or complying with a legal obligation when using Canvas LMS, as those bases are not applicable to the standard educational use of the platform.

[144] European Data Protection Board, 'Process Personal Data Lawfully' (2025) https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en accessed 24 October 2025.

B.2.2.1 Consent

Consent can make processing of personal data lawful, if and to the extent the purposes are specific (Article 6(1)(a) GDPR). When the processing has multiple purposes, consent should be asked for all of them separately. Article 4(11) GDPR, defines 'consent' as meaning 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. According to recital 42 of the GDPR, consent cannot be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. To ensure that consent is freely given, consent should not be relied upon to provide a valid legal ground for the processing of personal data where there is a clear imbalance between the data subject and the controller.

Educational institutions should refrain from asking for consent from students and employees for the processing of their personal data. In view of the imbalance of power between students and universities, and employees and employers, consent can seldom be given freely.[145] Employees and students may not be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences.

According to the DPA, Instructure puts the main responsibility on the customer to obtain consent. The controller (Customer) bears full responsibility for ensuring that all necessary consents and notices have been obtained before any personal data is processed by Instructure. If the Customer fails to do so, and this results in harm or liability for Instructure, the Customer must accept full legal and financial responsibility. This aligns with the principle in data protection law that the controller determines the legal basis for processing and ensures its compliance. '*Customer represents, warrants, and covenants that it has complied with all applicable Data Protection Laws, including without limitation providing all notices and obtaining all consents and rights necessary under applicable Data Protection Laws for Instructure to Process any Customer Personal Data in its's provision of the Services*.'[146]

For example, an educational institution may include a clause in the student enrollment agreement stating that students are required to use the Canvas LMS. By enrolling, students are deemed to consent to all data processing necessary for the use of Canvas, as it is the platform used for submitting assignments and accessing course content.

Even though the clause in the DPA assumes that the consent is obtained properly: it does not prove that the consent was: freely given, informed, specific, or unambiguous. Generally, instructing the controller to obtain 'consent' from the end-users is not a legal basis according to the GDPR. According to Article 28 (3) (a): the processor shall process personal data only on documented instructions from the controller. If Instructure insists on consent, it may be overstepping its role and potentially assuming controller-like responsibilities.

---

[145] Recital 49 of the GDPR: "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case* ***where there is a clear imbalance between the data subject and the controller****, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.*"

[146] Instructure, 'Data Processing Addendum' (2025) https://www.instructure.com/policies/data-processing-addendum accessed 24 October 2025.

B.2.2.2 Necessity for the performance of a contract

The legal ground of necessity for the performance of a contract (Article 6 (1) (b) GDPR) is limited to situations where organisations have contract with specific data subjects (such as an employment contract or an education agreement), and the processing is strictly necessary to perform the contract with such individual data subjects. The European Data Protection Authorities explain: *"The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. Thus, this ground can never be invoked by a party that does not have its own contract with that individual."*[147]

If controllers want to rely on the ground of performance of a contract, the processing must pass the necessity and proportionality tests. In particular, the controller must assess whether the purpose for which the personal data are processed cannot reasonably be achieved in another way which is less prejudicial to the persons involved in the processing of personal data.[148] The CJEU has a strict interpretation of the 'necessity' requirement. In order for the processing of personal data to be regarded as necessary for the performance of a contract, within the meaning of that provision, the processing must be *"objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject."*[149] The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur.[150] In the case of Meta vs Bundeskartellamt the CJEU considers: *"The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor ... is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives."*[151]

The legal ground of contract cannot be invoked by organisations for the processing of personal data of data subjects that do not have a contractual relationship with that organisation. Furthermore, the educational institutions cannot invoke the legal ground of contract for the processing of personal data for purposes that are not necessary for the performance of the contract with each individual data subject.

If the processing is not necessary to deliver what the contract promises, then an educational institutions cannot rely on the contract to justify that processing. It must find a different legal basis such as consent or legitimate interest.

One of the mentioned legal obligations stemming from the contractual obligation that stem from the DPA agreement with educational institutions is that the processor must ensure

[147] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, paragraph 26 and 30.
[148] ABRvS 20 September 2017, ECLI:NL:RVS:2017:2555.
[149] CJEU 4 July 2023, ECLI: EU:C:2023:537 (Meta vs Bundeskartellamt) paragraph 98.
[150] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, nr. 13. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.
[151] CJEU 4 July 2023, ECLI: EU:C:2023:537 (Meta vs Bundeskartellamt) paragraph 99.

that each subprocessor is bound by data protection obligations. Upon request, the processor must provide the education Institution with copies or relevant sections of these subprocessor agreements.[152]

B.2.2.3 Processing is necessary for a task in a public interest or for the legitimate interests of the controller or a third party

Article 6 (1) (e) GDPR reads*: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"*.

It follows from the CJEU ruling Meta vs Bundeskartellamt that a task of public interest within the meaning of Article 6(1)(e) GDPR is not sufficient as a basis for data processing in itself. Lawful processing of personal data on the basis of Article 6(1)(e) GDPR presupposes not only that a task of public interest is thereby performed, but also that the processing is based on EU law or on Member State law to which the controller is subject, and that that legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued (Article 6 (3) GDPR).

In the situation of Canvas LMS, this ground is not valid. Even when used by public educational institutions, it is essentially a procured service, not an activity mandated by law in the exercise of public authority.

[152] DPA agreement with an MBO institute, article 11 (1) DPA.

B.3 Purpose Limitation

The principle of purpose limitation is that data may only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR not be considered to be incompatible with the initial purposes" (Article 5 (1)(b) GDPR). Essentially, this means that the controller must have a specified purpose for which he or she collects personal data and can only process these data for purposes compatible with that original purpose.

According to the EDPB both purpose limitation and data minimisation principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis. *"Technological advancements make it possible for controllers to easily collect and process more personal data than ever before. As a result, there is an acute risk that data controllers may seek to include general processing terms in contracts in order to maximize the possible collection and uses of data, without adequately specifying those purposes or considering data minimisation obligations."*[153]

The predecessor of the EDPB, the Article 29 Working Party, has previously stated: *"The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail - usually not meet the criteria of being 'specific'."*[154]

Data controllers must be able to prove, based on Article 5(2) of the GDPR, that they comply with the principle of purpose limitation (accountability).

Instructure is a separate controller for the purposes mentioned in the Table 3 Instructure's data processing purposes:

- to manage customer accounts and communications;
- provide support services;
- collect user feedback;
- fulfil legal obligations;
- and, ensure the security and proper functioning of the Canvas LMS.

These purposes include activities such as billing, responding to user requests, improving system performance using anonymized data, and preventing abuse or policy violations. For these specified purposes, Instructure acts in the capacity of a data controller and determined the means and purposes of the processing independently from the Customers (education institutions). Additionally, according to the CJEU held in the same judgment that

[153] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Adopted on 9 April 2019, p. 5-6. URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

[154] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), p. 15–16.

a commercial interest of the controller could constitute a legitimate interest, within the meaning of Article 6(1)(f) GDPR, provided that it is not contrary to the law. The existence of such an interest and its lawfulness should however be assessed on a case-by-case basis (see para. 49).[155]

According to Article 28 (3) GDPR (processor agreement compliance), a written data processing agreement should be in place between the data controller and a data processor involved. Therefore, the processor acts only on documented instructions from the controller. Instructure and education institutions regulate the contractual relationship through the established agreement.

Customer instructs Instructure to process Customer personal data for the following purposes:[156]

- In accordance with the Agreement and applicable Data Protection Laws.
- To follow other reasonable instructions from the Customer, provided they are consistent with the Agreement and Data Protection Laws.

Instructure will:

- Promptly notify the Customer if it determines that any Customer instruction violates Data protection laws.
- Promptly inform the Customer if it can no longer comply with applicable data protection laws.

Therefore, it is a limited agreement with a defined scope and subjects. This agreement describes processing activities that institutions request from Instructure, the data subject categories, and other aspects of the data processing.

To assess the legitimacy of this further processing for different purposes (Instructure's own purposes) the controller must assess the compatibility of the purposes for which the data are collected, with the purposes for the further processing. This assessment must be based on the criteria in Article 6(4) GDPR:

1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
4. the possible consequences of the intended further processing for data subjects;
5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

[155] CJEU, judgment of 4 October 2024, Case C-621/22, Koninklijke Nederlandse Lawn Tennisbond (ECLI:EU:C:2024:857), para 40.
[156] Instructure, 'Canvas LMS Cookie Notice' (2025) https://www.instructure.com/policies/canvas-lms-cookie-notice accessed 24 October 2025.

Third parties

When SURF conducted analysis on the third parties (subprocessors), the party called Google Looker was identified. This is peculiar since Instructure claims that it does not use analytics outside the USA.[157]

This vendor was mentioned in the Table 8 Sub-processors of Instructure's Canvas LMS. It is stated by Instructure that '*these analytic tools are used by Customers to analyse certain activities by their end-users. Primarily used for data caching for visualisation*.'

In order to exercise this feature, Instructure gets access to the customer data provided by educational institutions: Canvas LMS username, short name, email address, SIS identification number, and Avatar URL, hierarchy data (i.e., account, sub account, course, section, students), dimensions and their columns (i.e., assignments, calendar events, collaborations), and, facts and their measures (i.e., Canvas activity log including page view and participation count).

Even though both New Analytics and Analytics Hub have the use of role-based access controls combined with Looker's flexible and secure architecture ensure that data access remains appropriately limited while still supporting robust, customizable analytics across different user roles. Analytics runs on Looker, a business intelligence platform. It provides a data exploration and dashboarding interface for users, an IDE for data modelers, and embedding and API features for developers.

As was discussed in Crash Analytics, this service, provided by Google, collects and processes technical crash data to support application stability and performance monitoring. By default, Crashlytics data collection is enabled in the SDK ('Software Development Kit) and starts automatically when the app initializes the service. Unless specifically disabled in the app's configuration, this processing occurs without requiring explicit user opt-in.

These operations mean that this personal data such as SIS ID and avatar will be shared with Google Cloud. Looker Data Services Inc. is mentioned in the DPA with higher educational institutions.[158] This is Analytics tool that Instructure uses as a subprocessor. However, in public documentation, Instructure informs that analytics is not exercised in the EU, only for the US customers. If the personal data is sent to Google Cloud for processing for analytics, there is a risk of unlawful processing such as a breach of transparency obligations (Art 5(1) (a) and breach of purpose limitation. Instructure explained that Analytics tool are for the customers only, and they do not use these tools for the benefit of Instructure or other customers.[159]

Instructure explained that: '*Looker does not permanently store customer's data in their platform. With Looker, queries are made directly against the Canvas LMS database and not by moving or extracting data to workbooks, cubes, .csv files, proprietary databases, or desktops. This key promotes data integrity while keeping data movement to a minimum and*

[157] Instructure, 'Canvas LMS Cookie Notice' (2025) https://www.instructure.com/policies/canvas-lms-cookie-notice accessed 24 October 2025.
[158] DPA with theuniversity, Annex A, page 13, section about subprocessors.
[159] Instructure's feedback from the 16th of September 2025.

access to sensitive information restricted.'[160] However, the purpose of the processing and categories of personal data shared with Looker should be minimised by Instructure and educational institutions. Instructure, as a processor, has a contractual obligation to ensure that only minimum necessary data is shared with Looker if an educational institution uses this subprocessor for the analytics purposes, and to assist data controllers (educational institutions) in ensuring whether certain categories of personal data are not processed outside of agreed purposes and means.

Overall, it is difficult for universities to assess or ensure that any further processing complies with the requirements of Article 6(4) GDPR.

[160] Instructure's feedback from the 13th of November 2025.

B.4 Necessity and Proportionality

B.4.1 The concept of necessity

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which are processed must be necessary for the purpose pursued by the processing activity. Proportionality means the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. Subsidiarity means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the controller needs to decrease the amount of personal data to what is necessary.

Therefore, essentially, the data controller may only process the personal data that are necessary to achieve the legitimate purpose but may not process personal data he or she may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

B.4.2 Assessment of proportionality

The key questions are: are the interests properly balanced? And does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.

Lawfulness

Overall, Instructure bases its data processing on lawful grounds. However, due to the lack of legal clarity and information in public documentation, the lawfulness of processing is not based on lawful processing if their activities fall outside the agreed purposes between Instructure and the educational institutions.

In the cookie statement, an educational institution may include a provision in the student enrollment agreement requiring the use of the Canvas LMS. By enrolling, students are understood to have consented to the data processing necessary for using Canvas, as it serves as the primary platform for submitting assignments and accessing course materials.

If the use of Canvas is mandatory for submitting assignments, accessing course materials, or participating in classes, students may have no real choice but to agree to the processing. In such circumstances, the imbalance of power between the institution and the student combined with the absence of a genuine alternative. It means that the consent cannot be considered ‘freely given’ according to Article 4(11) GDPR. This would render consent invalid as a legal basis, and the institution would need to rely on another lawful

basis, such as the performance of a contract or the necessity of processing for a task carried out in the public interest, to legitimise the processing.

Additionally, the involvement of third parties such as Looker based on Google Cloud may compromise the lawfulness of the processing if their purposes differ from those outlined in the agreement between Instructure and the education institutions.

Fairness

Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, or misleading to the data subject.[161] There are several circumstances that might be unexpected for the data subject. If processing causes negative effects, those must be justified and proportionate.

Although Instructure generally maintains well-organized documentation, some of the services offered within the Canvas LMS may be unexpected or not clearly outlined for end-users. For example, the feature called 'Masquerade'. With this function, the administrator selects the target user and provides the opportunity to assume another user's identity. From that moment on, all actions taken are performed as if by the masqueraded user.

Masquerading, while useful for support and administration, has serious privacy implications. It must be used with strong safeguards, and accountability to protect the rights of data subjects and comply with data protection laws.

Transparency

The principle of transparency not only ensures that consent must be informed but that full transparency of data practices and rights is ensured to users. In the case of children, this means that information relating to data processing must be comprehensible, recognizable and accessible to them (Article 12 GDPR).

Instructure's cookie statement was found to be not fully showing the cookies that Instructure collects from the customers. Some of the cookies that SURF identified in technical research in Table 6 Found Cookies during Technical Research, were not shown in a cookie notice meaning

In addition to this it includes generic purpose descriptions and uses words as 'like' or 'for example'. In general, the use of ambiguous wording or vague terms can contradict the principle of fairness of Article 5 (1) (a) GDPR, since information cannot be considered transparent, making data subjects unable to understand the processing of their personal data and to exercise their rights. According to the EDPB, the use of conditional tense ('might') leaves users unsure whether their data will be used for the processing or not. The EDPB recalls that the use of conditional tense or vague wording does not constitute 'clear and plain language' as required by Article 12 (1) GDPR and may only be used if controllers are able to demonstrate that this does not undermine the fairness of processing.

[161] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and Default, version 2.0, adopted on 20 October 2020, p. 16, URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

Additionally, in the cookie notice, it was stated that Instructure does not implement analytical cookies outside the USA. Meaning that no tracking cookies on the end-user's devices in the EU.[162] However, as was discussed in Crash Analytics, service Crashlytics, provided by Google, collects and processes technical crash data to support application stability and performance monitoring, and it is used by default (automatically) without requiring explicit user opt-in.

B.4.3 Data minimisation and privacy by design

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary. The data must be *'adequate, relevant and limited to what is necessary for the purposes for which they are processed'* (Article 5(1)(c) of the GDPR. The principle of "data minimisation" precludes the combination, analysis and processing of all personal data obtained from the data subject or third parties by a controller, such as the operator of an online social media platform, and collected both on that platform and elsewhere, for the purposes of targeted advertising, without any limitation in time and without distinction as to the nature of that data.[163]

In the Privacy data sheet, Instructure provides a clear list of personal data and links it to the purpose of the data processing. Similarly, in the agreements between the education institutions and Instructure. For example, Instructure processes various categories of personal data within Canvas LMS:

- **Customer Data**: Content uploaded by institutions and users (e.g., lesson plans, videos, assignments), fully owned by the customer.
- **User Data**: Personal data submitted by end users through Canvas (detailed in Table 4 of the Privacy Data Sheet).
- **Functional Data**: Temporarily processed to enable essential system functions; deleted or anonymized immediately after use.
- **Diagnostic Data**: Used for system maintenance and performance; may include personal data, requiring GDPR safeguards if identifiable.
- **Support Data**: Collected during support interactions; must comply with GDPR transparency and confidentiality rules.
- **Institutional Data**: Business-related information about the educational institution (e.g., institution name and settings).

SURF submitted the DSAR requests to have a clearer picture on the purpose of the processing and the categories of personal data. The DSAR responses provided were incomplete and lacked critical transparency required under the GDPR. When reviewing the DSAR analysis, Instructure consistently mentioned that they are a processor, and not the controller to provide such a detailed information.[164] However, as a processor, Instructure needs to assist the controller (educational institutions) by appropriate technical

[162] Instructure, 'Canvas LMS Cookie Notice' (2025) https://www.instructure.com/policies/canvas-lms-cookie-notice accessed 24 October 2025.
[163] CJEU 4 October 2024, C-446/21 (Schrems vs Meta), par. 65.
[164] Instructure's feedback from the 27th of August 2025.

and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.[165]

B.4.4 Accuracy

The principle of accuracy requires that personal data must be accurate and, where necessary, kept up to date. It also requires that reasonable steps be taken to ensure that inaccurate personal data, in relation to the purposes for which it is processed, is promptly erased or corrected (Article 5(1)(d), GDPR).

The principle of accuracy requires that the personal data be accurate and, where necessary, kept up to date. "[E]very reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (article 5 (1) (d) GDPR). According to the EDPB, the controller should consider this principle "*in relation to the risks and consequences of the concrete use of data*."

Administrators and users are generally able to update their personal data when needed (their name, email or document contents). Additionally, Instructure constantly reviews its documentation to ensure that the information is the most accurate. Instructure during the meetings with SURF stated that the documentation is reviewed regularly.[166]

Personal data must be accurate and linked to a specific purpose. Based on the DSR responses, educational institutions are unable to clearly associate the personal data with its corresponding purpose and data subject categories. This limitation makes it more challenging to uphold the principle of accuracy in this context.

B.4.5 Storage limitation

The principle of storage limitation requires that personal data should only be kept for as long as necessary for the purpose for which the data are processed. Data must *'not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed*' (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that '*personal data may be kept longer in so far as the personal data are processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'* (Article 5(1)(e), second sentence, GDPR).

Since Canvas uses Amazon S3 storage for the data backups,[167] all backup data stored in Amazon S3 is encrypted at rest and in transit, and AWS data centers adhere to stringent security standards, including ISO 27001, SOC 2. These conditions apply to the period for which personal data is expected to be stored or the criteria for determining that period.

[165] Article 28 (3) (e) GDPR.
[166] Instructure MOM, 18th September 2025.
[167] LMS Architecture document #76, page 3.

Instructure updated its retention policies making it the maximum period of four (4) months. The current data recovery configuration enables Point-In-Time Recovery (PTR) for up to 30 days of aged data, monthly restores for four (4) months of aged data, and recoverability of object data such as files and uploaded media for a period of one year.[168] If object data remains recoverable for up to one year after deletion or modification, it means that even though is no longer accessible to users, it continues to exist in backup or recovery systems. This might conflict with the storage limitation principle, which requires that personal data be retained only for as long as necessary for the purpose for which it was collected.

While maintaining backups for disaster recovery is a legitimate purpose, keeping recoverable copies for a full year may be considered excessive unless there is a clearly defined operational or regulatory justification. Instructure did not mention the purpose of certain retention periods: to justify why it is proportionate to its recovery needs and that such backups are used strictly for continuity purposes (not for any active processing or secondary use). When SURF conducted the DPIA, one of the desired outcomes was the period for which personal data is expected to be stored or the criteria for determining that period. Despite receiving the DSAR, this information was absent.

Based on this analysis, it appears that while the retention of backups for disaster recovery purposes is justified in principle, the one-year recovery period may not be fully aligned with the storage limitation period. The explanation that this backup data is strictly retained for disaster recovery purposes and that is proportionate to the purposes will provide a more proportionate approach in determining the storage limit for object data.

B.4.6 Integrity and confidentiality

Personal data must be processed in such a way as to ensure its appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage (Article 5(1)(f) GDPR together with Article 32(1) and (2) GDPR).

Instructure mentioned in its updated documentation that its approach is continue *'building resilience into its processes, technology and people'*.[169] Instructure adheres to the ISO 27001:2022 standards where a proactive incident management framework is mentioned.[170] Insrtucture reviews this document annually, where the improvement points for the security and data-driven improvements and post-incident analysis are mentioned.

Additionally, Access Control policy covers the standards, responsibilities and requirements for managing access to information systems, data, and resources.[171] Even though the information about the roles and responsibilities of the Instructure Security Sterring Committee and who can access what data is mentioned in the documentation, there was a lack of the specifics regarding how that access is managed, monitored, and reviewed. The integrity and confidentiality principle will be enhanced if the data classification is included. For example, identifying data sensitivity levels.

[168] Business Continuity & Disaster Recovery September 2025.
[169] Business Continuity & Disaster Recovery September 2025, page 5.
[170] ISMS – Information Security Incident Response Policy – 260225-152721.
[171] Access Control Policy (October 2024).

B.5 Data Subject Rights

The GDPR grants data subjects several rights, including the right to information, access, rectification, erasure, objection to profiling, data portability, and the right to lodge a complaint. It is the responsibility of the data controller (such as a Dutch educational institution) to provide this information and respond to these requests accurately and within the required timeframe.

When the data controller engages a data processor, such as Instructure, the GDPR requires that the data processing agreement explicitly states that the processor will assist the controller in fulfilling these obligations related to data subject rights.

B.5.1 Right to information

The first data subject right to be discussed is the right to information. Data subjects have a right to information. This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.

Instructure provides the opportunity for the end-users to exercise the right to information. Additionally, to the official DSR request that admins request through the Instructure's support, a self-serve user data export (DSR) in Canvas LMS is developed that gives the same response to the manually requested.[172] The responses are the same as was discussed in the Section Data Subject Access Requests.

Overall, data subjects are able to exercise the right to information. According to Article 15 GDPR, the controller has to provide the information about the processing of personal data. In order to provide a complete confirmation to a data subject, educational institution should receive a corresponding information from a processor. This obligation extends to a processor if a controller uses a processor for its data processing activities.[173]

Educational institutions instruct Instructure on what data to process, however Instructure acts as a data controller for its own purposes as well. Accordingly, Instructure should further assist the controller (educational institutions) in providing:

1. Purposes of processing – Reports did not specify why personal data is processed.
2. Categories of personal data – No clear, consolidated list (e.g., identity, academic, usage data).
3. Recipients – Missing information on recipients, especially in third countries or international organisations.
4. Storage period/criteria – No details on retention periods or criteria for determining them.

[172] _Data Privacy Upcoming Releases.pdf (confidential documentation).
[173] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights – Right of Access' (2023) https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf accessed 24 October 2025, para 125.

5. Data source – Absent when data was not collected directly from the data subject.
6. Data subject rights – No information on how to rectify, erase, or object to processing.
7. Automated decision-making – No indication of profiling or automated decisions, nor their logic or consequences.
8. Logs and error reports – Detailed system or error logs not provided beyond basic interaction records.

According to the CJEU, the right to obtain a 'copy' of personal data means that the data subject must be given a faithful and intelligible reproduction of all those data.[174] It does not only relate to the document, but to the personal data which it contains, and which must be complete: all the personal data undergoing processing. All information about a data subject: in a concise, transparent, intelligible, and easily accessible form using plain and clear language.

SURF submitted to Instructure to explain which personal data was missing from Instructure's response to SURF's DSAR. Some personal data was missing, specifically:

1) Bram Visser (Instructor A): The "Sample Document - SURF.pdf" _file, which was uploaded by Bram in Scenario 2A. This information is considered personal data, because hypothetically might involve personal data.
2) Sven de Vries (Student A):
    a. Explicit confirmation of liking his own post in the announcement discussion during Scenario 2B.
    b. The actual content of the instructor's video feedback and explicit confirmation that Sven viewed it during Scenario 3B.
    c. The specific text of comments received by Lotte during peer review from Scenario 6.
    d. The textual content 'Seventy-two' submitted for the 'Technical' assignment during scenario 3B is not displayed in the 'Submissions' table, only the submission type 'online_text_entry'.
    e. The specific answer 'False' for the 'Fun Quiz' from scenario 3B is not explicitly stated in the 'Submissions' table, only the quiz attempt and its score.

    This information is considered personal data because it shows the behavioral personal data about individual's actions and interactions.
3) Lotte Jansen (Student B): The specific comments ("Splendid.") made during her peer review in Scenario 6. Personal data as well, because shows the behavioral personal data.
4) Tijn Smit (IT administrator): His "Page Views" only include a general dashboard view around the time of the action, but no direct confirmation of the help ticket submission and its content.

Therefore, Instructure is missing this information to provide sufficient information to the data subjects. Whereas a data subject should be given a faithful and intelligible reproduction of all those data. SURF and Instructure addressed this issue, and mititgating measures were agreed which may be checked in Part D of this DPIA.

[174] Case C-487/21 Österreichische Datenschutzbehörde v CRIF GmbH [2023] ECLI:EU:C:2023:358.

B.5.2 Right to access

Secondly, data subjects have a (fundamental) right to access personal data concerning them. Upon request, data controllers must inform data subjects whether they are processing personal data about them (directly, or through a data processor). If this is the case, they must provide data subjects with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

According to the DPA, Instructure is assisting the institutions for the data subject to exercise the right to access personal data. Additionally, Instructure shall to the extent legally permitted, promptly notify Customer if it receives a Data Subject Request.[175]

In some cases, administrators (as controllers on behalf of educational institutions) may experience issues with receiving the full information from the DSR responses. This challenges the right to access from the perspective of the end-user.

B.5.3 Right to object profiling

Data subjects have the right to object to an exclusively automated decision if it has legal effects.

Instructure contractually guarantees that it does not use the personal data from its customers (sales contacts or admins) for profiling purposes, unless the admin has provided specific instructions. Therefore, this specific right of objection does not apply in this case.

B.5.4 Right to data portability

End-users have a right to data portability if the processing of their personal data is carried out by automated means and is based on their consent or on the necessity of a contract. The exercise of the right to data portability is problematic in relation to Education-internal documents and data. Instructure needs to assist its customers with data portability requests from. Its employees and students.

B.5.5 Right to file a complaint

Finally, educational institutions as controllers must inform their employees about their right to
complain, internally to their Data Protection Officer (DPO), and externally, to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

[175] Instructure, 'Data Processing Addendum' (2025) https://www.instructure.com/policies/data-processing-addendum accessed 24 October 2025.

In sum, educational institutions are currently not in a position to (fully) honour the rights of data subjects.

Part C Description and Assessment of Risks to Data Subjects

C.1 Risks to Data Subjects

This part concerns the description and assessment of the risks for data subjects. This part starts with an overall identification of the risks to the rights and freedoms of data subjects as a result of the processing of the Customer personal data and metadata (including purposes of the processing of the corresponding personal data). The risks will subsequently be classified according to the likelihood they might occur, and the impact on the rights and freedoms of the data subjects when they do.

C.1.1 Classification of the risks

A risk matrix is used to visually represent and classify the factors of probability and impact.

The risk matrix consists of a table with two axes, one on the left and one on the right, with the probability of occurrence on the horizontal axis and the impact on the vertical axis.

Impact of the damage	Heavy impact	Low risk	High Risk	High risk
	Medium impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Low probability	Reasonable chance	High probability
	Chance of damage occurring			

Figure 6 Risk matrix

C.2 Assessment of risks

C.2.1 Insufficient information provided in the DSAR (Medium)

The insufficient information provided in the DSAR data protection risk can be analyzed as a transparency and accessibility risk that may ultimately undermine fundamental data subject rights.

SURF's technical research after submitting the DSAR to Instructure showed that Instructure gives the output in a comprehensive and human-readable format and include a comprehensive overview of various data types, such as per interactions, enrollments, logins, and file attachments/exports, presented in a tabular format, with each table appearing in its own sheet. Additionally, the system records actions like submissions and quiz attempts, linking them to relevant assignments or discussions. Overall, the DSAR responses demonstrate a commendable level of structure and granularity in terms of system-tracked data. The inclusion of timestamps, metadata, and links to relevant course materials supports transparency regarding user activity.

Influencing fundamental human rights

However, SURF observed that some of the information was not the part of the response. The fact that the format matches what is available through the DSR button but excludes some user content implies that the DSAR is not complete and it lacked information.

This creates a risk of non-compliance with GDPR obligations and gives the impression that the organization may be withholding relevant personal data. If it is not the case, Instructure can provide the full DSAR response with the full personal data that was input in the system. Specifically, it is important to demonstrate a clear record of what is the data flow of personal data in the Canvas LMS environment.

This not sufficient information creates the lack of context and difficulty understanding or verifying what is being processed. Also, it lacks the This could interfere with the user's fundamental rights such as:

- Right to access and rectification (Articles 15–16).
- Right to data portability (Article 20).
- Right to object or restrict processing (Articles 18–21).

According to the EDPB, data subjects are entitled to full access to all personal data concerning them. Unless the data subject specifies otherwise, an access request should be interpreted broadly to include all relevant personal data.[176] In the case of technical research by SURF, the specification was given on the types of personal data was expected to be obtained. Additionally, the manually submitted DSAR produced the same response as one requested by an admin through the DSR tool, raising the question of why the manual request required more time to process. Overall, despite the DSAR's good structure and comprehensive format, the insufficient information provided was classified as a high risk due to the opacity in data flows within Canvas LMS can lead to loss of control over personal data.

However, after Inctructure and SURF discussed the risks, the vendor agreed with the SURF's reasoning to add additional personal and course data to the existing format for the DSAR. As Instructure stated: ' It is more work than simply updating the timeline, it is updating the format of its narrative'.[177] Instructure's commitment keeps this risk at a medium level until the measure is implemented and verified by SURF. Although the impact is high, the likelihood is low because the probability of occurrence is reduced by Instructure's mitigation efforts.

C.2.2 Retention period misalignment with purpose (Medium)

In this section, the risk analysis of the described data retention will be provided.

Instructure informed SURF about the data retention periods that it has:

- **Database Data**: The updated information from Instructure shows that the full database backups (snapshots) are retained for up to four (4) months, with daily,

[176] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights – Right of Access' (2023) https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf accessed 24 October 2025.

[177] Instructure and SURF meeting on mititgating measures on the 18th Novemebr 2025.

weekly, and monthly snapshots. Point-In-Time Recovery (PITR) is available for up to four (4) months of aged data.
- **Object Data**: Files, documents, uploaded media, and other static assets are recoverable for a period of one year.

In the beginning, the first risk element was the duration of 12 months. Instructure decreased the retention period to 4 months during the DPIA process. This minimises the risk of personal data such as object data and database data being stored for longer than necessary and against the purpose of data processing. Furthermore, Instructure explained that the reasoning behind the built time frames is based on an average school year timeline.[178]

The data retention period became shorter, however retaining object data backups for up to 12 months without a clear, documented justification or specific purpose, may be unnecessary. At this moment, there is no defined legal or operational rationale for this retention period. Impact on the data subjects may be high due to the fact that object data such as files, documents, and uploading media are recoverbale for a period of one (1) year. This is because if a data subject deletes the object data, the risk of the data reappearing in the system is significant. The likelihood of the risk occurring is low because Instructure reviews its policies and already implements the changes according to the GDPR requirements, particularly Article 5(1)(e), about the purpose limitation principle.

Through the negotiations with SURF, Instructure committed to provide shorter retention periods that align with institutional requirements.[179] Instructure introduced the 4-month retention period which standardizes the retention period across all products. The institutions, on the other hand, will establish clear internal data retention periods to the communicate this to its users. This way, data subjects will understand the retention period and link it to the specific purpose or categories of personal data. Overall, the risk remains medium until Instructure clearly defines the purposes of the data-retention timelines and include the purposes in the documentation 'Business and Continuity Disaster Recovery'.

C.2.3 Data minimisation risk when leveraging feedback (Low)

This risk section will discuss the leveraging feedback risk. In Section Feedback functionality, it was mentioned that Instructure acts as a controller for the feedback data. It covers customers satisfaction surveys, surveys about support received, requests for product feedback. This feedback data includes the end-users such as full name, email address, survey responses, and job title (if it relates to or can be used to identify an individual).[180]

Instructure answered to the SURF's questions about the feedback mechanism that the answers are anonymous; however, Case ID allows response to be matched to the appropriate case. The case ID can identify a person if matched internally. The comment box allows users to enter personal or sensitive data.

[178] Ibid.

[179] Instructure's commitments mentioned in the feedback to the version 0.6 of this DPIA from the 8th of December 2025.

[180] Privacy Data Sheet (April 23, 2024), page 10.

Additionally, the data minimisation principle is at risk due to the unrestricted nature of the comment box, which allows users to enter any content. For example, a user may inadvertently upload a screenshot containing personal data. In the feedback section, there was no warning about oversharing personal data in the comment section. The open-ended nature of the comment box presents a risk of unintended personal data disclosure, especially if users inadvertently submit sensitive information such as screenshots with identifiable data. Since Instructure acts as a controller for this feedback data, the lack of input controls may lead to non-compliance with data minimisation requirements (Article 5(1)(c) GDPR) and increase exposure to data protection incidents.

In Section on Data Processing Purposes, SURF mentioned that the Instructure's user support ticketing system and user helpdesk support and technical operations support process and store any Customer Personal Data submitted through a support system in the USA. Users (data subjects) might include more personal data than necessary to support their requests such as screenshots containing sensitive information or system logs with hidden identifiers. Therefore, unnecessary personal data may be collected and stored, and potentially be used for secondary purposes, since Instructure is a controller of the feedback data.

The risk was classified as high due to the likelihood of users accidentally uploading files containing personal data and the presence of a Case ID, capable of linking submissions to identifiable individuals. Users were not properly informed, or/and Case ID is widely used to link feedback to a particular request (identities).

After discussing the mitigating measures with Instructure, Instructure's support team has added the following language in the submission box:

"*Please do not include any personal, sensitive, or confidential information in this form. Submissions are intended solely for feedback purposes.*"

This measure is completed which reclassifies this risk to low or remote given that institutions implement SURF recommendations.

C.2.4 Re-identification: The logging session and anonymisation features against data protection risks (Medium)

Canvas LMS offers limited anonymisation functionalities aimed at promoting impartial grading and privacy with the teaching and assessment workflows. These features include Anonymous Grading and Anonymous Instructor Annotations, both of which operate predominantly at the user interface level rather than within backend data systems. These functionalities are described in Section Anonymisation and Pseudonymisation.

In Table 5 List of Personal Data, SURF mentioned that log data falls within the category of diagnostic data. During the testing, SURF noticed that personal data was included in the logs. Accordingly, there are several risks that fall within the insufficient anonymisation mechanism:

1. **Re-identification risk,** since original identifiers remain accessible in backend systems and logs, there is a significant risk of re-identification.

2. **Unauthorized access:** the persistence of identifiable data in system logs and backups increases the risk of unauthorized access or data breaches. Instructure clarified that those who have appropriate access can exercise the anonymous grading and anonymous Instructor annotations.
3. **Lack of transparency:** students may wrongly assume their data is fully anonymised when it is not, impacting informed consent and data subject rights.
4. **Insufficient control over data:** anonymisation features are opt-in, assignment-specific, and sometimes limited in scope, potentially resulting in inconsistent application and residual exposure of personal data.

Instructure explained that users do not want to stay identifiable, and that there is anonymization on the backend.[181] At the same time, admins may disable pseudonymization to not be able to re-identify the users. However, annotations made before enabling the option of anonymising DocViewer (for example) remain identifiable and this feature cannot be corrected.

Although anonymization mechanisms are implemented on the backend to prevent user identifiability, there is a design limitation where annotation made before enabling anonymisation (DocViewer) remain identifiable. The impact of the risk is high, because if users explicitly expect anonymity and identifiability persists, this might contract Article 25 GDPR (data protection by design and by default). The inability to prevent admin re-identification indicates insufficient data protection controls (data protection by design). The likelihood is high, because there is anonymisation in the backend and there is a known administrative capability that may allow re-identification.

However, after sharing the identified risk with Instructure, the vendor explained that: *'It is not designed to actually anonymize the user activity data as a technique to protect personal data. Therefore we don't agree with this being positioned as a high risk, if a risk at all.*[182]*'* This created misunderstadnings in the usage of the anonymisation. Which means that the whole purpose of anonymisation is not to no longer trace the personal data to an individual by any means, but to provide '*a pedagogical value in creating an anonymous relationship between the educator reviewing the student work and the student'*.[183] This feature is specifically necessary for the interface-level privacy during grading and feedback.

Overall, following the discussion with Instructure on the actual purpose of the anonymisation, the impact of this risk is reclassified to medium. Students and educators may believe their identities are protected beyond what is actually provided. The likelihood of the risk is medium because it is partially mitigated. The vendor explicitly states the feature is not meant to anonymize personal data. This provides clarity going forward.

Instructure remains open to elaborate the term anonymisation more for the users. When Instructure presents their solutions, SURF will review this risk. At this moment, this risk remains medium.

[181] MOM with Instructure from the 18th of September 2025.

[182] Instructure's response tot he v0.5 of this DPIA from the 12th of November 2025.

[183] Instructure's response tot he v0.5 of this DPIA from the 12th of November 2025.

C.2.5 Nature of the data involved and excessive retention in the Inbox (Medium)

In the Section Messaging and Communication, SURF discussed Canvas LMS built-in messaging feature known as the Inbox, which allows users to exchange messages.

When permitted by institutional settings, the Inbox also supports differentiation tags, allowing messages to be targeted based on user roles or subgroups within a course (e.g., specific sections or assignment groups).

Firstly, the nature of the data involved that Canvas LMS processes and stores includes personal identifiers and course metadata such as:

- **User Identifiers**: Sender and recipient names, roles, and Canvas user IDs.
- **Course Metadata**: Course ID, name, and role context, used to determine message eligibility and scope.
- **Message Content**: Subject lines, body text, and timestamped message threads.
- **Attachments**: Uploaded files, which may contain structured or unstructured personal data depending on user input.
- **Activity Metadata**: Read/unread status, timestamps of sending and receiving, and interaction logs.

The metadata mentioned above is an identifiable data, and attachments might introduce the possibility of processing special categories of data if users upload sensitive documents unintentionally. For example, as part of the attachments to the inbox, a user uploads documents containing health information.

Additionally, another risk identified with Inbox is even when the message is deleted from the interface, attachments may persist in the user's personal file storage. This misalignment between user expectations and system behavior increases compliance risk and may undermine transparency. 'Attachments may therefore persist in user storage even if the corresponding message is deleted from the Inbox view.'

In sum, the risk of the nature of data involved in the processing and not meeting storage limitation and erasure obligations were identified as a high risk. However, during the mitigating measures negotiations, Instructure demonstrated their commitments to provide best practices guidance to educational institutions. Furthermore, Instructure will investigate further the additionas to the guidance of the content in Inbox. The measures introduced by Instructure lower the likelihood of the risk occurring as low despite the impact being high. Overall, the risk stays medium until Instructure demonstrates the better guidance to the user uploads.

C.2.6 Analytics and Google Cloud Looker: International data transfers (High)

The risk analysis relates to the Analytics service provided by Instructure. It was analysed in Analytics, that the New Analytics and Analytics Hub use role-based access control (RBAC) within Looker, a Google-owned business intelligence platform. This supports flexible data access while maintaining internal controls. Analytics runs on Looker, a business intelligence platform. It provides a data exploration and dashboarding interface for

users, an IDE for data modelers, and embedding and API features for developers (see A.7.3.1).

Instructure explained that data processing with Looker is governed by a separate agreement, which is used for the intelligent insights, and it is only available for the customers, and not for the Instructure's own purposes.

Since Looker is based on Google Cloud, it means that personal or institutional data processed through Analytics is potentially accessible to third-party processor: Google. Google Cloud infrastructure involves data being transferred outside the EU/EEA area, and the risk of cross-border transfer. Therefore, this may pose compliance concern under Articles 44-49 GDPR regarding the secure data transfer options: adequate safeguards such as Standard Contractual Clauses are in place. This risk can be classified as a high risk. However, it is possible for the institutions to disable Looker. This will prevent the usage of Looker for analytics. More measures are anticipated from Instructure to mitigate the risk in 2026, which will be checked by SURF.

C.2.7 Analytics and Google Cloud Looker: purpose and data minimisation risk (High)

Following the risk analysed in the previous section, it is important to mention that the use of Analytics and involvement of the third-party Looker may result in the collection or use of more personal data that is necessary for the stated purpose. Instructure states that the purpose of data processing is '*providing data visualisation services for in-application analytics (New Analytics & Admin Analytics'*.

In the Table 8 Sub-processors of Instructure's Canvas LMS, the types of personal data is included that it is processed by Looker for the data processing purpose mentioned above. The list of personal data is broad: starting from the username and ending with Canvas activity log including page view and participation count. Activity logs, page views, and participation counts are considered personal data if they can identify an individual directly or indirectly.[184] Having the combination of username, IP address, profile picture, and activity logs allows to identify a data subject. It impacts a data subject, since more personal data is collected than necessary and might be used for broader purposes than originally stated.

Unnecessary data processing may lead to unauthorized profiling, unfair outcomes, or over-retention. The impact and likelihood are high because the broad scope of personal data is shared with Looker. Therefore, this risk for data subjects and institutions is high.

Same recommendation applies as in the previous risk assessment. Educational institutions are able to disable Looker, while Instructure committed to update its subprocessor statements to clarify the purpose of Looker. Further risk mitigation is anticipated in 2026, which will be assessed by SURF.

C.2.8 Lack of transparency: Masquerading (High)

[184] Case C-487/21 Österreichische Datenschutzbehörde v CRIF GmbH [2023] ECLI:EU:C:2023:358.

The masquerade function described in the Section Masquerading Functionality, allows users with a certain role-based permission to masquerade as a user at EU-based institution, and an IT administrator at a university can impersonate any student or staff member without the permission.

Indeed, Instructure sets the feature that admins or support agents are reminded of their masquerading mode. Additionally, Canvas LMS records all actors taken during a masquerade session in the audit log.

However, there is a likelihood that masquerading may discourage the misuse since there is a lack of oversight making the misuse more possible. This makes the impact of this risk high because the impersonator can view and/or access personal data which can potentially lead to the unauthorised data access. Since the user is not informed pre- or post-session, more measures should be implemented to comply with transparency principle from Article 5 (1) (a) GDPR. This makes this feature a high risk for data subjects.

However, Instructure committed to provide the necessary notifications to the users and additional features which will notify the users that they are being maquaraded.[185] Until SURF confirms the measures are implemented, this risk remains to be high due to the high impact and likelihood of the risk occurring to a data subject.

Therefore, Instructure demonstrates the full commitment to provide notifications, additional features and updating relevant guidance on feature changes for masquerade. To mitigate this risk, educational institutions may disable this feature to classify this risk as low.

C.2.9 Instructure Community: lack of control over the data processing (Medium)

When users access the Instructure Community via single sign-on (SSO) from their institutional Canvas LMS account, their profile is automatically created and publicly displays personal information by default including full name, username, join date, and community activity (posts and replies).

From privacy perspective, the impact on a data subject is high because there is a full public display of full name and activity history. This can lead to unintentional overexposure. The additional jeopardy is that the public data on Instructure Community can be linked to social engineering: public names and activity could be used for profiling/phishing.

The likelihood of this risk is high because many users access the Community by default through their Canvas LMS account and their account is automatically publicly displayed. According to Instructure, there is currently no technical method to disable access to the Instructure Community at the educational organisational or admin level[186]. This means educational institutions cannot prevent users from accessing the Community site via technical controls but can manage expectations or communicate use limitations through internal guidance.

[185] Instructure's feedback to the version 0.6 of this DPIA (8th December 2025).
[186] Email response from Instructure to SURF's questions (May 19th, 2025)

Instructure provided more clarity about the access to the Instructure Community, specifically about the privacy choice controls such as[187]:

- Display my profile publicly
- Display my email publicly
- Anonymize my analytics data

Instructure furthermore adds that '*the old Community platform was built in Khoros and the new Community platform is implemented in higher Logic Vanilla abd has gone live.'*[188]

There are available privacy options, and by default, Community settings keep a user's last name and e-mail address private.[189] The controls mentioned above are available to each member. These additions make it possible to use the Instructure Community, and lowers the intitial risk. Overall, the impact and likelihood of this risk are medium due to the measures implemented by Instructure. Before SURF is able to test and confirm the effectivieness of the measures, it is advised to disable this feature for the educational institutions to lower the risk.

C.2.10 Lack of transparency and incomplete user information: Consent (Medium)

After conducting a technical and legal analysis over the cookies used by Instructure, a risk was observed that data subjects are not fully or clearly informed about how their personal data is collected, processed, and according to which purposes.

Firstly, Instructure relies on contractual necessity which is based on Article 6 (1) (b) GDPR for any processing outside of the scope of the agreements with education institutions. From the institution perspective, it is unclear how and when consent is obtained. From data subject consent, it is more complex since a tacit consent may be obtained from end-users.

While the DPA clearly defines the roles of Instructure and education institutions, there might be a responsibility confusion over who controls the data processing because Instructure decides on the vendor choices. When SURF conducted the technical analysis to define the cookies used by Instructure, new cookies were found which are not mentioned in the Cookie Notice. This list may be found in the Table 7 Found Cookies during Technical Research.

Instructure is working on updating their Third-party service provider guide to include the subprocessors that operate the cookies on Canvas LMS platform. The new subprocessor found in the updated guide is Snowflake, Inc.[190]

There is a lack of transparency if education institutions cannot exercise control over personal data. Users are unaware of certain cookies which violates core transparency obligations. However, the impact is medium because Instructure is updating the

[187] Instructure's feedback to the DPIA version 0.6 from the 8th of December 2025.
[188] Instructure's feedback to the DPIA version 0.6 from the 10th of December 2025.
[189] Ibid.
[190] Instructure, 'Third-Party Processing Guide' (2024) https://community.canvaslms.com/t5/Privacy-Articles/Instructure-s-Third-Party-Processing-Guide/ta-p/606339 accessed 24 October 2025.

information to correspond to the transparency principle. Therefore, the risk is medium until Instructure presents a full updated information on its subprocessors.

C.2.11 API Security and token management in Canvas LMS environment (Medium)

From the section Application Programming Interfaces (APIs), SURF explained that Canvas LMS is used with OAuth 2.0 with short-lived access tokens and RBAC to protect API access. While the system is well-architected, it is important to mention that the use of APIs introduces the risks.

The risks discussed in this section are:

1. Token compromise because unauthorized parties may gain access to or intercept access tokens, enabling them to impersonate legitimate users or applications.
2. Token generation misuse, since tokens could be generated improperly or exploited by malicious actors due to weaknesses in the token issuance process or insufficient safeguards.

The use of APIs in Canvas LMS introduces risks primarily related to the compromise or misuse of access tokens. The likelihood of unauthorized access and processing of personal data is medium because the OAuth 2.0 with short lived tokens reduces the likelihood of anauthorised access, but does not remove the impact on data subjects' privacy.

The impact is high due to the risk of malicious actors exploiting tokens without any measures. Additionally, the potential risks mentioned above might affect the interfaces and lead to the misuse of tokens. This risk would be given as high, however there were measures which were completed by Instructure, and further improvements in API management and reporting on 3rd party partner API usage which are anticipated in 2026. This measure corresponds to the recommendations mentioned in the CNIL guidelines on providing traceability measures enable to identify unauthorised access in addition to the security measures that Instructure has in place.[191]

The measures which Instructure develops lowers the risk. Until SURF confirms the implementation of the remaining Instructure's actions, this risk remains medium. Without implementing the measures, the risk leans towards high due to the potentially severe consequences of token compromise.

C.2.12 Residual personal data in legacy backups (Medium)

When SURF started the DPIA, it was observed that Instructure did not perform regular reconciliation or validation to ensure deleted data is scrubbed from legacy backups over time. For example, to check whether data that has been deleted from active systems is also being removed (or "scrubbed") from older backup files over time. This means that even if personal data is deleted upon request, it might still exist in archived backups for a certain period, and Instructure is not actively verifying or cleaning those backups to remove that data.

[191] CNIL 'Technical recommendation on the use of Application Programming Interfaces (APIs)' (CNIL) dates 7th July 2023, page 9.

According to the GDPR, data subjects have the right to erasure ("right to be forgotten"). While it's common for backup systems to retain data temporarily, not having a clear process to eventually remove that data from backups could raise compliance concerns, especially if the data is ever restored or becomes accessible.

GDPR principles to consider:

1. Right to erasure (Article 17 GDPR) : data subjects have the right to have their personal data erased.
2. Accountability and data minimization (Articles 5 and 24) :controllers and processors must be able to demonstrate compliance and ensure data is not retained longer than necessary.
3. Security of processing (Article 32): appropriate measures must be in place to prevent unauthorized access to retained data.

Instructure stores Canvas LMS data redundantly in AWS Zones. There are daily database backups, backups of transaction logs, and Customer Content are configured using AWS backup and recovery solutions.[192] This is beneficial for business continuity because daily backups help recover data quickly in case of a system failure or data loss. But, daily backups rapidly accumulate copies of personal data, making it harder to manage, track, and eventually erase it.

If data is deleted from the live system, it may still reappear in the next backup cycle until actively excluded. Without exclusion mechanisms, deleted personal data continues to be stored, breaching the storage limitation principle (Article 5(1)(e)). It may still exist in archived backups for an extended period without systematic removal or verification.

The risk is medium, because backups are not routinely accessed, but the risks increases if they are restored or compromised. Instructure states that the back-ups are already encrypted and scrubbed.[193] SURF will conduct further tests to confirm the effectiveness of these measures. If Instructure uses incremental backups, the risk of deleted data resurfacing is lower, but not eliminated fully. To minimse the risk, Instructure may have a mechanism to identify deleted or corrected personal data, enabling such data to be located and removed if a backup is restored.

C.2.13 Lack of effective encryption key management for education institutions (Low risk)

Section on Encryption mentioned the information that Instructure does not support CMKs (customer-managed keys). Instructure explained to SURF that in a current architecture, they cannot support the CMKs, and it would defeat the purpose of having a complete control of encryption keys and effective security.[194] *'The benefit is that you can revoke the access to the key anytime. And there are no human users who run the encryption."*[195]

[192] Privacy Data Sheet, April 23, 2024, page 11.

[193] Feedback from Instructure to the v0.6 from the 10th of December.

[194] MOM with Instructure from the 18th of September 2025.

[195] MOM with Instructure from the 18th of September 2025.

The crucial aspect of cloud encryption is when a CMK is used (for example, on the AWS), the customer controls the key lifecycle and can configure key access policies that determine who can use which CMKs for which purposes. Instructure also mentioned that the security of the architecture can be undermined if someone is granted the access without the proper IAM. According to the SURF whitepaper on AWS encryption, '*overbroad access permissions for keys negate the protections offered by encrypting data: anybody who can use a CMK, can potentially read data protected with that key. In addition, access logs for key usage are available for CMKs (who used which key, at what time and for which kind of operation).*'[196]

The disadvantage for education institutions is that they dependent on Instructure's access policies, AWS KMS configurations, and associated audit and compliance frameworks (such as SOC 2 and ISO/IEC 27001 certifications) for the protection of cryptographic assets.

Based on the explanations offered by Instructure and overall CMSs practices, there is a heavy impact, but the chance of occurring is low. Instructure argues that there are more control mechanisms for the IAM. Even though the key is at the Instructure, Instructure argues that no one accesses the key to the customers. This leaves the occurrence of the risk at low level. Even though the impact might be high, because institutions do not exercise the control over encryption keys, Instructure confirms that this is the safest and most reliable option.

C.2.14 Unauthorised access to EU personal data (Medium)

Instructure Support Staff (located in the USA) can use a masquerade function to impersonate a student or instructor to troubleshoot support issues. During the meeting, Instructure confirmed that U.S.-based staff technically have access to EU personal data, though they "typically do not" exercise that access.[197] However, there are no strict access controls or procedural safeguards to prevent or monitor such access.

The potential impact on compliance and data subjects is high due to the unauthorised access risks if support staff has to access EU personal data. Even though Instructure claims that staff 'do not normally' access the EU data, there are no access controls and the capability itself presents a high compliance risk. Instructure has the office in Budapest, Hungary.[198] Therefore, the support staff from the EU should only have access to EU personal data for the purpose of providing support to the customers. The likelihood is medium. Because there are no strict technical or procedural controls preventing such access, this setup represents a potential security risk and raises compliance concerns under Articles 5(1)(f) and 32 of the GDPR. Overall, this risk is classified as high.

However, Instructure is planning to introduce an ability (likely globally on or off) to allow the customer to limit Instructure support staff access with additional improvements. Once Instructure will implement this feature, SURF will reclassify the risk.

[196] SURF & Xebia, 'Encryptie in de cloud van Microsoft Azure en Amazon Web Services' (2023) https://communities.surf.nl/files/Artikel/download/Rapport_Encryptie_in_de_cloud_van_Microsoft_Azure_en_Amazon_Web_Services.pdf accessed 24 October 2025.
[197] MOM with Instructure from the 18th of September 2025.
[198] Instructure, 'Contact Us' (2025) https://www.instructure.com/contact-us accessed 24 October 2025.

Part D Description of Proposed Mitigation Measures

D.1 Mitigation Measures

The following section contains a table of the mitigating technical, organisational and legal measures that need to be taken by the education organisation or by Instructure to reduce or solve the identified 3 high, 9 medium risks and 2 low risk for the data subjects.

The first 6 risks are qualified as high risks because the organisations themselves cannot take sufficient measures to mitigate the risk, other than by not using Canvas LMS.

The 6 risks are qualified as medium because Instructure and the Education and Research organisations can take effective measures to reduce the probability of occurrence to remote (or zero), even though the impact may still be high. This DPIA assumes that the organisations will adopt these measures. Low risks are risks that education institutions should mitigate within their own institutions.

D.1.1 Insufficient information provided in the DSAR

Insufficient information provided in the DSAR						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	Despite the DSAR's good structure and comprehensive format, the insufficient information provided poses a high risk due to opacity in data flows within Canvas LMS, which can lead to loss of control over personal data		**Low**	**High**	**Medium**	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 1	• Institutions will have an opportunity to file the service tickets through a standard operational procedure with a customer. Institutions will share their feedback directly with the vendor.	• Providing a complete and intelligible DSAR response, including all personal data input into the system. • Map and document the data flow within Canvas LMS, showing how data moves, is stored, and shared. • Ensure responses are contextualized, not just raw	**Low**	**Low**	**Low**	

	data dumps, so users can understand and verify processing.	

Suggested measures by Instructure	Timeline
Instructure plans to make a number of improvements to our existing DSAR process and outputs in 2026: ● Add additional product data to the existing output format for DSAR in the areas of course content, assignment details, discussions, and assessment as referenced in the SURF analysis. ● Improve the format of the DSAR output to provide additional context, categories, and details alongside the raw data outputs. ● Include relevant customer service ticket data and communications in DSAR output along with product data.	By June 2026 By November 2026 Customer support has confirmed relevant customer service tickets data and communications can be provided upon request.

D.1.2 Retention period misalignment with purpose

Retention period misalignment with purpose						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	Instructure's current data retention practices, retaining backups for up to 4 months without clear purpose.		**Low**	**High**	**Medium**	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 2	• Establish a clear internal data retention and deletion policies and require Instructure to follow the retention periods. • Monitor deletion requests and outcomes which are initiated by educational institutions.	Instructure provided the purpose for selecting the 4-month data retention period. The period was chosen for the reason of standardising retention period across all products, and to align with industry best practices. Instructure specified that '*We did not find any company who had a full restore greater than 4 months*'. SURF advised to include this purpose in the document 'Business and Continuity Disaster Recovery' from September 2025 and	**Low**	**Low**	**Low**	

	recurring updated documentations.	

Suggested measures by Instructure	Timeline
● We can provide shorter retention periods that align with institutional requirements.	

D.1.3 Leveraging feedback

Leveraging feedback						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	The significant likelihood of users inadvertently uploading personal data and the use of Case IDs linking submissions to individuals.		**Low**	**Low**	Low	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 3	• Institutions can raise user awareness through internal guidance. For example, providing LMS usage guidelines.	● Instructure confirmed that customer support will add verbiage about not adding any personal data in the textbook. SURF additionally recommends: ● Mandatory confirmation checkbox Require users to confirm. For example *"I confirm that this submission does not include personal or sensitive data."* ● Internal review workflow: Implement an internal moderation/review queue before feedback is stored or processed to manually verify that no personal data is included.	**Low**	**Low**	**Low**	

Suggested actions by Instructure	Timeline

The support team has added the following language in the submission box: "Please do not include any personal, sensitive, or confidential information in this form. Submissions are intended solely for feedback purposes."	Completed

D.1.4 The logging session and anonymisation features against data protection risks

The logging session and anonymisation features against data protection risks						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	Canvas LMS provides limited anonymisation features focused on interface-level privacy during grading and feedback.		**Medium**	**Medium**	**Medium**	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 4	• Provide clear internal guidance on the purposes of the anonymisation such as explaining clearly to data subjects that certain features marked as 'anonymisation' do not fully anonymise data. This falls within another purpose: pegagogical purpose.	• Explaining to end-users the difference between the anonymisation features (for the pedagogical purposes) and anonymisation techniques (to actually anonymise the personal data) in public documentations. • Renaming the feature used for the pegagogical purpose. • Implementing stronger backend anonymisation or pseudonymisation techniques to protect personal data in logs and storage. • Restrict access to logs containing personal data through strict access controls and regular audits. • Enhance transparency by clearly informing data subjects and	**Low**	**Low**	**Low**	

			educational institutions about the limits of anonymisation features.			

Suggested actions by Instructure	Timeline
● Instructure will update user help guides/documentation/descriptions to clarify the meaning of anonymization for this feature, explicitly stating that it is not designed as a data anonymization feature.	January 2026

D.1.5 Nature of the data involved and excessive retention in the Inbox

Nature of the data involved and excessive retention in the Inbox						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	Identifiable metadata and the potential processing of sensitive data through user-uploaded attachments, such as health information, which may be uploaded unintentionally		**Low**	**High**	**Medium**	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 5	• Attachments in an inbox is standard functionality which data subjects and institutions would normally navigate with intention. Therefore, institutions	● Content control: Instructure should provide clear guidance or warnings to users before uploading attachments. ● Deletion: auto-delete attachments – to delete inbox	**Low**	**Low**	**Low**	

	should develop training and procedures for data subjects to navigate the features of the Inbox.	messages or prompts the user to manage file storage. • Insturcture will help and consult customers through the customer support service.				

Suggested actions (Instructure)	Timeline
• Instructure customer implementation and support teams are informed and able to provide best practices guidance to institutions.	Currently available
• Instructure will investigate additions to the user experience that add warnings/guidance when a user uploads content; with the goal of providing a follow up timeframe and specific improvements.	March 2026

Note to SURF: Unintentional uploads should not be considered high risk when the behavior of the user is something that is in the direct control of the institution, not Instructure. Attachments in an inbox is standard functionality which data subjects and institutions would normally navigate with intention. Additional warning verbiage, while useful, also would not completely inhibit the ability to upload sensitive data unintentionally. We do not agree that this is a high risk, but we can work towards improved wording.

D.1.6 Analytics and Google Cloud Looker: International data transfers

Analytics and Google Cloud Looker: International data transfers						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	**Current risk**
	Analytics service provided by Instructure, which operates through Looker, a Google Cloud–based business intelligence platform using role-based access control (RBAC) to manage data access.		**High**	**High**	**High**	
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 6	• Disable Analytics features by default. If institutions would want to use the features, there will be separate options available. • Educate teachers and administrators to not use these analytics features	• Ability to disable Analytics on an institutional level and have this disabled by default. Extensive use of these analytics may introduce bias in teachers' evaluations. • Conduct a TIA: it is needed to	**Low**	**Low**	**Low**	

		for profiling purposes. ● Raise awareness about the ethical contstraints of analytics features.		assess the legal and practical enforceability of SCCs in the third country (US); ● Transparency to institutions: Institutions must be informed in clear terms about what data is transferred, for what purpose, and how it is protected. ● User notification and consent: what are the mechanisms for the consent? ● Restrict types of personal data is sent to Looker. ● Scrubbing from user's file storage if a file has been deleted due to a DSAR request. This means that Canvas LMS environment no traces of this deleted remain anymore.		

Suggested actions (Instructure)	Timeline
● Instructure allows disabling of the Intelligent Insights add-on product, which would prevent all use of Looker for analytics.	Already available
● Instructure will update sub-processor statement for Intelligent Insights product as well as Course and Admin Analytics to clarify use of Looker is only for these specific analytic solutions in Canvas.	January 2026
● Instructure allows the disabling of Admin Analytics and Course Analytics to ensure Looker is not used for data visualisation.	Currently available

D.1.7 Analytics and Google Cloud Looker: purpose and data minimisation risk

Analytics and Google Cloud Looker: purpose and data minimisation risk						
Reference	Reason	Consequence	Chance	Impact	Risc Score	Current risk

	The use of Analytics and involvement of the third-party Looker may lead to the collection and processing of more personal data than necessary for the stated purpose of providing data visualization services.		**High**	**High**	**High**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**
Risk 7	• Disable Analytics features by default. If institutions would want to use the features, there will be separate options available. • Educate teachers and administrators to not use these analytics features for profiling purposes. • Raise awareness about the ethical contstraints of analytics features.	• Ability to disable Analytics on an institutional level and have this disabled by default. Extensive use of these analytics may introduce bias in teachers' evaluations. • Conduct regular audits and reviews of analytics usage patterns; • Configure Looker to enforce row-level data access in order to minimize the visibility of unnecessary fields. • Implement purpose driven data views for the specific roles; • Limit the purpose and explicitly state in the documentation. • Implement privacy enhancing technology.	**Low**	**Low**	**Low**

Suggested actions by Instructure	**Timeline**
● Instructure allows disabling of the Intelligent Insights add-on product, which would prevent all use of Looker for analytics.	Already supported
● Instructure will update sub-processor statement for Intelligent Insights product as well as Course and Admin Analytics to clarify use of Looker is only for these specific analytic solutions in Canvas.	January 2026 Currently available

- Instructure allows the disabling of Admin Analytics and Course Analytics to ensure Looker is not used for data visualisation.

D.1.8 Lack of transparency: Masquerading

Masquerading						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	Masquerading poses the risk of unauthorized access to personal data and undermines transparency, as users are not notified before or after such sessions.		**High**	**High**	**High**	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 8	• Disable masquerading until SURF confirms the implemented measures by Instructure. • Strict access controls in order to limit masquerading permissions only to essential personnel and roles, applying the principle of least privilege. • Apply enhanced oversight and monitoring. This will allow to regularly review audit logs and establish automated alerts for suspicious or unauthorized masquerading activities. • User notifications such as informing users promptly when their accounts have been accessed via masquerading, both before and after the session, to enhance transparency.	• Real-time notifications for the users via email that the masquerade session has occurred. For example, it should be visible not only for the admin, but for the users who are being masqueraded on. • Role-based limitations: restrict what an impersonator can access during a session. • Provide clear guidelines on this feature for the education institutions to raise awareness for the data subjects.	**Low**	**Low**	**Low**	

Suggested actions (Instructure)	Timeline
● Instructure will add the ability, via site level setting, to notify an end user via existing notification services when an admin has used the masquerade feature to access their account.	October 2026
● Instructure will update existing "Act As" (masquerade) feature to inform the admin user that the end user will be notified of their action.	October 2026
● Instructure will update relevant help/guides based on feature changes for masquerade and best practices.	October 2026

D.1.9 Instructure Community: lack of control over the data processing

Canvas Community: lack of control over the data processing						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
Risk 9	When users access the Instructure Community via single sign-on from their institutional Canvas LMS account, their profiles are automatically created and publicly display personal information such as full name, username, join date, and activity history.		**Medium**	**Medium**	**Medium**	**Curren t risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
	• Disable this feature until SURF confirms the effectiveness of the measures implemented by Instructure.	● Provide institutions the ability to disable or restrict Instructure Community access to the admin level; ● Default profile visibility to private; ● Minimise shared data: for example, only username.	**Low**	**Low**	**Low**	

Suggested actions (Instructure)	Timeline

When someone visits the Instructure Community, they can choose to log in, but logging in (or creating an account) is not required to access or use any Canvas or product self-support materials.

If a user does choose to create an account through Canvas single sign-on, they are first asked whether they want to create an account. They are then given the option to personalize an automatically generated username and are shown the Community Terms of Service. An account is not created automatically - the user must actively opt in.
By default, Community settings keep a user's last name and email address private. Each member also has additional privacy controls in their personal profile, where they can choose to turn the following on or off:

- **Display my profile publicly**
- **Display my email publicly**
- **Anonymize my analytics data**

There is no need to disable this feature. New technology has already been implemented.

The old Community platform was built in Khoros and the new Community platform is implemented in Higher Logic Vanilla and has gone live. SURF will test the new technology implemented by instructure before approving that this measure mitigates the risk of automatically creating profiles and publicly displaying personal information.

D.1.10 Lack of transparency and incomplete user information: Consent

Lack of transparency and incomplete user information: Consent						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
	Risks related to insufficient transparency and unclear consent regarding the collection and processing of personal data.		**Medium**	**Medium**	**Medium**	**Current risk**
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 10	• Admin level setting to opt-out.	• Provide clear and comprehensive information required under Article 13 and 14 GDPR. • Audit and update cookie notice.	**Low**	**Low**	**Low**	

Suggested actions (Instructure)	Timeline
Instructure is taking action in the following areas:	
• Conducting a cookie audit across our products and will update our cookie notice.	March 2026
• Implement an updated cookie consent tool that will allow for the needed information and control of cookies to users.	April 2026

D.1.11 API Security and token management in Canvas LMS environment

API Security and token management in Canvas LMS environment						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	**Current risk**

	The risks remain, including token compromise. Where unauthorized parties gain access to tokens and token generation misuse, this allows malicious actors to exploit weaknesses in token issuance.		**Medium**	**Medium**	**Medium**

Risk 11	**Measures Institution**	**Measures Vendor**	**Chance**	**Impact**	**Risc score**
	• Monitor tokem usage and unusual access patterns.	• Strict token lifecycle management; • Secure storage, monitoring; • More details about the incident response.	**Low**	**Low**	**Low**

Suggested actions by Instructure	**Timeline**

• Instructure requires user API tokens for API access to expire no longer than 180 days from creation.
• Admins are able to set shorter expiration timeframes on user API tokens.
• Admins can revoke user keys immediately.
• Instructure is planning to make additional improvements to API management and reporting throughout 2026 focused initially on 3rd party (partner) API usage. Exact timeframes are still pending technical discovery and planning.
  ○ Enhanced reporting on 3rd party partner API usage showing overall traffic and usage against endpoint domains or scopes.
  ○ Improved configuration over scopes and permissions for developer keys.
• The ability to manage rate limiting for specific partners or developer keys.
	Currently available
	
	Currently Available
	
	Currently Available
	Throughout 2026, completion by November 2026

D.1.12 Residual personal data in legacy backups

API Security and token management in Canvas LMS environment						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	
Risk 12	No currently performing regular reconciliation or validation to ensure deleted data is scrubbed from legacy backups over time.		**Medium**	**Medium**	**Medium**	**Current risk**

Measures Institution	Measures Vendor	Chance	Impact	Risc score
• Be specific regarding contractual requirements on backup deletion and verification.	• Implement a backup data retention policy which will include information about the backup. • Establish a regular reconciliation and validation process. • Use backup encryption and access controls. • Engage with backup service providers to enable data scrubbing.	**Low**	**Low**	**Low**

Suggested actions by Instructure	Timeline

Instructure's backups are protected such that no person or entity can mutate or delete to both align with industry standards and to protect against ransomware . When Instructure receives a data deletion request, the conical ID of the data entry is logged. When a backup is selected for restore, the conical IDs for deleted data are assessed against the restored conical IDs. For IDs that are on the list of deleted data, we then perform the same scrubbing action which originally took place upon the initial request, preserving the deletion of the object.

The 4-month retention period was defined to standardize retention period across all products, and to align with industry best practices. We did not find any company who had a full restore greater than 4 months.

Back up are already encrypted and scrubbed: *Instructure's backups are protected such that no person or entity can mutate or delete to both align with industry standards and to protect against ransomware . When Instructure receives a data deletion request, the conical ID of the data entry is logged. When a backup is selected for restore, the conical IDs for deleted data are assessed against the restored conical IDs. For IDs that are on the list of deleted data, we then perform the same scrubbing action which originally took place upon the initial request, preserving the deletion of the object.*

D.1.13 Lack of effective encryption key management for education institutions

Lack of effective encryption key management for education institutions						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	**Current risk**
Risk 13	Instructure does not support the CMKs.		**Low**	**Medium**	**Low**	

Measures Institution	Measures Vendor	Chance	Impact	Risc score
• Education institutions can add specific encryption requirements in their DPAs. That the encryption should be stored in the EU. • Education institutions should request key management controls where vendor describes how encryption keys are generated, stored, and rotated. • Ask the vendor to limit personnel access to encrypted data.	• Instructure should ensure that personal data in education institutions' tenant is encrypted before this data is uploaded.	**Low**	**Low**	**Low**

Suggested actions (Instructure)	Timeline

D.1.14 Unauthorised access to EU personal data

Unauthorised access to EU personal data						
Reference	**Reason**	**Consequence**	**Chance**	**Impact**	**Risc Score**	**Current risk**
	Instructure's support staff can access the EU Customer data.		**Medium**	**Medium**	**Medium**	
	Measures Institution	**Measures Vendor**	**Chance**	**Impact**	**Risc score**	
Risk 14	• Institutions can strengthen contractual and Governance controls such as the DPA explicitly stating that access to EU personal data by non-EU support staff is permitted only when necessary.	• Instructure should implement technical access restrictions. For example, limit the use of masquerade feature to EU-based support teams when dealing with EU customers. Access by US staff should	**Low**	**Low**	**Low**	

require specific and explicit authorization.
- Apply Role-Based access control (RBAC), so that only specific roles can perform the tasks.

Suggested actions (Instructure)	Timeline
● By June 2026 we will have basic ability (likely globally on or off) to allow the customer to limit Instructure support staff access with additional improvements planned by November 2026. ● This capability will not be on by default as it can severely limit support response times for users and customers. Customers can request that it be enabled if required and with awareness of potential impacts to support.	

Conclusion

This DPIA identified 3 high, 9 medium risks and 2 low risks associated with the use of Instructure's Canvas LMS. Measures have been proposed for all these risks to reduce the risk level to low, both on the part of the institutions and on the part of Instructure.

Throughout the DPIA process, Instructure was highly cooperative and supporting SURF at every stage of the assessment and demonstrating a strong level of transparency about its processes by consistently providing informative and detailed responses to our questions. Overall, SURF determines that the DPIA has been satisfactory performed together with Instructure.

The vendor has implemented several measures to mitigate the risks already. These measures were taken into account when SURF was classifying the risk levels. Remaining high risks concern the use of the subrocessor Looker specifically during the international data transfers and the collection of processing of more personal data than necessary. Educational institutions can lower these two risks by disabling this subprocessor and the related feature such as Intelligent Insights. The third high risk concerns the lack of transparency associated with the feature 'Masquerading'. Instructure has committed to implement the relevant mitigating measures in 2026. However, until such measures are live and SURF has assessed their effectiveness, educational institutions are advised to disable this feature.

While some measures are already implements such as for the risk 'Leveraging feedback', the mitigating measures for remaning medium risks have been only partially completed or are planned for full implementation in 2026.

Appendix 1 Technical Testing Scenarios

This appendix describes the testing scenarios that were executed for data flow analysis, how they were performed, and what they tested, alongside the setup for executing the scenarios.

1.1 Testing Software and Hardware

In conducting man-in-the-middle (MITM) data flow gathering, a stable and reproducible test environment is critical. We tested Canvas LMS on two platforms: web-based and mobile-based. This section outlines the software and hardware used at the time of testing.

For intercepting HTTP(S) traffic, we used HTTP Toolkit. HTTP Toolkit allows us to intercept both local traffic generated on the machine, as well as external devices by hosting a proxy server. HTTP Toolkit ran on the following machine:

- Apple MacBook Pro 2023 14", M3 Pro (11-core CPU, 14-core GPU, 18GB RAM)
- macOS Sequoia 15.4.1
- HTTP Toolkit v1.20.1

For testing the web-based Canvas LMS platform, we used Google Chrome v136.0.7103.94, which ran on the aforementioned machine (local traffic). Chrome was configured to accept the HTTP Toolkit root certificate for SSL/TLS interception.

For testing the mobile-based Canvas LMS platform, specifically Canvas for Android[199], we used:

- Samsung Galaxy S21 5G (SM-G991B/DS)
- Samsung One UI 7.0
- Android 15 (Vanilla Ice Cream)
- Version: G991BXXUEHYD5 / G991BOXMEHYD5 / G991BXXUEHYD5
- Security patch level: 1 April 2025

To be able to intercept traffic from Canvas for Android, the code had to be modified. Canvas for Android does not accept user certificates by default, which is necessary for HTTP Toolkit to intercept traffic. A good security measure, but difficult for our testing purposes, nonetheless. Our device does not have an unlocked bootloader or is otherwise rooted to allow us to inject certificates or modify the application during runtime on demand. Luckily, Canvas for Android is largely open-source and thus, modifying the code to allow user certificates is trivial[200].

For all platforms, network traffic logs were captured for each session and stored securely for further analysis. Screenshots were made during every step in the testing process. Scenarios were executed on the web-based Canvas LMS platform, unless otherwise specified.

[199] Instructure, 'canvas-android' (GitHub) https://github.com/instructure/canvas-android accessed 24 October 2025.
[200] https://github.com/RillJ/canvas-android/commit/fbde030d239cff1d073dd993fc437b10db4f1e86.

1.2 Canvas LMS Accounts

Full Name	Display Name	Sortable Name	Email	SIS ID	Actor Role	Actor Number
Sven de Vries	Sven de Vries	Vries, Sven de	julian.rill+svendevries@surf.nl	S2025 00001	Student	A
Lotte Jansen	Lotte Jansen	Jansen, Lotte	julian.rill+lottejansen@surf.nl	S2025 00002	Student	B
Daan van den Berg	Daan van den Berg	Berg, Daan van den	julian.rill+daanvandenberg@surf.nl	S2025 00003	Student	C
Bram Visser	Bram Visser	Visser, Bram	julian.rill+bramvisser@surf.nl	L2025 00002	Instructor	A
Noa de Jong	Noa de Jong	Jong, Noa de	julian.rill+noadejong@surf.nl	L2025 00003	Instructor	B
Tijn Smit	Tijn Smit	Smit, Tijn	julian.rill+tijnsmit@surf.nl	*N/A*	IT Administrator	*N/A*

Table 9 Accounts used during technical testing within Canvas LMS

1.3 Scenario 1: Login and Authentication

Features Tested

- **Authentication:** Allows end users of Canvas LMS to authenticate and authorise their identity and get access to the features of Canvas LMS.

Actors

- Student

Scenario Description

A student receives an email from the system about their ability to create a password for their Canvas LMS account. The student follows this email to configure a password and proceed to the dashboard.

Prerequisites

- IT Administrator created an account for Student (A).

Steps

1. Student (A): Navigates to the login page.
2. Student (A): Enters their email and password and clicks 'Log In'. The dashboard appears.

Platforms

The test should be executed on both the web-based and mobile-based Canvas LMS platforms.

1.4 Scenario 2A: Course Setup & Content Development

Business Processes

- Onderwijsmateriaalontsluiting
- Onderwijseenheidontwikkeling
- Voorbereiding onderwijsuitvoering
- Toepassing leermaterialen

Features Tested

- **Courses**: Create and manage a new course based on default settings.
- **Modules**: Organise content into units or weeks.
- **Pages**: Develop detailed resource pages.
- **Enrollment**: Simulate student (and instructor) enrollment actions manually to mimic the SIS process for testing purposes.
- **Syllabus**: The syllabus details are reviewed and updated as needed.

Actors

- IT Administrator
- Instructor

Scenario Description

An Instructor uses the web user interface to design a new course by creating the course, setting up its Modules and Pages, and preparing the course content. This phase simulates the standard design/setup activities without involving enrollment actions since manual enrollment is used in the testing environment.

Prerequisites

- IT Administrator is logged in.

Steps

1. IT Administrator: Navigates to Courses > 'All Courses'.
2. IT Administrator: Clicks '+ Course' to add a course.
3. IT Administrator: Selects 'Canvas LMS Review' as the account and writes 'Technical Privacy Research' as the course name, then clicks on 'Create'. The dashboard appears.
4. IT Administrator: Clicks 'People' in the sidebar.
5. IT Administrator: Clicks '+ People'.
6. IT Administrator: Adds Instructor (A) by writing their email address and selects 'Teacher' as role, then clicks on 'Next'. does the same for Student (A) and Student (B) but with 'Student' as role
7. IT Administrator: Clicks 'Add Users'.
8. IT Administrator: Clicks '+ People'.
9. IT Administrator: Adds Student (A) and Student (B) but with 'Student' as role by writing their email address and selects 'Student' as role, then clicks on 'Next'.
10. IT Administrator: Clicks 'Add Users'.
11. IT Administrator: Clicks 'Account'.
12. IT Administrator: Clicks 'Log out.
13. Instructor (A): Logs in (same steps as Scenario 1).
14. Instructor (A): Clicks 'Accept' at the top of the dashboard for the 'Technical Privacy Research' course.
15. Instructor (A): Clicks 'Courses' and then 'Technical Privacy Research'.
16. Instructor (A): Clicks 'Create a new Module'.
17. Instructor (A): Calls the module 'Lecture 1' and clicks 'Add Module'.
18. Instructor (A): Clicks '+ Module'.
19. Instructor (A): Calls the module it 'Lecture 2' and under 'Prerequisites' adds 'Lecture 1', then clicks on 'Add Module'.
20. Instructor (A): Clicks '+' under module 'Lecture 1'.
21. Instructor (A): Selects to add a 'Page' and assigns the name 'Welcome', then clicks 'Add Item'.
22. Instructor (A): Clicks the 'Welcome' page.
23. Instructor (A): Clicks 'Edit'.
24. Instructor (A): Adds 'Welcome to this course!' in the page body, then clicks 'Save'.
25. Instructor (A): Clicks 'Home'.
26. Instructor (A): Clicks '+' under module 'Lecture 1'.
27. Instructor (A): Selects to add a 'File' and selects 'Sample Document - SURF.pdf', then clicks 'Add Item'.
28. Instructor (A): Clicks '+' under module 'Lecture 2'.
29. Instructor (A): Selects to add a 'Page', selects 'Welcome', and clicks 'Add Item'.
30. Instructor (A): Clicks 'Syllabus'.
31. Instructor (A): Clicks 'Edit'.

32. Instructor (A): Writes ‘We will talk about technical research.’ in the body and clicks ‘Update Syllabus’.
33. Instructor (A): Clicks ‘Home’.
34. Instructor (A): Clicks ‘Publish All’ and then ‘Publish all modules and items.
35. Instructor (A): Clicks ‘Continue’ in the disclaimer.
36. Instructor (A): Clicks ‘Unpublished’ under ‘Course Status’, and then ‘Publish’.

1.5 Scenario 2B: Course Announcement After Enrolment

Business Processes

- Onderwijsmateriaalontsluiting
- Voorbereiding onderwijsuitvoering

Features Tested

- **Announcements**: Publish messages to inform students about important course updates post-enrollment.

Actors

- Instructor
- Student

Scenario Description

After manually enrolling students (and instructors) to simulate the administrative enrollment process, the Instructor finalises the course setup by issuing Announcements.

Prerequisites

- Scenario 2A was executed.
- Instructor (A) is logged in and is on the ‘Home’ page of the ‘Technical Privacy Research’ course.
- Student (A) is logged in and is on the ‘Dashboard’.
- Student (A) and Student (B) accepted the invitation to the course.

Steps

1. Instructor (A): Clicks ‘Announcements’.
2. Instructor (A): Clicks ‘Add Announcement’.
3. Instructor (A): Writes ‘Course starts’ in the title and ‘Today.’ in the body. Selects options ‘Allow Participants to Comment’, ‘Enable podcast feed’ and ‘Allow liking’. Finally, clicks ‘Publish’.
4. Student (A): Clicks on the announcement icon within the course ‘Technical Privacy Research’.
5. Student (A): Clicks on the made announcement.
6. Student (A): Clicks ‘Reply’.
7. Student (A): Writes ‘Excited!’ in the body and clicks ‘Reply’.
8. Student (A): Clicks ‘Like’ on the post they just made.

1.6 Scenario 3A: Assignment and Quiz Design

Business Processes

- Toetsvoorbereiding
- Vaststelling verworven competenties

Features Tested

- **Assignments**: Create assignments intended for assessment purposes.
- **Quizzes**: Develop practice quizzes for formative assessment purposes.
- **SpeedGrader**: Configure grading settings and set up rubrics.
- **Gradebook (Setup)**: Prepare for later grade import/export actions.

Actors

- Instructor

Scenario Description

An Instructor designs assessments by creating assignments and quizzes using the Canvas interface. The focus is on setting up the assessment instruments and grading tools (including SpeedGrader), ensuring that the design fits the intended formative assessment approach.

Prerequisites

- Scenario 1 was executed.
- Instructor (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.

Steps

1. Instructor (A): Clicks 'Assignments'.
2. Instructor (A): Clicks '+ Assignment'.
3. Instructor (A): Writes and selects the following before clicking on 'Save':
    a. Assignment Name: 'Technical'
    b. Body: 'Let's dive in.'
    c. Points: 5
    d. Submission Type: 'Online', 'Text Entry'
4. Instructor (A): Clicks on '+ Rubric'.
5. Instructor (A): Writes and selects the following before clicking on 'Create rubric':
    a. Description: 'Description of criterion'
    b. Long Description: 'Long description of criterion'
6. Instructor (A): Clicks 'Publish'.
7. Instructor (A): Clicks 'Quizzes'.
8. Instructor (A): Clicks '+ Quiz'.
9. Instructor (A): Selects 'New Quizzes' and clicks 'Submit'.
10. Instructor (A): Writes 'Fun Quiz' as the name and clicks 'Build'.
11. Instructor (A): Clicks '+'.
12. Instructor (A): Selects 'True or False'.
13. Instructor (A): Writes 'Research is fun' as the question stem and clicks 'Done'.
14. Instructor (A): Clicks 'Return'.
15. Instructor (A): Clicks on the crossed-out sign to 'Publish'.

1.7 Scenario 3B: Assessment Execution and Grade Management

Business Processes

- Toetsuitvoering
- Toetsbeoordeling

Features Tested

- **Assignments**: Students submit work that is later reviewed.
- **Quizzes**: Students complete formative quizzes.
- **SpeedGrader**: Review submissions and manage the publication or hiding of grades.
- **Gradebook**: Import and export grade data for further processing.

Actors

- Instructor
- Student

Scenario Description

Students submit assignments and complete quizzes. The Instructor uses SpeedGrader to review submissions and manages the Gradebook, including import/export of grades from files. Particular attention is given to the functionality that controls the publication and hiding of grades within the Gradebook.

Prerequisites

- Scenario 2 and 3A were executed.
- Student (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.
- Instructor (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.
- The 'Technical' assignment is published.

Steps

1. Student (A): Clicks 'Assignments'.
2. Student (A): Clicks 'Technical'.
3. Student (A): Clicks 'Start Assignment'.
4. Student (A): Writes 'Seventy-two' in the body and clicks 'Submit assignment'.
5. Student (A): Clicks 'Quizzes'.
6. Student (A): Clicks 'Fun Quiz'.
7. Student (A): Clicks 'Begin'.
8. Student (A): Clicks 'False' followed by 'Submit'.
9. Student (A): Clicks 'Submit' in the confirmation window.
10. Instructor (A): Clicks 'Assignments'.
11. Instructor (A): Clicks on the three dots next to 'Technical' and clicks on 'SpeedGrader'.
12. Instructor (A): Clicks on 'View Rubric'.
13. Instructor (A): Clicks on the message bulb icon under 'Pts'.
14. Instructor (A): Enters '4' under 'Pts' and writes 'Decent' in 'Comments' then clicks on `Save`.
15. Instructor (A): Clicks on the camera to start recording a video.
16. Instructor (A): Clicks on 'Start Recording'.

17. Instructor (A): Says ‘Hello’ during the recording, clicks ‘Stop Recording’.
18. Instructor (A): Clicks ‘Save Media’.
19. Instructor (A): Enters ‘4’ under ‘Grade out of 5’.
20. Instructor (A): Clicks ‘Submit’.
21. Instructor (A): Clicks the button in the top left to go to the Gradebook.
22. Instructor (A): Clicks ‘Export’ and then ‘Export Entire Gradebook’.
23. Student (A): Clicks ‘Grades’.
24. Student (A): Clicks ‘Technical’.
25. Student (A): Clicks on the media video.
26. Student (A): Clicks on the play button.

1.8 Scenario 4: Collaborative Group Work

Business Processes

- Toepassing didactische werkvorm
- Onderwijsuitvoeringsbegeleiding

Features Tested

- **Groups**: Create and manage groups and verify enrollment in groups and related sections.
- **Discussions**: Facilitate asynchronous forum discussions for brainstorming and Q&A.
- **Collaborations**: Enable real-time co-authoring of documents using the default or integrated tool (default analysis applies to Canvas' own tool if available).

Actors

- Instructor
- Student

Scenario Description

An Instructor sets up groups within the course to support project work and collaborative tasks. The scenario tests group enrollment (simulated manually), the association between sections and groups, and the use of Discussions for Q&A.

Prerequisites

- Scenario 2 was executed.
- Student (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.
- Instructor (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.

Steps

1. Instructor (A): Clicks 'People'.
2. Instructor (A): Clicks '+ Group Set'.
3. Instructor (A): Writes 'Work Group' under 'Group Set Name' and clicks 'Save'.
4. Instructor (A): Clicks '+ Group'.
5. Instructor (A): Writes 'First Group' under 'Group Name' and clicks 'Save'.
6. Instructor (A): Drags Student (A) and Student (B) into 'Work Group'.
7. Instructor (A): Clicks 'Discussions'.
8. Instructor (A): Clicks 'Add Discussion'.
9. Instructor (A): Writes and selects the following before clicking 'Save':
    a. Topic Title: 'Time to Discuss'
    b. Topic content: 'Go ahead.'
    c. This is Group Discussion: 'Work Group'
10. Instructor (A): Clicks the 'Publish Time to Discuss' icon.
11. Student (A): Clicks 'Discussions'.
12. Student (A): Clicks 'Time to Discuss'.
13. Student (A): Clicks 'Reply'.
14. Student (A): Writes 'Desk chair' and clicks 'Reply'.

1.9 Scenario 5: Real-Time Virtual Class and Interactive Sessions

Business Processes

- Toepassing didactische werkvorm
- Onderwijsuitvoeringsbegeleiding

Features Tested

- **Conferences**: Use the default Canvas conference tool (e.g., BigBlueButton, if enabled) or the default virtual classroom setup for real-time sessions.
- **Inbox**: Provide follow-up communication post-session.

Actors

- Instructor
- Student

Scenario Description

An Instructor schedules a virtual class using the Canvas default conference tool. After the session, the Instructor follows up with messages sent through the Inbox, to simulate communication flow that is maintained during and after the session.

Prerequisites

- Scenario 2 was executed.
- Student (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.
- Instructor (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.

Steps

1. Instructor (A): Clicks 'BigBlueButton'.
2. Instructor (A): Clicks 'Add Conference'.
3. Instructor (A): Clicks 'Create'.
4. Instructor (A): Clicks 'Start' near the just created conference. BigBlueButton (out of scope) starts.
5. Instructor (A): In BigBlueButton, the actor joins the call listen only.
6. Student (A): Clicks 'BigBlueButton'.
7. Student (A): Clicks 'Join' near the just created conference.
8. Student (A): In BigBlueButton, the actor joins the call listen only.
9. Instructor (A): Clicks the red leave icon and clicks 'End session for all'.
10. Instructor (A): Clicks 'End session for all users'.
11. Instructor (A): Clicks 'Open Learning Analytics Dashboard'.
12. Instructor (A): Closes the two windows.
13. Instructor (A): Clicks 'End' near the just created conference.
14. Instructor (A): Clicks 'Inbox' within Canvas LMS.
15. Instructor (A): Clicks the 'Compose a new message' icon.
16. Instructor (A): Writes and selects the following before clicking on 'Send':
    a. Course: 'Technical Privacy Research'
    b. To: 'All in Technical Privacy Research'
    c. Subject: 'Fun conference'
    d. Message: 'It was fun!'

17. Student (A): Clicks ‘Inbox’ within Canvas LMS.
18. Student (A): Clicks the email ‘Fun conference’.

1.10 Scenario 6: Peer Review and Structured Feedback

Business Processes

- Toetsbeoordeling
- Vaststelling verworven competenties

Features Tested

- **Peer Reviews**: Enable students to review each other's submissions in a structured manner.
- **SpeedGrader**: Supplement the peer review process and verify feedback quality.
- **Outcomes and Rubrics**: Apply standardised criteria in assessing competence.

Actors

- Instructor
- Student

Prerequisites

- Scenario 2 was executed.
- Student (A) and Student (B) are logged in and are on the 'Home' page of the 'Technical Privacy Research' course.
- Instructor (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.
- An assignment is created with the following configuration:
    - Assignment Name: 'Technical Peer'
    - Body: 'Let's dive into peers.'
    - Points: 5
    - Submission Type: 'Online', 'File Uploads'
    - Selected 'Require peer reviews', with 'Manually assign peer reviews'

Steps

1. Instructor (A): Clicks 'Assignments'.
2. Instructor (A): Clicks 'Technical Peer'.
3. Instructor (A): Clicks 'Peer reviews'.
4. Instructor (A): Clicks 'Give <Student (B)> another submission to assess', selects Student (A), and clicks 'Add'.
5. Instructor (A): Repeats step 4 but reverses the students.
6. Instructor (A): Clicks 'Back to assignment'
7. Instructor (A): Clicks 'Publish'.
8. Student (A): Clicks 'Assignments'.
9. Student (A): Clicks 'Technical Peer'
10. Student (A): Clicks 'Start Assignment'.
11. Student (A): Drags 'Sample Document - SURF.docx' in the file upload and clicks 'Submit assignment'.
12. Student (B): Clicks 'Assignments'.
13. Student (B): Clicks 'Technical Peer'
14. Student (B): Clicks 'Start Assignment'.
15. Student (B): Drags 'Sample Document - SURF.pdf' in the file upload and clicks 'Submit assignment'.
16. Student (B): Clicks '<Student (A)> under 'Assigned peer reviews'.

17. Student (B): Clicks ‘Sample Document - SURF.docx’ to download it.
18. Student (B): Writes ‘Splendid.’ in the ‘Add a comment’ body and clicks ‘Save’.
19. Student (A): Clicks ‘Grades’.
20. Student (A): Clicks the comment icon near ‘Technical Peer’

Scenario Description
Within a peer review assignment, an Instructor orchestrates the process where Students are assigned to review their peers' work using Canvas’s Peer Review functionality. The Instructor then uses SpeedGrader to verify, complement, and calibrate the reviews with predefined outcomes and rubrics.

1.11 Scenario 7: Analysing Student Data with Analytics

Business Processes

- Toepassing leermaterialen
- Onderwijseenheidontwikkeling

Features Tested

- **Analytics Hub**: Use the New Analytics feature to process and display performance data.

Actors

- Instructor

Scenario Description

An IT Administrator accesses the Analytics Hub to analyse student performance data. In doing so, the scenario tests that Intelligent Insights operates with anonymised or aggregated data. This ensures that while performance trends and group-level insights are available, individual student data remains protected to comply with privacy regulations.

Prerequisites

- Scenarios 1 until 6 were executed.
- Instructor (A) is logged in and is on the 'Home' page of the 'Technical Privacy Research' course.

Steps

1. Clicks 'New Analytics'.
2. Clicks 'Weekly Online Activity'.
3. Clicks 'Students'.
4. Clicks 'Reports'.
5. Clicks 'Run report' behind 'Class Roster'.
6. Clicks 'Run report'.

1.12 Scenario 8: Reporting an Issue

Business Processes

- Onderwijsuitvoeringsevaluatie

Features Tested

- Canvas Admin Console: Enable the reporting of issues via the administrative console rather than through the Help Function.

Actors

- Instructor

Scenario Description

- An instructor uses the help functionality to formally report an issue encountered during testing. The process includes the creation of a support ticket through the console, ensuring that problems are communicated and resolved by the central functional team.

Prerequisites

- Instructor (A) is logged in and is on the 'Dashboard'.

Steps

1. IT Administrator: Clicks 'Help'.
2. IT Administrator: Writes and selects the following before clicking on 'Submit Ticket:
    a. Subject: 'Help Ticket Test'
    b. Description: 'Please discard.'
    c. How is this affecting you?: 'Just a casual question, comment, idea, or suggestion'

Appendix 2 Default Roles and Authorisations

The table below shows all the default course roles and authorisations within Canvas LMS. The cursive text within the permissions column means that those permissions can be controlled independently. 'All' means that this role has been assigned all permissions, and 'None' means no permissions have been assigned.

Permissions	Student	Teacher	TA	Designer	Observer
Analytics - view pages	None	All	All	None	None
Announcements - view	All	All	All	All	All
Conversations - send messages to entire class	None	All	All	All	None
Conversations - send messages to individual course members	All	All	All	All	None
Course Calendar - add / edit / delete	None	All	All	All	None
Courses - change visibility	None	All	All	All	None
Discussions - create	All	All	All	All	None
Discussions - moderate	None	All	All	All	None
Discussions - post	All	All	All	All	None
Discussions - view	All	All	All	All	All
Grades - edit	None	All	All	None	None
Grades - select final grade for moderation	None	All	All	None	None
Grades - view all grades	None	All	All	None	None
Grades - view audit trail	None	None	None	None	None

Groups - view all student groups	None	All	All	All	None
Item Banks - manage account	None	None	None	None	None
Item Banks - share with subaccounts	None	None	None	None	None
Learning Outcomes - add / edit / delete	None	All	None	All	None
Learning Outcomes - import	None	All	None	All	None
Manage Assignments and Quizzes ***(add / delete / edit)***	None	All	All	All	None
Manage Course Content ***(add / delete / edit)***	None	All	All	All	None
Manage Course Files ***(add / delete / edit)***	None	All	All	All	None
Manage Course Sections ***(add / delete / edit)***	None	All	None	All	None
Manage Courses ***(conclude / delete / publish / reset)***	None	Conclude, publish	None	Conclude, publish	None
Manage Groups ***(add / delete / manage)***	None	All	All	All	None
Manage LTI ***(add / delete / edit)***	None	All	All	All	None
Manage Pages	None	All	All	All	None

(create / delete / update)					
Outcome Mastery Scales - add / edit	None	None	None	None	None
Outcome Proficiency Calculations - add / edit	None	None	None	None	None
Question banks - view and link	None	All	All	All	None
Reports - manage	None	All	All	All	None
Rubrics - add / edit / delete	None	All	All	All	None
SIS Data - read	None	All	None	None	None
Student Collaborations - create	All	All	All	All	None
Submission - Submit on behalf of student	None	None	None	None	None
Users - Designers ***(add / remove in courses)***	None	All	None	None	None
Users - Observers ***(add / remove in courses)***	None	All	All	All	None
Users - Students ***(add / remove in courses)***	None	All	All	All	None
Users - TAs ***(add / remove in courses)***	None	All	None	None	None
Users - Teachers ***(add / remove in courses)***	None	All	None	None	None
Users - allow administrative actions in courses	None	All	None	None	None

Users - generate observer pairing codes for students	None	None	None	None	None
Users - manage students in courses	None	All	All	All	None
Users - view list	All	All	All	All	None
Users - view login IDs	None	All	All	None	None
Users - view primary email address	None	All	All	None	None
Web Conferences - create	All	All	All	All	None

Table 10 Default Course Roles and Authorisations

Appendix 3 Mapped Endpoints

Scenario	Endpoint	Seen	ISP	Location
Scenario 1 - Canvas Student Android - Student (A)	canvaslmsreview.instructure.com	150	Amazon Technologies Inc.	Germany
Scenario 1 - Canvas Student Android - Student (A)	du11hjcvx0uqb.cloudfront.net	3	Amazon.com Inc.	Netherlands
Scenario 1 - Canvas Student Android - Student (A)	sso.canvaslms.com	1	Amazon.com Inc.	United States
Scenario 1 - Student (A)	canvaslmsreview.instructure.com	109	Amazon Technologies Inc.	Germany
Scenario 1 - Student (A)	du11hjcvx0uqb.cloudfront.net	3	Amazon.com Inc.	Netherlands
Scenario 1 - Student (A)	fonts.cdnfonts.com	1	CloudFlare Inc.	United States
Scenario 1 - Student (A)	sso.canvaslms.com	1	Amazon.com Inc.	United States
Scenario 2A - Part 1 - IT Administrator	canvaslmsreview.instructure.com	87	Amazon Technologies Inc.	Germany
Scenario 2A - Part 1 - IT Administrator	du11hjcvx0uqb.cloudfront.net	2	Amazon.com Inc.	Netherlands
Scenario 2A - Part 2 - Instructor (A)	canvaslmsreview.instructure.com	203	Amazon Technologies Inc.	Germany
Scenario 2A - Part 2 - Instructor (A)	du11hjcvx0uqb.cloudfront.net	6	Amazon.com Inc.	Netherlands
Scenario 2B - Part 1 - Instructor (A)	canvaslmsreview.instructure.com	52	Amazon Technologies Inc.	Germany
Scenario 2B - Part 2 - Student (A)	canvaslmsreview.instructure.com	15	Amazon Technologies Inc.	Germany
Scenario 3A - Instructor (A)	canvaslmsreview.instructure.com	78	Amazon Technologies Inc.	Germany
Scenario 3A - Instructor (A)	canvaslmsreview.quiz-lti-fra-prod.instructure.com	49	Amazon Technologies Inc.	Germany
Scenario 3A - Instructor (A)	du11hjcvx0uqb.cloudfront.net	1	Amazon.com Inc.	Netherlands

Scenario 3B - Part 1 - Student (A)	canvaslmsreview.instructure.com	34	Amazon Technologies Inc.	Germany
Scenario 3B - Part 1 - Student (A)	canvaslmsreview.quiz-lti-fra-prod.instructure.com	57	Amazon Technologies Inc.	Germany
Scenario 3B - Part 2 - Instructor (A)	canvaslmsreview.instructure.com	340	Amazon Technologies Inc.	Germany
Scenario 3B - Part 2 - Instructor (A)	du11hjcvx0uqb.cloudfront.net	14	Amazon.com Inc.	Netherlands
Scenario 3B - Part 2 - Instructor (A)	fonts.cdnfonts.com	2	CloudFlare Inc.	United States
Scenario 3B - Part 2 - Instructor (A)	sso.canvaslms.com	1	Amazon.com Inc.	United States
Scenario 3B - Part 3 - Student (A)	canvaslmsreview.instructure.com	41	Amazon Technologies Inc.	Germany
Scenario 3B - Part 3 - Student (A)	du11hjcvx0uqb.cloudfront.net	2	Amazon.com Inc.	Netherlands
Scenario 4 - Part 1 - Instructor (A)	canvaslmsreview.instructure.com	88	Amazon Technologies Inc.	Germany
Scenario 4 - Part 2 - Student (A)	canvaslmsreview.instructure.com	20	Amazon Technologies Inc.	Germany
Scenario 5 - Instructor (A)	canvaslmsreview.instructure.com	45	Amazon Technologies Inc.	Germany
Scenario 5 - Instructor (A)	mxoa230004.rna1.blindsidenetworks.com	113	OVH Hosting Inc.	Canada
Scenario 5 - Student (A)	canvaslmsreview.instructure.com	38	Amazon Technologies Inc.	Germany
Scenario 5 - Student (A)	mxoa230004.rna1.blindsidenetworks.com	61	OVH Hosting Inc.	Canada
Scenario 6 - Part 1 - Instructor (A)	canvaslmsreview.instructure.com	27	Amazon Technologies Inc.	Germany
Scenario 6 - Part 2 - Student (A)	canvaslmsreview.instructure.com	28	Amazon Technologies Inc.	Germany
Scenario 6 - Part 3 - Student (B)	canvaslmsreview.instructure.com	37	Amazon Technologies Inc.	Germany
Scenario 6 - Part 3 - Student (B)	du11hjcvx0uqb.cloudfront.net	1	Amazon.com Inc.	Netherlands

Scenario 6 - Part 4 - Student (A)	canvaslmsreview.instructure.com	4	Amazon Technologies Inc.	Germany
Scenario 7 - Instructor (A)	canvas-analytics-fra-prod.inscloudgate.net	38	Amazon Technologies Inc.	Germany
Scenario 7 - Instructor (A)	canvaslmsreview.instructure.com	22	Amazon Technologies Inc.	Germany
Scenario 8 - Instructor (A)	canvaslmsreview.instructure.com	5	Amazon Technologies Inc.	Germany

Table 11 Mapped Endpoints during Technical Research